Revista Científica Multidisciplinar G-ner@ndo

ISSN: 2806-5905

Vinculación con la sociedad: capacitación para el buen manejo de las tecnologías por parte de la Universidad Técnica "Luis Vargas Torres" de Esmeraldas

Links with society: training for the good management of technologies by the Technical University "Luis Vargas Torres" of Esmeraldas.

Ing. Rómulo Sandino Jurado Calero; Ing. Richard A. Macias-Lara; Ing. Alan Eduardo Leyva Méndez; Ing.Héctor Andrés Sacón-Klinger; Ing. Cindy Johanna Choez Calderón

APRENDIZAJE

Diciembre, V°3-N°2; 2022

- ✓ **Recibido:** 10/11/2022
- ✓ **Aceptado**: 30/11/2022
- ✓ **Publicado:** 05/12/2022

INSTITUCIÓN

- **Universidad Técnica Luis Vargas Torres de Esmeraldas**
- **Universidad Técnica Luis Vargas Torres de Esmeraldas**
- **Universidad Técnica Luis Vargas Torres de Esmeraldas**
- **Universidad Técnica Luis Vargas Torres de Esmeraldas**
- **Universidad Técnica Luis Vargas Torres de Esmeraldas**

CORREO:

- ✉ romulo.jurado.calero@utelvt.edu.ec
- ✉ alejandro.macias@utelvt.edu.ec
- ✉ alan.leyva@utelvt.edu.ec
- ✉ hector.sacon.klinger@utelvt.edu.ec
- ✉ cindy.choez.calderon@utelvt.edu.ec

ORCID:

- https://orcid.org/0000-0001-7642-692X
- https://orcid.org/0000-0003-2164-3171
- https://orcid.org/0000-0002-1647-1953
- https://orcid.org/0000-0001-6585-4793
- https://orcid.org/0000-0003-3968-9397

FORMATO DE CITA APA.

Jurado, R. Macias, R. Leyva, A. Sacón, H. Choez, C. *(2022). Propuesta de una virtualización de servicios usando Amazon Web Services para la Universidad Técnica Luis Vargas Torres de Esmeraldas*. Revista *G-ner@ndo, V°3 (N°2,).115 -129.*

Resumen

Los estragos que dejó la pandemia Covid-19 se enmarcan en el desempleo y el uso indiscriminado de la tecnología con acceso a internet, causando este segundo ítem problemas muy concurrentes en la actualidad y que cada vez van sumando, este uso fue prácticamente obligatorio para toda la ciudadanía debido al teletrabajo y educación virtual tanto para personas que tenían conocimiento sobre ella y para los que no tienen conocimiento de los riesgos a los que se enfrentan. Del mismo modo, luego de varios años haber terminado la pandemia, los niños, adolescentes y adultos siguen usando la tecnología llegando a la adicción de esta. El objetivo principal de este proyecto es socializar conocimientos de los riesgos que se presentan en la web, personas vulnerables, identificar a los ciberdelincuentes, evitar se víctima, y leyes que regulan con pena privativa de libertas estos delitos. Se empleó la metodología mixta cualitativo-cuantitativo que permitió evaluar la experiencia de capacitadores y realizar el análisis estadístico de los temas capacitados. Las personas de este sector pueden reconocer los tipos de delitos informáticos, como actuar ante un delito, como brindar ayuda y sobre todo las medidas necesarias para evitar ser víctima.
Palabras claves: buen manejo de tecnologías, ciberdelincuentes, COIP, uso indiscriminado de la tecnología.

Abstract

The ravages left by the Covid-19 pandemic are part of unemployment and the indiscriminate use of technology with internet access, causing this second item very common problems today and which are adding up each time, this use was practically mandatory for all citizenship due to teleworking and virtual education both for people who were aware of it and for those who are unaware of the risks they face. In the same way, after several years of the end of the pandemic, children, adolescents and adults continue to use technology, becoming addicted to it. The main objective of this project is to socialize knowledge of the risks that occur on the web, vulnerable people, identify cybercriminals, avoid being a victim, and laws that regulate these crimes with custodial sentences. The qualitative-quantitative mixed methodology was used, which allowed the evaluation of the experience of trainers and the statistical analysis of the subjects trained. People in this sector can recognize the types of computer crimes, how to act in the face of a crime, how to provide help and, above all, the necessary measures to avoid being a victim.

