Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática

Frequent cases, criminalization and prevention of computer crimes in Ecuador: a brief systematic review

Casos frequentes, criminalização e prevenção de crimes informáticos no Equador: uma breve revisão sistemática

Richard Alejandro Macías-Lara
alejandro.macias@utelvt.edu.ec
https://orcid.org/0000-0003-2164-3171
Universidad Técnica Luis Vargas Torres de Esmeraldas-Ecuador

Miguel Fabricio Boné Andrade
miguel.bone@utelvt.edu.ec
https://orcid.org/0000-0002-8635-1869
Universidad Técnica Luis Vargas Torres de Esmeraldas-Ecuador

Francisco Quiñonez Angulo
francisco.quinonez.angulo@utelvt.edu.ec
https://orcid.org/0000-0002-5290-6969
Universidad Técnica Luis Vargas Torres de Esmeraldas-Ecuador

José Javier Mendoza Loor
jose.mendoza.loor@utelvt.edu.ec
https://orcid.org/0000-0001-8623-872X
Universidad Técnica Luis Vargas Torres de Esmeraldas-Ecuador

Giuseppe Estupiñan-Troya
Giuseppe.estupinan.troya@utelvt.edu.ec
https://orcid.org/0000-0002-4625-9259
Universidad Técnica Luis Vargas Torres de Esmeraldas-Ecuador

Jaime Darío Rodríguez Vizuete
jaime.rodriguez.vizuete@utelvt.edu.ec
https://orcid.org/0000-0003-1397-718X
Universidad Técnica Luis Vargas Torres de Esmeraldas-Ecuador

RESUMEN

Los delitos informáticos a nivel internacional y nacional han aumentado de manera significativa durante y después de pandemia, tal es el caso que los reportes de los diarios, redes sociales y noticias televisivas del Ecuador mencionan que los casos más comunes de este tipo es la suplantación de identidad, falsificación de documentos, apropiación fraudulenta por medios electrónicos, acoso no consentido a un sistema informático, contacto con la finalidad sexual con menores, ataques a la integridad de sistemas informáticos, interceptación ilegal de datos, transferencia electrónica sin consentimiento y revelación ilegal de datos. Este estudio tiene como objetivo principal dar a conocer las técnicas que utilizan los ciberdelincuentes en el Ecuador, socializar la penalización y sugerencias para evitar ser víctima de este tipo de delitos. Para culminar con el proceso se empleó la metodología Estudio de Mapeo Sistemático (SMS), donde permitió iniciar con la definición de la búsqueda, luego con la ejecución de la búsqueda y finalizando con la discusión y resultados. Como resultados se generaron respuestas de las preguntas de investigación específica (PIs1, PIs2, PIs3, PIs4 y PIs5) teniendo éxito en la revisión sistemática. En conclusión, se sugiere al gobierno e instituciones públicas y privadas promover capacitaciones donde se socialicen los riesgos y tipos de delitos informáticos, reglamento que regula estos actos delictivos con relación a la tecnología y consejos para poder protegerse y estar a la vanguardia de los cibercriminales.

Palabras claves: Ciberdelincuencia, Delitos Informáticos en el Ecuador, COIP, Prevención de Delitos Informáticos.

ABSTRACT

Computer crimes at the international and national level have increased significantly during and after the pandemic, such is the case that the reports of newspapers, social networks and television news in Ecuador mention that the most common cases of this type are identity theft, falsification of documents, fraudulent appropriation by electronic means, non-consensual harassment of a computer system, sexual contact with minors, attacks on the integrity of computer

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

systems, illegal interception of data, electronic transfer without consent and illegal disclosure of data. The main objective of this study is to publicize the techniques used by cybercriminals in Ecuador, socialize the penalty and suggestions to avoid being a victim of this type of crime. To culminate with the process, the Systematic Mapping Study (SMS) methodology was used, where it allowed to start with the definition of the search, then with the execution of the search and ending with the discussion and results. As a result, answers to the specific research questions (PIs1, PIs2, PIs3, PIs4 and PIs5) were generated, being successful in the systematic review. In conclusion, it is suggested to the government and public and private institutions to promote training where the risks and types of computer crimes are socialized, regulations that regulate these criminal acts in relation to technology and advice to protect themselves and be at the forefront of cybercriminals.

Keywords: Cybercrime, Computer Crime in Ecuador, COIP, Prevention of Computer Crimes.

RESUMO

Os crimes informáticos a nível internacional e nacional aumentaram significativamente durante e após a pandemia, tal é o caso que reportagens de jornais, redes sociais e telejornais do Equador mencionam que os casos mais comuns deste tipo são a falsificação de identidade, falsificação de documentos, apropriação fraudulenta por meios eletrónicos, assédio não consensual de sistema informático, contacto com menores para fins sexuais, ataques à integridade de sistemas informáticos, interceção ilegal de dados, transferência eletrónica sem consentimento e divulgação ilegal de dados. O principal objetivo deste estudo é divulgar as técnicas utilizadas pelos cibercriminosos no Equador, socializar a pena e sugestões para evitar ser vítima desse tipo de crime. Para completar o processo, foi utilizada a metodologia Systematic Mapping Study (SMS), onde permitiu iniciar com a definição da busca, depois com a execução da busca e finalizando com a discussão e resultados. Como resultados, foram geradas respostas às questões específicas da pesquisa (IPs1, IPs2, IPs3, IPs4 e IPs5), obtendo-se sucesso na revisão sistemática. Em conclusão, sugere-se que o governo e as instituições públicas e privadas promovam treinamentos onde os riscos e tipos de crimes informáticos sejam socializados, regulamentações que regulem esses atos criminosos em relação à tecnologia e assessoria para se proteger e estar na vanguarda dos cibercriminosos.