Keywords: good management of technologies, cybercriminals, COIP, indiscriminate use of technology.

Introducción

Los diferentes problemas de tipo económico, social, ambiental en que se debate la provincia de Esmeraldas, constituye un serio y preocupante factor que ha sumido en la desesperación no solo a los esmeraldeños, sino a todo el pueblo ecuatoriano, situación que se ahonda más si consideramos las afectaciones y repercusiones a las que están sometidas las comunidades por el desenfrenado impacto que generó la pandemia del Covid19, cuya expresión fatal, es el desempleo masivo y delincuencia (Macías et al., 2021). Es muy común observar, la pobreza de las clases marginales, despidos intempestivos, desocupación, escuelas y colegios cerrados, con un Sistema de Educación Virtual y otros de manera indefinida. Sin embargo, cabe mencionar que otro de los efectos secundarios que dejó la pandemia fue la del uso y abuso de las tecnologías tanto en adolescentes, adultos y niños generando adicción y cambios en el comportamiento de las personas (Cobo, 2019).

Esmeraldas ciudad del Ecuador; según el Instituto Nacional de Estadística y Censos (INEC) 2010, con alrededor de 130.000 habitantes; del cual el 5.80% representa la parroquia Vuelta Larga donde será aplicado este proyecto, teniendo el 82% de personas que hacen uso del internet desde teléfonos inteligentes y computadoras; cuya cantidad aumentó considerable mente y aún se mantienen luego de la pandemia Covid-19, se constatan mediante redes sociales, canales de noticias locales y mediante la policía nacional la denuncia sobre: acoso sexual, fraude electrónico, extorsión entre otros delitos informáticos.

Las personas que no tienen amplio conocimiento pasan desapercibidas de los avances y desarrollos tecnológicos, cuyo rol es causado por la extrema pobreza y limitaciones, unida a la falta de medios y de capacitación para desarrollo de una educación virtual. Frente a este agudo problema, la Dirección de vinculación con la comunidad y Prácticas Pre-profesionales de la Carrera de Tecnología de la Información, de la Facultad de Ingenierías de la Universidad Técnica Luis Vargas Torres, fiel a uno de los principios que establece tanto la Ley de Educación Superior, como los Estatutos de la Universidad, ha considerado importante desarrollar e implementar un

proyecto de capacitación en materia de seguridad en el uso de las tecnologías de la información y comunicación (TIC) en la parroquia de Vuelta Larga, con participación de los estudiantes y docentes colaboradores de esta carrera.

El propósito fundamental de este Proyecto es el aprovechamiento de la voluntad, interés de los docentes, padres de familia, moradores de la parroquia y estudiantes con el fin de desarrollar un modelo teórico – práctico, para mejorar y propiciar la comunicación en relación con el avance y alcance tecnológico, en el marco de la Vinculación Comunitaria; teniendo como principio: a) capacitar técnicamente a la comunidad en el desarrollo de la información y comunicación; b) fortalecer la capacidad individual como colectiva, de aportar conocimientos, habilidades y actitudes para el buen uso de las TIC, y, coordinar con los líderes comunales el fortalecimiento y aplicación de los conocimientos adquiridos.

El artículo está seccionado de la siguiente manera: en la sección I, el estado del arte; donde se detallarán los conceptos fundamentales sobre los delitos más concurridos en la actualidad; en la sección II, los materiales y métodos empleados para la búsqueda y fortalecimiento de la información empleados, y, técnicas empleadas para cumplir los objetivos de este proyecto; en la sección III, los resultados obtenidos luego de realizar las sesiones de capacitaciones a los moradores del lugar; en la sección IV, las conclusiones generadas y en la última sección las referencias bibliográficas científicas.