Palavras-chave: Cibercrime, Crimes Informáticos no Equador, COIP, Prevenção de Crimes Informáticos.

1. Introducción

El avance recurrente de la tecnología ha hecho que las personas dependan de dispositivos que puedan estar conectados a la red mundial del internet (CEPAL, 2020), dado es el caso que a medida que inició la pandemia sanitaria obligatoria hubo un aumento considerable de usuarios y contenidos en las redes sociales como: Facebook, Whatsapp, Youtube, Instagram, Twitter, Snapchat y Tiktok (Prada et al., 2020). Además, We Are Social & Hootsuite (2022) líderes mundiales en especialización y gestión de redes sociales, afirman en su último informe Digital 2022 que existen 4620 millones de usuarios en redes sociales equivalentes al 58% de la población mundial representando un incremento de suscripción interanual del 10%, y, a su vez existe un aumento del 1% diario de personas que optan por contratar internet para estar conectados, estos utilizan alrededor de 7 horas diarias en redes sociales o realizando otra actividad en la red.

De este modo, las personas emprendedoras y grandes empresarios al ver tanta afluencia y contenidos en las redes sociales, han optado por iniciarse en el comercio electrónico y ofrecer productos o servicios para poder abarcar más clientes en el mercado (Tomas et al., 2022). Si bien es cierto, las redes sociales y otras aplicaciones en internet incluyendo la empresa Google y Facebook tienen servicios de pago que permiten generar marketing automatizados a manera de publicidad inmersa en sus aplicaciones (Gómez & Palacios, 2021). De hecho, es un mecanismo que ha generado mucha producción en este tipo de negocios, uno de los datos más llamativos del reporte de We Are Social & Hootsuite (2022) es que la efectividad de este tipo de publicidad en redes sociales queda demostrada frente a la creciente variedad de información durante la pandemia sanitaria obligatoria y los últimos 12 meses, teniendo que más de 1 de cada 4 usuarios entre 16 a 64 años descubren cada día nuevas marcas, productos y servicios a través de anuncios, y, más de 7 de cada 10 usuarios en edad laboral que representan el 71,5% indican que pagan por algún tipo de producto o servicio que ven en las redes sociales.

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

Al mismo tiempo, a medida que surgen nuevos avances tecnológicos existen grupos delictivos que se aprovechan de esta, y también del poco conocimiento sobre delitos informáticos que tienen los nuevos usuarios que llegan diariamente a la red; incluyendo personas de 12 a 64 años. De hecho, en el estudio sistemático de Mayer & Oliver (2020) afirman que el denominado ciberdelito surge debido a la comisión de estafas informáticas asociadas a transferencias electrónicas de fondos hace aproximadamente cuatro décadas, y, hasta la fecha el fraude informático continúa siendo centro de los cibercriminales debido al impacto económico potenciado por el auge del comercio electrónico.

Dicho en otras palabras, se denominan delitos informáticos o ciberdelitos, a los actos ilícitos que se realizan con ayuda de las Tecnologías de la Información (TI) (Díaz, 2010). También, en Acosta et al. (2020) lo definen como cualquier intención acción culposa o no culposa con intensión o sin ella, que cause daño directo mediante herramientas informáticas a personas o entidades. Concluyendo, Suárez (2020) afirma que no solo se vincula a una conducta delictiva que afecta a personas y entidades, sino también a la afectación de información y vulneración de sistemas.

En este sentido, en la investigación de Rojas & Yepes (2022) limitada a América Latina, exponen que la rapidez con que avanza la tecnología ha traído consigo diferentes tipos de problemáticas asociadas a: delitos informáticos, ciberadicciones, uso problemático del internet, monetización sexual, entre otros. De este modo, esta revisión se centra más en los delitos informáticos que se cometen constantemente y qué hacer para prevenirlos; en el país Ecuador.

Es necesario mencionar que la investigación está estructurada de la siguiente manera: en la primera sección se encuentra la metodología; el cual indica los procesos empleados para obtener y clasificar la información que se menciona en este estudio, seguidamente se tienen los resultados y discusión; donde se evidencian los resultados de la revisión sistemática y respuestas a las preguntas de investigación planteadas en la metodología, por último pero no menos importante se tienen las conclusiones.

2. Metodología

Para ubicar los temas de investigación más relevantes acorde a este estudio se empleó la metodología de Estudio de Mapeos Sistemáticos (SMS) propuesta por Carrizo & Moller (2018) el cual se basó en los modelos de (Carrizo, 2015; Petersen et al., 2008), cuyo propósito de esta revisión es proporcionar una visión general de los campos científicos, áreas de interés, enfoque y tendencias de los investigadores de ingeniería. Sin embargo, esto no es tan exhaustivo como una revisión sistemática de la literatura destinada a generar el cuerpo de conocimiento.

Por otra parte, este modelo se manifiesta en tres bloques: *a) definición de la búsqueda*; en esta parte se define la pregunta de investigación, delimitación, criterios de inclusión y exclusión de la búsqueda, *b) ejecución de la búsqueda*; aquí se van a definir los trabajos primarios referentes a este estudio, y *c) discusión y resultados*; en esta sección se analizarán los esquemas de caracterización y analizarán los resultados.