Estado del arte

Los niños y jóvenes pasan cada vez más tiempo libre frente a las pantallas, los motivos van desde las puras necesidades educativas hasta el ocio y las relaciones sociales con los compañeros. Por ende, cualquier cosa que se pueda dirigir correctamente puede tener un impacto positivo en la persona, puede salirse fácilmente de control y afectar negativamente su capacidad para manejar las relaciones sociales, el comportamiento y las emociones. Por otra

parte, la tecnología en sí no es dañina, pero las actitudes habituales hacia la tecnología pueden generar cambios negativos a nivel personal y social (Vega, 2012).

En la misma línea, Alberola (2020) indica que: el debate sobre el mal uso de los smartphones, ordenadores, videojuegos y otros dispositivos ha abierto un nuevo capítulo con el primer caso de 'Whatsappitis' del mundo. Esto a su vez causa efectos secundarios como: patología por movimientos y esfuerzos de repetición, la fatiga auditiva, además, el excesivo uso de estos dispositivos no acarrea solo problemas físicos si no psicológicos, estos han sido vinculados a la dependencia de estos dispositivos, llevando incluso a producir temores como la 'nomofobia', el miedo a quedarse sin cobertura, que se agote la batería o no encontrar el móvil.

De esta manera, en el caso de niños y adolescentes, la falta de control por parte de los adultos deja el camino libre para acceder sin control a internet. Por ende, si el equipo informático no dispone de filtros que limiten el acceso a este tipo de información, de forma accidental o buscando nuevos amigos y estímulos se irán encontrando allí con toda clase de contenidos, servicios y personas, todo lo que inicia por curiosidad puede acabar en una adicción ya que los niños y los adolescentes son fácilmente atraídos, y, por desgracia hay muchas personas que no son conscientes de estos peligros que ahora se multiplican en Internet; cada vez más omnipresente y accesible a todos en las casas, escuelas, cibercafés, smartphones, entre otros. De este modo, todas las funcionalidades de Internet como: navegación por las páginas web, publicación de weblogs y webs, correo electrónico, mensajería instantánea, foros, chats, gestiones y comercio electrónico, entornos para el ocio, entre otros, pueden comportar algún riesgo, al igual que ocurre en las actividades que realizamos en el mundo real (Macías et al., 2022; Peris et al., 2018).

En la misma línea, los delitos informáticos son toda aquella acción que tiene como existencia un delito con ayuda del uso de la informática, y, entre ellos como menciona (Fernández & Martínez, 2018; Macías et al., 2022) se tiene los siguientes delitos: contra la libertad (amenaza, acoso), contra la integridad moral (trato degradante), contra la libertad sexual (child grooming,

pornografía infantil), contra la intimidad (descubrimiento y revelación de datos secretos), contra el honor (Injurias/Calumnias), contra el patrimonio y orden socioeconómico (estafa, descubrimiento de secretos empresariales, daños informáticos o sabotaje, delito a la propiedad intelectual, delito contra servicios), falsedad o falsificación, discriminación o violencia y odio.

Con base en lo anterior, es necesario comprender algunos de los métodos más empleados por los ciberdelincuentes que afectan la integridad de las personas y/o sistemas, entre ellos están: a) Malware; es el método más empleado haciéndose pasar como un software que es enviado por correo electrónico o algún tipo de mensajería o en otras ocasiones oculto en descargas de archivos, entre ellos destacan los siguientes tipos (virus; un archivo que se introduce en el sistema operativo con la capacidad de reproducirse infectando todo, troyano; este tipo se disfraza como un software legítimo que se encarga de recopilar información del usuario y en otros casos causando daño al equipo, spyware; software que se registra en secreto generalmente usado para capturar datos de tarjetas de crédito, ransomware; aplicación que bloqueo los archivos del usuario con amenazas de eliminarlos o difundirlos a cambio de pago, adware; software que muestra mucha publicidad en páginas o equipos con la intensión de difundir algún malware, y, botnets; redes de computadoras que los hackers utilizan para realizar acciones sin consentimiento de los usuarios), b) Inyección de código SQL; que por sus siglas significa lenguaje de consultas estructurado, generalmente lo utilizan hackers que se aprovechan de las vulnerabilidades de los sistemas para hacerse con información confidencial que se almacena en las bases de datos, c) Phishing; generalmente este tipo de ataques con empleados por mejería haciéndose pasar por empresas que solicitad información de datos personales o tarjetas de crédito, d) ataque de tipo “man-in-the-middle”; hombre en medio generalmente ocurre cuando la red wifi no es tan segura y es accedida por hackers escuchando todos los paquetes que se envían y reciben a través del internet, e) ataque de negación de servicios; ataques dirigidos especialmente a empresas para evitar que sus aplicaciones satisfagan las solicitudes sobrecargando las redes y los servidores. Cabe mencionar que uno de los casos más frecuentes