2.1. Definición de búsqueda

2.1.1. Preguntas de investigación

El auge de los delitos informáticos en la actualidad está generando mucha intriga en los investigadores, especialistas de la seguridad informática y unidades antidelictivas. Es así como surge la siguiente pregunta, ¿Qué tipos de delitos informáticos son los más usuales en Ecuador, y qué se está haciendo para prevenir y castigar este tipo de crímenes informáticos? Para responder a esta pregunta, estratégicamente se plantearon cinco preguntas de investigación específicas (PIs).

- **PIs1:** ¿Qué tipos de delitos informáticos existen a nivel general?

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

- **PIs2:** ¿Qué técnicas son las más comunes empleadas por los cibercriminales para capturar víctimas en Ecuador?
- **PIs3:** ¿Cuál es el principal riesgo a las que las personas están expuestas con los avances tecnológicos?
- **PIs4:** ¿Existen leyes que regulen los ciberdelitos en el Ecuador, de ser así; cuáles son estos artículos?
- **PIs5:** ¿De qué manera los internautas pueden estar protegidos ante este tipo de delitos?

2.1.2. Alcance de investigación

El estudio se enfatiza en realizar una búsqueda literaria a través de bases de datos científica, lo que implica una exploración automatizada de términos. Las bases de datos científicas que se emplearon para realizar la indagación fueron: Redalyc, Scielo, World Wide Science, Dialnet y RearchGate.

Las cadenas de búsqueda empleadas en estas bases de datos científicas fueron:

- (*delitos informáticos* OR *estafa electrónica* OR *acoso en la web* OR *bullying on the web* OR *cybercrime* OR *electronic fraud*)
- (*delitos informáticos* OR *estafa electrónica* OR *acoso en la web* OR *bullying on the web* OR *cybercrime* OR *electronic fraud*) AND (*Ecuado*r)
- (*delitos informáticos* OR *estafa electrónica* OR *fake new* OR *noticias falsas* OR *acoso en la web* OR *bullying on the web* OR *cybercrime* OR *electronic fraud*) AND (*Ecuador*) AND (*COIP* OR *regulación* OR *regulation* OR *ley penal* OR *penal law* OR *reglamenteo*)

Es necesario mencionar que cada cadena se adaptó a los formatos de búsqueda de cada base de datos en la que arrojaron: Redalyc = 324, Scielo = 181, World Wide Science = 105, Dialnet = 23, RearchGate = 100 documentos entre papers, artículos, libros y tesis doctorales.

2.1.3. Criterios de inclusión y exclusión

Para filtrar los estudios y poder obtener los más relevantes acorde a esta investigación, se emplearon los siguientes criterios de inclusión/exclusión:

- Se seleccionaron sólo las que tengan relación con los delitos informáticos y leyes que los regule
- Se incluyeron los lineamientos de la revisión sistemática como enfoques y metodologías
- Se incluyeron estudios en el idioma de inglés y español
- Se incluyeron investigaciones a partir del 2018
- Sólo se incluyeron estudios de nivel primario
- Se excluyeron estudios que no tenían una estructura correcta y diseño de investigación

2.1.4. Conducta de búsqueda

En la selección que se llevó a cabo para las investigaciones primarias se emplearon los siguientes criterios de revisión:

- Título; se revisaron títulos que coincidan con la problemática del estudio
- Resumen/Abstract; luego se realizó la revisión y correcta estructura del resumen donde se pueda observar la problemática, metodologías, resultado y conclusión
- Estructura y diseño: se revisó que tengan estructura correcta los estudios y un buen diseño metodológico.

2.2. Ejecución de la revisión

2.2.1. Selección de estudios primarios

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

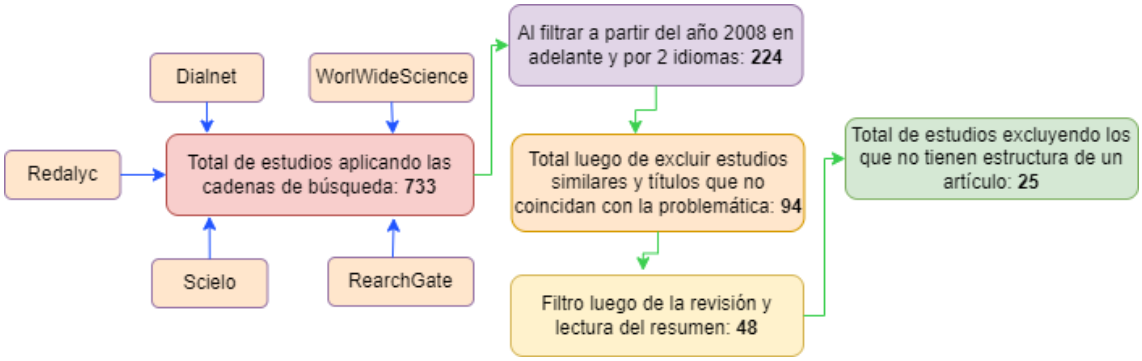
Sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

Luego de aplicar los criterios para el filtro antes mencionado, se obtuvieron un total de 25 estudios incluyendo libros, cuyos resultados se pueden observar en detalle en la figura 1.

Figura 1

Filtro de estudios relacionados



3. Resultados y Discusión

En base a la selección de estudios antes mencionados, en esta sección se presentan los resultados descritos dentro de los 25 estudios analizados, a su vez se responden cada una de las PIs formuladas en esta investigación para dar respuesta a la pregunta general.

PIs1: ¿Qué tipos de delitos informáticos existen a nivel general?