que se están viendo luego de pandemia son relacionados con: pornografía infantil y estafa en la web.

Ahora bien, según Linvill & Warren (2018) los trolls; personas que se cuelan en cualquier lugar en la red donde se puedan hacer comentarios para causar controversia y fomentar el enfrentamiento entre otros llamando la atención y molestar, esto viene a raíz de los 90 donde el troleo tenía la intención de realizar bromas, pero, a partir del avance de la tecnología surge un cambio de concepto llamado flame “flameo” que es la práctica de publicar comentarios que se cruzan con el troll que abunda en las redes sociales, foros o páginas web. Esto era necesario mencionarlo porque es latente en el día a día.

También, es necesario saber que el perfil del delincuente informático varía mucho y cada vez estos van tomando nuevas medidas para no ser detectados aprovechándose generalmente de personas vulnerables y sobre todo de la información que suelen publicar en redes sociales o registrar en páginas de dudosa procedencia. En el estudio de Arroyo (2020) se afirma que el 76% de los delincuentes imputados son de género masculino, siendo especialmente partícipes den delitos sexuales con un (75%) y en usurpación de información con un (20%) mientras que en falsificación y fraude informático se registran entre el (1% y 5%), y, paralelamente un estudio realizado por el primer investigador de seguridad informática de américa latina analizando 13.000 dispositivos de diversos sectores con el fin de prever las tendencias en seguridad informática, se obtuvieron los siguientes resultados sobre el perfil de un ciberdelincuente: constatando con las investigación de (Arroyo, 2020; Cedeño, 2022; Fernández & Martínez, 2018; González, 2019; Mayer & Calderón, 2020; Suárez, 2020) se tiene que son una criminalidad joven masculina que oscila entre los 14 y 40 años teniendo un promedio de 35 años.

Por otra parte, en Garitaonandia et al. (2020) exponen que: en cada casa existen alrededor de una media de 5,4 dispositivos conectados al internet, esto desde ya representa un riesgo si no se tienen las medidas necesarias. En este caso, la ciberseguridad juega un papel muy importante siendo esta la práctica de defender cualquier dispositivo electrónico que esté

conectado al internet, de esta manera se reduce de significativamente los delitos cibernéticos, ciberataques, ciberterrorismo, también, la ciberseguridad proporciona beneficios en: seguridad de red, seguridad de las aplicaciones, seguridad de la información, seguridad operativa, recuperación ante desastres y la continuidad de cualquier negocio (Kaspersky, 2022).

En efecto, con la información antes mencionada es evidente que existe gran variedad de riesgos especialmente en los niños que hacen uso libre del internet, es por ello que es necesario mencionar ciertos aspectos que ayudarían a reducir en gran medida este tipo de delitos, y entre ellos tenemos el control parental; es una herramienta que permite a los padres controlar o limitar ya sea por filtros u horario predeterminado del contenido que visualizan en internet, evitando así caer en alguno de los ciberdelitos antes mencionados, y, entre las características que más se destacan en el control parental son: a) Control Web; permite bloquear sitios en funciones de las categorías existentes, b)control de aplicaciones; se puede bloquear el acceso a diferentes aplicaciones como mensajerías o navegadores web, c) bloqueo de llamadas; en el caso de los teléfonos no podrían recibir ni hacer llamadas solo al número predeterminado que se deje configurado si fuera el caso, d) tiempo de uso; se puede bloquear el dispositivo de acuerdo al tiempo en horas o minutos que se configure, e) alarmas; se pueden programar alarmas en base a lo que dispone el tipo de aplicación instalada, f) geolocalización; puede obtener la dirección en tiempo real del dispositivo configurado, y por último el botón de emergencia; que en caso de requerir al presionar automáticamente sonará la alarmar en todos los dispositivos configurados (Coronel, 2018; Villanueva & Serrano, 2019).

En el mismo campo, en varios estudios como son el de (Coello & Saltos, 2022; Koplewicz, 2021; Coronel, 2018), y páginas web se recomiendan las siguientes aplicaciones gratuitas para el control parental: a) Secure Kids; herramienta que dispone de una página web y una aplicación para dispositivo móvil para poder controlar todos los movimientos del dispositivo configurado, este tiene las características de internet, llamadas, geo localizador, interacción con dispositivo, alarmas, descansos y botón de emergencia, y b) FamiSafe; aplicación con cierto periodo de

tiempo gratuito, al igual que la anterior cuenta con una aplicación para dispositivos móviles pero para IOS presenta menos funcionalidades, de igual manera cuenta con: bloqueador de aplicaciones, tiempo de uso del dispositivo, historial de ubicaciones, historial de navegación y filtrado de páginas web.

Acuñando a lo antes expuesto, en Kaspersky (2022) y Macías et al. (2022) afirman las siguientes recomendaciones para evitar ser víctima de este tipo de delitos.

Tabla 1

Recomendaciones para evitar ser víctima de delitos informáticos

Recomendaciones
Abrir cuentas bancarias solo en equipos personales.
Activar el Wifi, Bluetooth y GPS cuando sea necesario; cabe mencionar que solo se debe conectar a redes Wifi de confianza y nunca a las que están abiertas (sin protección).
Aprender a reconocer páginas seguras para no caer en los *fake page* (clones de páginas, páginas falsas).
Conservar los mensajes, correos electrónicos y cualquier evidencia que sea necesaria para denunciar en caso de ser víctima de la ciberdelincuencia.
Crear una copia de seguridad de los archivos importantes que no quiera perder en caso de infección al equipo.
Denunciar páginas que cometan delitos informáticos.
Descargar aplicaciones de sitios seguros (tiendas oficiales).
Enseñar a los niños el uso del internet y establecer horarios con la supervisión de un adulto de ser necesario.
No abra los correos electrónicos que están en spam, desecharlos inmediatamente.
No compartir claves personales con terceras personas.
No creer en ofertas o premios que ofrecen dinero en internet.
No dar clic a los enlaces que le llegan por correo electrónico, redes sociales o navegando por el internet; copie y pegue el enlace en la barra donde se coloca el URL para verificar que éste sea legítimo.
No divulgar enlaces que promuevan la pornografía, exclusión, xenofobia, autodestrucción, trata de personas o cualquier actividad al margen de la ley.
No guardar contraseñas en computadoras o navegadores públicos, evite la estafa o robo de identificación.
No registrar o brindar información personal en las redes sociales, páginas u otras aplicaciones.
Para proteger la identidad digital, se debe hacer buen uso de las redes sociales y de toda publicación que se realice; así no será blanco fácil para los delincuentes informáticos.
Realizar un filtro de las amistades en Redes Sociales; debe tener solo amistades de confianza y configurar las restricciones de ésta para no mostrar información personal.
Tener actualizado el sistema operativo y aplicaciones de los dispositivos con los que accede regularmente al internet.

Usar contraseñas seguras combinando: mayúsculas, minúsculas, números y algún caracter especial; no usar la misma contraseña para otras cuentas.
Usar un antivirus y cortafuegos con licencia para computadores y smartphone.

Nota. (Macías et al., 2022), es necesaria la obligatoriedad de las recomendaciones antes mencionadas para evitar ser víctima de los riesgos que acarrean en la web.