Es importante saber identificar los diferentes tipos de delitos informáticos debido a que permiten estar a la vanguardia (Acosta et al., 2020; Vinelli, 2021). Además, es necesario saber que proporcionar información de primer nivel (financiera, personal, empresarial, familiar, entre otros) a sitios y aplicaciones que pueden ser fácilmente vulnerados por personas expertas en la tecnología (piratas informáticos, crackers, hackers, entre otros) tiene un impacto alto al delito informático, puesto que las organizaciones delictivas se valen de esta información para buscar víctimas (García, 2022).

Mediante el análisis de los estudios de (Acosta et al., 2020; Díaz, 2010; Enríquez & Alvarado, 2015; Mayer & Oliver, 2020; Rojas & Yepes 2022; Vinelli, 2021) sobre delitos informáticos nacionales e internacionales, se creó una agrupación y clasificación de los tipos de delitos informáticos, como se puede observar en la figura 2.

Figura 2

Tipos de delitos informáticos

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

El orden de los delitos informáticos expuestos en la figura 2 no quiere decir que uno sea más ofensivo que el otro, es más a continuación se detallan. En primer punto hablaremos del *fraude informático*, generalmente ocurre muy a menudo y se refiere al engaño que está destinado a perjudicar el patrimonio o bien de una persona; esto se hace mediante medios electrónicos, redes sociales o llamadas telefónicas para obtener datos confidenciales y timar a la persona objetivo, también es muy conocido como *Haking* (Rojas & Yepes, 2022; Vinelli, 2021).

En segundo punto tenemos el *acoso o espionaje informático*, en varios estudios (Acosta et al., 2020; Carrión, 2021; Mayer & Oliver, 2020) se afirma que este delito se refiere a toda persona que amenaza, humilla, atormenta o molesta de alguna manera a otra; mediante el uso del internet o cualquier aparato electrónico. Además, va de la mano con la adquisición, revelación y transferencia de información virtual de tipo confidencial o comercial; sin autorización del propietario con el fin de obtener beneficios o generar pérdidas económicas. También, en Luna (2018) como se citó en Acosta et al. (2020) mencionan que estos actúan como instigador, acechador y vigilan de manera disimulada con el fin de obtener información. Asimismo, indican que existe el tipo de espionaje informático e industrial; el industrial se centra en la forma ilícita de obtener información sobre investigaciones, proyectos o desarrollos tecnológicos con la intención de obtener ventaja sobre alguna organización, y, el informático; se centra en obtener datos personales de un sujeto utilizando redes sociales o cualquier otro medio para luego poder ser usados en su contra.

Por consiguiente, *el sabotaje informático (o piratería)* consiste en la conducta dirigida intencionalmente a eliminar o modificar datos de un equipo electrónico o sistema sin autorización previa, entre estos los de mayor frecuencia son: a) gusanos, virus que se infiltran en programas del sistema (servidor) generando copias en diferentes ubicaciones y se propagan por correo electrónico, programas P2P, entre otros; b) bombas lógicas, son pequeñas líneas de código que se ejecutan cada cierto tiempo como estrategia de ataque; c) malware y virus, maliciosos con la intensión de reproducirse y dañar el sistema; d) ataques de negación de servicios, con la única intención de colapsar el sistema hasta generar la caída de los servicios (Acosta et al., 2020; Enríquez & Alvarado, 2015; Mayer & Oliver, 2020). Es necesario mencionar que este tipo de delito también tiene que ver con la piratería (crackeo) de sistemas de pago.

Seguidamente, *la pornografía infantil*; en varios estudios (Enríquez & Alvarado, 2015; Holt & Bossler, 2020; Mayer Lux & Oliver, 2020; Rojas & Yepes, 2022) se describe como cualquier representación visual de una conducta sexual explícita que involucra a un menor (personas menores a 18 años), también, las imágenes de pornografía infantil se conocen como imágenes de abuso sexual infantil, sin embargo, este término no logra describir el verdadero horror que enfrentan innumerables niños cada año a través del internet, inclusive, la producción de pornografía infantil crea un registro permanente del abuso sexual de un niño. Por ende, cuando estas imágenes se colocan en Internet y se difunden en línea, la victimización de los niños continúa a perpetuidad, también, es necesario mencionar que la pornografía infantil se difunde por el internet 24/7 (Vilks, 2019).

Luego, *la Infracción a la propiedad intelectual y derechos del autor*; según los estudios de (Acosta et al., 2020; Carrión, 2021; Luque et al., 2021; Mayer & Oliver, 2020; Vinelli, 2021) ésta se define como la violación de un derecho de propiedad intelectual, por ejemplo; la creación de una publicación o de una lista utilizando la imagen, marca comercial, logotipo, diseño, entre otros; sin permiso correspondiente del propietario de esta información. Cabe indicar que existen varios tipos de violación a la propiedad intelectual y estos son: *infracción de derechos de autor*; esta violación puede ocurrir cuando copia o carga una imagen, sin permiso, que no es suya, propia o no tiene licencia para usted. Así mismo, *la infracción y falsificación de marcas comerciales*; esta infracción ocurre cuando se realiza el uso no autorizado de una marca registrada de una manera que probablemente confunda a los consumidores en cuanto a la fuente del producto, o en cuanto a si existe algún patrocinio o afiliación entre la persona que vende el producto y la persona propietario de la marca registrada. También, *la falsificación*; los productos falsificados a menudo son réplicas