Asimismo, dentro de todo este marco existen leyes que regulan cada uno de estos tipos de delitos informáticos y en cada país estas penalizaciones pueden variar, en nuestro caso, Ecuador maneja los siguientes reglamentos expuestos y publicados por (COIP, 2021; Macías et al., 2022) ordenados de acuerdo a los años de sentencia privativa.

Tabla 2

Leyes que regulan los tipos de delitos informáticos

Art. COIP	Delito	Sanción (años)
103	Pornografía con utilización de niñas, niños o adolescentes	16 a 19
186	Estafa	5 a 7
211	Supresión, alteración o suposición de la identidad y estado civil	3 a 5
229	Revelación ilegal de base de datos	3 a 5
230	Interceptación ilegal de datos	3 a 5
231	Transferencia electrónica de activo patrimonial	3 a 5
232	Ataque a la integridad de sistemas informáticos	3 a 5
233	Delitos en contra de la información pública reservada legalmente	3 a 5
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5
476	Interceptación de las comunicaciones o datos informáticos	3 a 5
178	Violación a la intimidad	1 a 3
190	Apropiación fraudulenta por medios electrónicos	1 a 3
191	Reprogramación o modificación de información de equipos terminales móviles	1 a 3
192	Intercambio, comercialización o compra de información de equipos terminales móviles	1 a 3
194	Comercialización ilícita de terminales móviles	1 a 3
195	Infraestructura ilícita	1 a 3
298.- punto (8,9,10)	Defraudación tributaria	1 a 3

Nota. (Macías et al., 2022)

Método y materiales

Para obtener el material actualizado sobre este proyecto, se empleó la técnica de la burbuja e ir coincidiendo en investigaciones recientes desde las bibliografías de los artículos seleccionados, claro está que se partió de una cadena de búsqueda: (abuse [AND] technology [OR] indiscriminate [AND] use [AND] technology [OR] good [AND] use [AND] technology) que se empleó en distintas bases de datos científicas (Dialnet, Scielo, Worldwidescience, IEEE y para otros temas relevantes se utilizó Google Académico), esta cadena de búsqueda permito obtener los mejores y más actualizados estudios, reuniendo 48 investigaciones de las cuales se terminaron seleccionando 10 que se acercaron más al tema luego de la revisión del resumen, métodos, resultados y conclusiones, además, las otras 5 referencias bibliográficas se obtuvieron de las referencias de los 10 artículos antes mencionados.

Es así, que de estas investigaciones se pudo obtener la mejor manera de aplicar y enseñar los temas modernos a niños adolescentes y adultos. También, se tomó un diseño cuasiexperimental que considera los resultados antes, durante y después de la capacitación empleada, además, para determinar los alcances y las limitaciones se fundamentó en un enfoque mixto cualitativo-cuantitativo, el alcance de esta investigación abarcó de manera amplia el tema en cuanto a la desinformación y mal uso de las tecnologías en el sector Vuelta Larga de la Provincia de Esmeraldas. Mediante la técnica del muestreo aleatorio simple, se pudo obtener una muestra de 86 participantes, sin embargo, asistieron 102 personas entre niños, adolescentes y adultos. Cabe mencionar, que se empleó el enfoque mixto debido a que se utilizó el cualitativo para evaluar a docentes y estudiantes en cuanto a la experiencia con respecto al tema capacitado, del mismo modo se aplicó el modo cualitativo para el análisis estadístico mediante la aplicación de la técnica de la encuesta sobre los conocimientos adquiridos en cuanto a los delitos informáticos y el buen uso de las tecnologías, además de poder identificar los tipos de delitos y los ciberdelincuentes que acarrean la web.