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

Sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

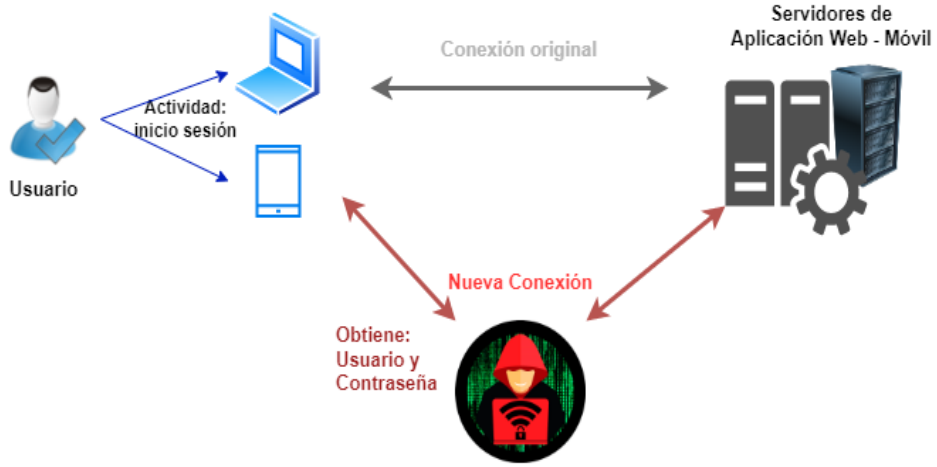
https://doi.org/10.51798/sijis.v3i2.324

falsas o no autorizadas de productos reales y están destinados a defraudar o engañar a los consumidores haciéndoles creer que el producto es auténtico. Después, *la infracción de patente*; las patentes protegen una invención contra la reproducción, el uso, la copia o la venta no autorizada, en tal motivo, hacer, usar, vender u ofrecer una invención o diseño patentado sin el permiso del propietario de la patente puede constituir una infracción de la patente. Y, *derechos de publicidad*; estos protegen los derechos de las personas contra el uso no autorizado de sus nombres, semejanzas u otros aspectos reconocibles de sus personalidades. Por esto, el uso de los derechos de publicidad de un tercero sin la debida autorización puede constituir una violación del derecho de publicidad.

Por último, pero no menos importante se tiene la *interceptación no autorizada*; este delito consiste en la interceptación ilegal de la transmisión de datos informáticos, también, es considerada como la tipificación complementaria en la relación con el acceso sin derecho (Enríquez & Alvarado, 2015; Jasso, 2020; Rojas & Yepes, 2022; Suárez, 2020). Un ejemplo claro sería la vigilancia de forma encubierta de alguna línea telefónica donde se pueden escuchar todas las conversaciones y leer mensajes de texto. Otro ejemplo relacionado con los ordenadores o teléfonos inteligentes más conocido como "*man-in-the-middle*" (hombre en medio) se muestra en la figura 3.

Figura 3

man-in-the-middle obteniendo usuario y contraseña



Nota: Se puede observar claramente que el usuario intenta acceder desde uno de sus dispositivos de preferencia hacia su aplicación ya sea Web o móvil, donde la acción normal sería una conexión directa que en la imagen está como "conexión original", sin embargo como la red está siendo interceptada por una persona no deseada; la conexión con los datos o credenciales ingresadas se envían hacia la trampa que ha colocado el *man-in-the-middle* obteniendo la información que el usuario ha enviado; luego de realizar su acción maliciosa con éxito este redirige hacia los servidores originales todas las peticiones del usuario, cabe mencionar que toda información va a ser vigilada; suele suceder a menudo cuando se conectan a redes abiertas, públicas o no confiables.

PIs2: ¿Qué técnicas son las más comunes empleadas por los cibercriminales para capturar víctimas en Ecuador?

En este contexto se puede presentar gran cantidad de tecnologías empleadas por los ciberdelincuentes y el surgimiento continuo de nuevas formas de piratear o eludir las medidas de seguridad de los sistemas; a continuación, se realiza una descripción general de los métodos más comunes usados por los ciberdelincuentes los cuales han sido expuestos en los estudios de (Acosta et al., 2020; Carrión, 2021; CEPAL, 2020; Holt & Bossler, 2020; Luque et al., 2021; Saltos et al., 2021) realizados en Ecuador; en orden de frecuencia.

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

En primer punto tenemos al *bot malicioso (Malicious bot - botnet)*, es de tipo malware[1] creado especialmente para robar información o infectar un equipo que a menudo se usa mucho, también, se distribuye mediante el sistema con el código malicioso y en ocasiones forma parte de un kit de explotación, según informes los ataques por *bot malicioso* ascendieron a un 77% en referencia a los otros tipos.

Posteriormente la suplantación *de identidad (Phishing)*, están diseñados para robar dinero; los delincuentes pueden hacer esto instalando programas maliciosos en el computador de la víctima, robando información personal del equipo o engañando a la víctima para hacer clic en algún enlace que infecta el sistema operativo con malware; esto lo puede hacer mediante mensajes por correo electrónico, mensaje de texto o redes sociales, sitios web que visiten y llamadas telefónicas.

Luego, los *Ataques basados en web (Web-based attacks)*, utilizan sistemas y servicios habilitados para la web, como navegadores y sus extensiones, sitios web que incluyen Sistema de Gestión de Contenidos (CMS) y componentes de Tecnología de la Información (TI) de servicios web y aplicaciones web. En este tipo de estafa, los piratas informáticos suelen utilizar inyección mediante *hombre en el navegador (Man-in-the-browser)* para distribuir botnet a través de phishing, descargas ocultas o puertos Server Message Block (SMB)[2]. Después, el script Java se inserta en la página de comercio electrónico o banca de su navegador. Esto permite que un atacante obtenga credenciales y robe una cuenta bancaria.