Análisis de resultados

Mediante el proyecto de capacitación en materia de seguridad en el uso de las TIC´s, en la parroquia Vuelta Larga del cantón Esmeraldas desarrollado por los estudiantes de la carrera de Ingeniería en Sistemas Informáticos, dio a conocer a los participantes de la misma, los riesgos que corren en el uso de internet sin las debidas precauciones, lo propensos que son los menores de edad a caer en redes de pornografía infantil, la importancia de verificar información en las fuentes oficiales antes de ser compartida en las redes sociales, los efectos negativos que estos pueden tener en nuestra vida cotidiana, a ser responsables de la información personal que se publica y se exhibe diariamente, además, tomando como delitos principales: la estafa cibernética, usurpación de identidad, pornografía infantil y ciberbulling. La audiencia mostró interés a los temas expuestos; estudiantes de 4to y 5to de bachillerato de la Unidad Educativa “León Febres Cordero” se hicieron presentes en esta capacitación formando parte del público espectador e interactuando con los expositores, con preguntas y reflexiones referentes a los diferentes temas. Una vez concluida la capacitación, se realizó una encuesta formada por 12 preguntas para valorar los conocimientos obtenidos por los 102 participantes del evento, los resultados de las preguntas más relevantes se muestran a continuación:

Figura 1

¿Conoce los peligros que esconde el internet?

Nota. El 75,67% de los encuestados están conscientes de los peligros que están latentes en la web, a la espera víctimas que no tengan conocimiento y caigan en sus trampas.

Figura 2

¿Sabe identificar los distintos delitos informáticos que a través de redes sociales?

***Nota*.** De las personas capacitadas, el 87,5% sabe identificar de manera muy eficiente los tipos de delitos informáticos que se comparten con o sin consentimiento alguno.

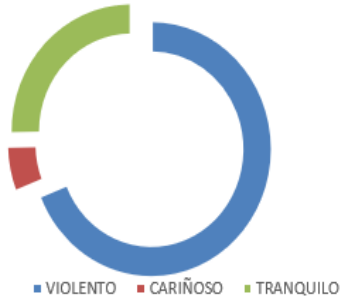
Figura 3

¿Ha sido víctima de algún delito informático?

Nota. *Al saber identificar los delitos informáticos, el 68,75% de las personas reconocen haber sido víctima de algunos delitos informáticos.*

Figura 4

¿Identifica los tipos de personas malintencionadas que están a través del internet?



***Nota*.** Se asevera que el 73% del perfil de un acosador es violento, mientras que el 5% puede ser cariñoso y el 22% está oculto a través de la personalidad tranquila.

Figura 5

¿Los delitos informáticos influyen en el suicido de algunas personas?

Nota. Las causas de suicidio en una víctima de este tipo de ataques según los encuestados son generando en un 42.5% por la depresión, y, 57.5% por baja autoestima, todo esto siendo estragos del Ciberbulling.

Figura 6

¿Conoce quien regula y donde denunciar este tipo de delitos?

***Nota*.** El 83,33% de los encuestados tiene conocimiento de la penalización de este tipo de delitos, y saben a dónde acudir para denunciarlos.

Conclusiones

Los participantes obtuvieron conocimientos sobre los peligros que esconde la internet, la responsabilidad que tiene cada individuo con la información que publicita en las redes sociales y los riesgos que corren los menores a través de los medios digitales. Luego de finalizar la capacitación, los encuestados reconocen haber sido víctima de ciberbulling, estafa, suplantación de identidad y reconocen los trols que están al asecho en el internet. Adquirieron conocimiento sobre las leyes que regulan este tipo de delitos informáticos en el Ecuador, además, saben a dónde acudir cuando sean víctima de algún tipo de delito. Conocen y realizan la instalación de aplicaciones de control parental para llevar el control de los contenidos que visualizan en internet los menores de edad.

Referencias

Alberola, C. (2020). Experiential avoidance and excessive smartphone use: a Bayesian approach. Adicciones, 22(4), 397–404.

Arroyo, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. Derecho y Cambio Social, 60, 470–512. www.derechoycambiosocial.com

Cedeño, R. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la situación actual en el Ecuador. Revista Tecnológica Ciencia y Educación Edwards Deming, 50–62. https://doi.org/10.37957/rfd.v6i1.88

Cobo, C. (2019). Usos y abusos de las tecnologías digitales. https://eduteka.icesi.edu.co/articulos/santillana-cobo-acepto-las-condiciones

Coello, A., & Saltos, M. (2022). Análisis práctico comparativo de herramientas de control parental con licencias gratuitas y pagadas para la seguridad integral a menores de edad en ambientes digitales en la ciudad de guayaquil [Universidad de Guayaquil]. Http://repositorio.ug.edu.ec/bitstream/redug/59774/1/B-CINT-PTG-N. 757 Coello Chancay Analía Pamela. Saltos Bazurto Milena Lilibeth.pdf

COIP. (2021). Código Orgánico Integral Penal. Registro Oficial - Órgano Del Gobierno Del Ecuador, 144. https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Coronel, C. (2018). Seguridad en los niños mediante herramientas de control parental que permita a los padres supervisar el uso de internet. Escuela Superior de Educación En Ciencias Sociales. https://iconline.ipleiria.pt/bitstream/10400.8/3745/1/UPTIC_Cindy%2BCoronel.pdf

Fernández, D., & Martínez, G. (2018). Ciberseguridad, Ciberespacio y Ciberdelincuencia. http://hdl.handle.net/20.500.12226/84

Garitaonandia, C., Karrera-Xuarros, I., Jiménez-Iglesias, E., & Larrañaga, N. (2020). Menores conectados y riesgos online: contenidos inadecuados, uso inapropiado de la información y uso excesivo de internet. El Profesional de La Información, 1–10. https://doi.org/10.3145/epi.2020.jul.36

González, A. (2019). Perfil criminológico del ciberciminal. https://dialnet.unirioja.es/servlet/articulo?codigo=7235547

Kaspersky. (2022). Ciberseguridad. Web Page. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?awc=13872_1670425489_a9244fcad414bbd40a15fdbdb62301d7&redef=1&THR&reseller=de_dach-aff-q1-21_pro_ona_afm__onl_b2c__banner_nay_____&m_soce=AWIN&m_medi=cpa&m_campaign=Home-Sec_AffNayDE&naytrack=nay_an_de

Koplewicz, H. (2021). Scaffold Parenting: Raising Resilient, Self-Reliant, and Secure Kids in an Age of Anxiety (Harmony (ed.)). https://lccn.loc.gov/2020021227

Linvill, D. L., & Warren, P. L. (2018). Troll Factories: the IRA and State-Sponosred Agenda Building. Working Paper.

Macías, R., Fabricio, M., Andrade, B., Angulo, F., Mendoza, J., Loor, M., & Estupiñan, G. (2022). Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática. Sapienza, 3, 231–243. https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/324/199

Macías, R., Alvarado, L., & Días, M. (2021). El Covid-19 en la incidencia delictiva. Estudios Multidisciplinarios en América Latina y el Caribe (2021). http://www.editoraappris.com.br/

Mayer, L., & Oliver Calderón, G. (2020). El delito de fraude informático: concepto y delimitación. Revista Chilena de Derecho y Tecnología, 9(1), 151. https://doi.org/10.5354/0719-2584.2020.57149

Peris, M., Maganto, C., & Garaigordobil, M. (2018). Escala de riesgo de adicción-adolescente a las redes sociales e internet: Fiabilidad y validez (ERA-RSI). Revista de Psicologia Clinica Con Ninos y Adolescentes, 5(2), 30–36. https://doi.org/10.21134/rpcna.2018.05.2.4

Suárez, A. (2020). El delito informático. In Manual del delito informático en Colombia. Análisis dogmático de la ley 1273 de 2009 (pp. 49–70). Universidad del Externado de Colombia. https://doi.org/10.2307/j.ctv1503j6n.7

Vega, M. (2012). Aspects and advances in science, technology and innovation. Colombian Journal of Bioethics., 11(33). https://www.redalyc.org/articulo.oa?id=30525012025

Villanueva, V., & Serrano, S. (2019). Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género. Revista de Psicología y Educación - Journal of Psychology and Education, 14(1), 16. https://doi.org/10.23923/rpye2019.01.168