De igual manera el *Relleno de credenciales (Credential stuffing)*, los que piratean sistemas informáticos; generalmente lo hacen con la intención de asegurar las credenciales de los usuarios y luego intentan usar estas credenciales con otros sistemas mediante el uso de herramientas automatizadas. Por ende, generalmente la tasa de víctimas más alta son de usuarios que utilizan la misma contraseña para diferentes cuentas o sistemas informáticos.

Asimismo, el *Ataques DDoS (DDoS attacks)* este es de tipo rasomware cuyo principal objetivo es cifrar los datos de la víctima y luego pedir rescate para descifrarlos. Además, los ataques DDoS principalmente interfieren con la disponibilidad del servicio y rendimiento del servidor o empresa objetivo; entre estos ataques los más utilizados son: ataque de conexión TCP, ataque de fragmentación, ataque de aplicaciones y ataques volumétricos.

PIs3: ¿Cuál es el principal riesgo a las que las personas están expuestas con los avances tecnológicos?

No se podía dejar de lado este riesgo que ha batido racord en los últimos años en personas de 14 a 64 años, si bien es cierto, el uso de quipos electrónicos con conexión a internet está arraigado en la sociedad, y a su vez, no se habla mucho de los efectos de adicción en el funcionamiento psicológico, salud mental y bienestar general (Hoeg, 2022). En Rojas & Yepes (2022) afirman que la *ciberadicción* es el principal riesgo, y este se define como la acción o deseo que se convierte en un obstáculo y se antepone a los aspectos más importantes de la vida, como relaciones, trabajo, escuela, entre otros. En el mismo contexto, en las investigaciones de (Escobar & Álvarez, 2022; Hoeg, 2022; Rojas & Yepes, 2022; Román, 2017) clasifican la ciberadicción en 5 tipos: a) adicción al cibersexo, b) compulsiones netas, c) adicciones a las relaciones cibernéticas (en línea), d) búsqueda compulsiva de información, y, e) adicción a la computadora, teléfono o al juego virtual.

PIs4: ¿Existen leyes que regulen los ciberdelitos en el Ecuador, de ser así; cuáles son estos artículos?

[1] *Archivo o código, generalmente enviado a través de la red que infecta, explora, roba o realiza cualquier comportamiento que desee el atacante.*

[2] *Protocolo de software que permite a los dispositivos electrónicos y programas de una red local comunicarse por medio de hardware y transmitir datos*

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

En el reporte del Banco Interamericano de Desarrollo (2020) donde se muestra una estadística específica de cada país en referencia a la ciberseguridad que tienen, afirman que Ecuador aún no cuenta con estrategias de seguridad cibernética, sin embargo, si está mejorando con ayuda del establecimiento EcuCERT, que es el equipo de respuesta ante incidentes cibernéticos del país que depende de la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL). Además, EcuCERT es miembro de CSIRT Américas, por lo que se beneficia de la red de colaboración, estímulo, intercambio y participación en proyectos de técnicas de defensa, policiales y gubernamentales de los países, también, la Dirección de Arquitectura Tecnológica y Seguridad de la información es responsable de la coordinación de la seguridad cibernética en el país cuya principal tarea es la gestión y coordinación de los principales programas de seguridad cibernética. En el mismo contexto, en la figura 4 se puede observar la evolución del marco legal sobre los delitos informáticos en el Ecuador.

Figura 4

Evolución de marco legal y regulatorio del Ecuador 2016-2020

Nota. Esta es una referencia entre el año 2016 y 2020 sobre la evolución del marco legal de los delitos informáticos, en el que se observa claramente que en la actualidad existen muchas reformas en cuanto al marco legal y regulaciones, sin embargo, las reformas para combatir los delitos cibernéticos no han avanzado a gran escala, cabe indicar que en 2020 fue el último reporte publicado por el Banco Interamericano de Desarrollo (2020).

En referencia estos antecedentes, en varios estudios (Aparicio, 2022; Cedeño, 2022; Rojas & Yepes, 2022; Saltos et al., 2021) se exponen los artículos del marco legal que combaten estos delitos informáticos, cabe indicar que hacen referencia a la última versión del Código Integral Penal del Ecuador (COIP, 2021). Así pues, en la tabla 1 se presenta el número del artículo, título del artículo y sentencia de este.

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

Tabla 1

Artículos del COIP que sancionan los delitos informáticos

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

PIs5: ¿De qué manera los internautas pueden estar protegidos ante este tipo de delitos?

Asimismo, en el reporte del Banco Interamericano de Desarrollo (2020) se expone que el Ecuador con respecto a la socialización de los delitos, riesgos y acciones de cómo operar frente a un dispositivo electrónico o redes sociales no ha mostrado un avance desde el 2016, esto se puede observar en la figura 5.

Figura 5

Formación y capacitación sobre la seguridad en el internet

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

Nota. Banco Interamericano de Desarrollo (2020)

No obstante, por parte de las instituciones educativas y plataformas de formación gratuita socializan este tipo de peligros, pero no tienen mucha aceptación hacia el público puesto que la mayoría no revisa este tipo de plataformas. Por otra parte, las instituciones educativas si hacen llegar la información puesto que capacitan presencialmente y en sectores seleccionados, sin embargo, no generan gran impacto debido a que las pocas instituciones que realizan esta actividad no se abastecen para la gran cantidad de personas que manejan la tecnología.

Cabe considerar, que en los estudios (Cedeño, 2022; Celuch et al., 2022; CEPAL, 2020; Escobar & Álvarez, 2022; Holt & Bossler, 2020; Luque et al., 2021; Majadi et al., 2018; Moreno et al., 2019; Radoniewicz, 2022; Rojas & Yepes, 2022; Vilks, 2019) nacionales e internacionales, se exponen varios consejos que se deben adoptar para minimizar el riesgo de ser víctima; se refiere a minimizar porque gran parte de la problemática viene de la mano con el avance tecnológico y muchas veces no se está preparado para estos cambios, las estrategias se muestran en la tabla 2.

Tabla 2

Estrategias para minimizar el riesgo de ser víctima de los ciberataques

N°	Consejos
1	Tener actualizado el sistema operativo y aplicaciones de los dispositivos con los que accede regularmente al internet.
2	Usar un antivirus y cortafuegos con licencia para computadores y smartphone.
3	Enseñar a los niños el uso del internet y establecer horarios con la supervisión de un adulto de ser necesario.
4	No abra los correos electrónicos que están en spam, desecharlos inmediatamente.
5	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.
6	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.
7	Aprender a reconocer páginas seguras para no caer en los *fake page* (clones de páginas, páginas falsas).
8	Usar contraseñas seguras combinando: mayúsculas, minúsculas, números y algún caracter especial; no usar la misma contraseña para otras cuentas.
9	Abrir cuentas bancarias solo en equipos personales.
10	Crear una copia de seguridad de los archivos importantes que no quiera perder en caso de infección al equipo.
11	Denunciar páginas que cometan delitos informáticos.
12	No compartir claves personales con terceras personas.
13	No creer en ofertas o premios que ofrecen dinero en internet.
14	Descargar aplicaciones de sitios seguros (tiendas oficiales).
15	No guardar contraseñas en computadoras o navegadores públicos, evite la estafa o robo de identificación.
16	No divulgar enlaces que promuevan la pornografía, exclusión, xenofobia, autodestrucción, trata de personas o cualquier actividad al margen de la ley.
17	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).
18	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.
19	No registrar o brindar información personal en las redes sociales, páginas u otras aplicaciones.
20	Conservar los mensajes, correos electrónicos y cualquier evidencia que sea necesaria para denunciar en caso de ser víctima de la ciberdelincuencia.

Recebido: 01/03/2022
Aceito: 28/04/2022
Disponível: 30/04/2022

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

4. Conclusiones

Puesto que los delitos informáticos afectan tanto a personas, empresas públicas y privadas que hacen uso de la tecnología conjuntamente con el internet; deben implementar políticas y procedimientos de seguridad al momento de manejar los equipos interconectados, además, en las empresas se debe capacitar constantemente al personal de Tecnologías de la información u comunicación y empleados para que adopten métodos de seguridades informáticas, de esta manera se disminuye el riesgo de ser víctima.

Las personas de entre 12 y 64 años deben conocer los delitos y riesgos mencionados en la **PIs2 y PIs3** a los que se exponen por el mal uso de la tecnología, además, los consejos de protección expuestos en la tabla 2 de la **PIs5**.

Basado en toda la información expuesta en este estudio, la responsabilidad del mal uso de los equipos informáticos, internet, redes sociales, entre otros, recae directamente en el usuario.

Es necesario que los internautas conozcan las sanciones impuestas por el COIP del Ecuador expuestas en el **PIs4** relacionados con los delitos informáticos; de esta manera pueden saber cuándo han sido víctima o están violando algún artículo, además, el gobierno debe promover capacitaciones por cualquier medio sobre el buen uso de la tecnología y socialización de los delitos informáticos.

Referencias

Acosta, M., Benavides, M., & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia*, *89*(89). https://doi.org/10.37960/revista.v25i89.31534

Aparicio Izurieta, V. V. (2022). *Delitos informáticos en Ecuador según el COIP*. *3*. https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/284/162

Banco Interamericano de Desarrollo. (2020). Ciberseguridad, Riesgos, Avances y el camino a seguir en America Latina y El Caribe. *Bid- Oea*, *1*, 116–119. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Carrión Valdez, G. C. (2021). *Ciberacoso en niños , niñas y adolescentes* [Universidad Católica de Santiago de Guayaquil]. http://repositorio.ucsg.edu.ec/bitstream/3317/16548/1/T-UCSG-PRE-JUR-DER-726.pdf

Carrizo, D., & Moller, C. (2018). Estructuras metodológicas de revisiones sistemáticas de literatura en Ingeniería de Software: un estudio de mapeo sistemático. *Ingeniare. Revista Chilena de Ingeniería*, *26*, 45–54. https://doi.org/10.4067/s0718-33052018000500045

Carrizo Moreno, D. (2015). Atributos contextuales influyentes en el proceso de educción de requisitos: una exhaustiva revisión de literatura. *Revista Chilena de Ingeniería. Scielo*, *23*, 208–2018. https://doi.org/DOI 10.4067/S0718-33052015000200006

Cedeño Villacís, 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

Celuch, M., Savela, N., Oksa, R., Latikka, R., & Oksanen, A. (2022). Individual factors predicting reactions to online harassment among Finnish professionals. *Computers in Human Behavior*, *127*, 107022. https://doi.org/10.1016/j.chb.2021.107022

CEPAL. (2020). La ciberseguridad en tiempos del COVID-19 y el tránsito hacia una ciberinmunidad. *Cepal*, *6*. https://repositorio.cepal.org/bitstream/handle/11362/46275/S2000679_es.pdf?sequence=1&isAllowed=y

COIP. (2021). Código Orgánico Integral Penal. *Registro Oficial - Órgano Del Gobierno Del Ecuador*, 144.

Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica de Derecho de La Universidad de La Rioja (REDUR)*, *8*, 169. https://doi.org/10.18172/redur.4071

Enríquez Herrera, J. V., & Alvarado Salinas, Y. C. (2015). Los delitos informáticos y su penalización en el código orgánico integral penal ecuatoriano. *Sathiri*, *8*, 171. https://doi.org/10.32645/13906925.404

Escobar Macías, A. D., & Álvarez Galarza, M. D. (2022). Análisis de ciberataques sobre el uso de redes sociales en

sapienza International Journal of Interdisciplinary Studies
ISSN: 2675-9780

https://doi.org/10.51798/sijis.v3i2.324

relación a la protección de datos personales en Ecuador. *Dominio de Las Ciencias*, *8*(1), 10. https://dominiodelasciencias.com/ojs/index.php/es/article/view/2622/5928

García, V. (2022). *La "nueva" moda de los ciberdelincuentes: soborno y extorsión a empleados*. Revistabyte.Es. https://revistabyte.es/actualidad-it/ciberdelincuentes-soborno/

Gómez Carreño, E., & Palacios Alvarado, W. (2021). *Revisión de literatura sobre Marketing en Redes Sociales*. *4*(1), 63–68. http://www.unilibrecucuta.edu.co/ojs/index.php/ingenieria/article/view/511

Hoeg, N. (2022). *No Title*. Centro de Adicciones y Recuperación. https://www.addictioncenter.com/drugs/internet-addiction/

Holt, T. J., & Bossler, A. M. (2020). The palgrave handbook of international cybercrime and cyberdeviance. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. https://doi.org/10.1007/978-3-319-78440-3

Jasso, C. (2020). *Prevención del delito y tecnología : La instalación de cámaras de videovigilancia y alarmas como medida de protección*. https://d1wqtxts1xzle7.cloudfront.net/59159783/2019_10-prevencion-del-delito-y-tecnologia20190507-80765-1fid3gr-with-cover-page-v2.pdf?Expires=1639453213&Signature=bIsvCABg9PRst6yHPd9gd4Itnwn9GA9gQrEcmjyMpkWtaepd8f7RsLo~JbrOTI9D2R2gni~pU-3bSucRvWewoIl3F~z

Luque, H., Chirinos, H., Antonio, J., & Vílchez, M. (2021). Electronic Contracting and Computer Crimes. In Consumer Protection in Peru. In *Lex* (Vol. 19, Issue 28, pp. 197–236). https://dialnet.unirioja.es/servlet/articulo?codigo=8255000

Majadi, N., Trevathan, J., & Gray, H. (2018). A run-time algorithm for detecting shill bidding in online auctions. In *Journal of Theoretical and Applied Electronic Commerce Research* (Vol. 13, Issue 3). https://doi.org/10.4067/S0718-18762018000300103

Mayer Lux, 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

Moreno, J., Sanchez, C., Salavarrieta, J., & Vargas, L. (2019). Technological Solutions for Fraud Prevention and design of a Transactional Risk Prevention Model for the Payment Button. *Entre Ciencia y Tecnologia*, *13*(26), 36–42. https://doi.org/10.31908/19098367.1154

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008). Systematic mapping studies in software engineering. *In 12th International Conference on Evaluation and Assessment in Software Engineering*, *17*(1), 68–67.

Prada Nuñez, R., Hernandez Suarez, C. A., & Maldonado Estevez, E. A. (2020). Diagnóstico del potencial de las redes sociales como recurso didáctico en el proceso de enseñanza en época de aislamiento social. *Espacios*, *41*(42), 260–268. https://doi.org/10.48082/espacios-a20v41n42p22

Radoniewicz, F. (2022). Cybersecurity in Poland. In *International Regulations of Cybersecurity*. https://doi.org/10.1007/978-3-030-78551-2_5

Rojas Díaz, J. S., & Yepes Londoño, J. J. (2022). Panorama de riesgos por el uso de la tecnología en América Latina. *Trilogía Ciencia Tecnología Sociedad*, *14*(26), 40. https://revistas.itm.edu.co/index.php/trilogia/article/view/2020

Román, C. A. (2017). El uso del celular y su influencia en las actividades académicas y familiares de los estudiantes de primer año de bachillerato de la Unidad Educativa Sagrados Corazones de Rumipamba de la ciudad de Quito. *Universidad Andina Simón Bolívar*, 85. http://repositorio.uasb.edu.ec/bitstream/10644/6164/1/T2591-MIE-Roman-El uso.pdf

Saltos, M., Robalino, J. L., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Revista Conrado*, *17*(78), 343–351.

Social, W. A., & Hootsuite. (2022). *DIGITAL REPORT 2022: EL INFORME SOBRE LAS TENDENCIAS DIGITALES, REDES SOCIALES Y MOBILE*. Digital 2022. https://wearesocial.com/es/blog/2022/01/digital-report-2022-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/

Suárez Sáchez, 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

Tomas, D., Ribas, A., & Gonzalo, A. (2022). Tendencias y predicciones de marketing digital. In *cyberclick*.

Vilks, A. (2019). Cybercrime and sexual exploitation of children in e-environment in the context of strengthening urban and rural security. *SHS Web of Conferences*, *68*, 11. https://doi.org/10.1051/shsconf/20196801010

Vinelli Vereau, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius et Praxis*, *053*, 95–110. https://doi.org/10.26439/iusetpraxis2021.n053.4995