EL IMPACTO DEL CIBERDELITO EN LA SOCIEDAD ECUATORIANA

Jordán Uquillas, Tiffany Andrea
tjordan@est.ecotec.edu.ec

1. Resumen

El presente artículo se enfocó en el análisis de los ciberdelitos en Ecuador, destacando su creciente incidencia y los desafíos que plantean para la ciberseguridad en el país. Este estudio abarcó información del período comprendido desde 2016 hasta 2023, centrándose en las denuncias de ciberdelitos recopiladas por la Fiscalía General del Ecuador, donde se hallaron con mayor incidencia a la estafa, apropiación fraudulenta por medios electrónicos y a la violación a la intimidad. Además, se empleó una metodología de investigación descriptiva, utilizando el método documental para recopilar y analizar información de diversas fuentes, como libros, revistas científicas y datos oficiales. El análisis reveló un aumento alarmante en la incidencia de ciberdelitos en Ecuador, a consecuencia de la pandemia del COVID-19, lo que ha puesto de manifiesto vulnerabilidades en la infraestructura cibernética nacional. Se identificaron diversos desafíos en la lucha contra los ciberdelitos, como la falta de distinción conceptual entre delitos informáticos y cibercrímenes, la escasez de estadísticas confiables y la dificultad para acceder a la justicia para las víctimas. Para abordar estos desafíos, se proponen soluciones como una mejor capacitación del personal judicial en materia de ciberseguridad, la implementación de políticas públicas efectivas, la promoción de la conciencia y educación digital, y la mejora de la colaboración internacional en la lucha contra los delitos informáticos. Estas medidas son fundamentales para restaurar la confianza en el mercado digital y garantizar la seguridad en línea de los ciudadanos ecuatorianos.

Palabras claves: Ciberdelitos, delitos informáticos, incidencia, ciberseguridad, desafíos, confianza a los entornos digitales, sociedad ecuatoriana.

2. Introducción

En las últimas décadas, el rápido avance tecnológico ha hecho necesario darle un mayor protagonismo a la ciberseguridad, tanto en Ecuador como a nivel mundial. Esto ante el aumento de información privada inundando internet, ya que hasta el 2020 a nivel mundial en solo un minuto se generaron alrededor de 42 millones de mensajes en la aplicación de Whatsapp, 150 mil mensajes en Facebook y más de 500 horas de contenido en Youtube, esto sin mencionar las demás actividades realizadas en otras aplicaciones, lo que termina evidenciando una gran flujo de información (De la Fuente & Contreras Caballol, 2021).

En la actualidad, estos datos han aumentado debido a que cada año crece la cantidad de nuevos usuarios y la cantidad de información que se genera y circula en internet, por lo que en un entorno donde las personas están cada vez más interconectadas y que con tan sólo unos clics generan información, incluso sin saberlo, dado que muchas aplicaciones se ejecutan en segundo plano para recopilar información, se ha vuelto crucial darle prioridad a la protección y privacidad de los datos. (Saura García, 2022).

Aunque inicialmente los usuarios, con la aparición de la tecnología, no le daban la mayor importancia a la protección de sus datos porque simplemente usaban el internet para visualizar la información, más no para ingresar sus datos personales, siendo utilizada la web unidireccional 1.0. Esto ha cambiado de forma

radical en los últimos años con la evolución de la web 2.0 y 3.0, junto a la aparición de las redes sociales, las páginas para realizar compras electrónicas, las aplicaciones de delivery, e inclusive sistemas de pago online, donde los usuarios deben ingresar datos cada vez más sensibles como la información financiera y la personal. (Cruz Estrada & Miranda Zavala, 2023).

Con esta evolución tecnológica, aparecieron también los delitos informáticos o ciberdelitos que son todos aquellos comportamientos ilegales realizados con el uso inapropiado de la tecnología, que terminan vulnerando la privacidad de los usuarios a través del ciberespacio, estos incluyen tanto el espionaje informático, extracción o eliminación de información, robo de identidad y de fondos bancarios, y todo aquello que violente la privacidad y seguridad de los usuarios. (Acosta, Benavides, & García, 2020).

A pesar de los constantes esfuerzos para mejorar la ciberseguridad en Ecuador, el boletín de estadísticas del 2023 de la compañía de seguridad Kaspersky, reveló que en el 2022 entre los países donde los usuarios enfrentan un mayor riesgo de infección en línea, se encuentra Ecuador en el puesto 16 con 19,02% ataques a nivel mundial, demostrando que la ciudadanía ecuatoriana enfrenta mayores desafíos para protegerse contra las amenazas cibernéticas y para poder salvaguardar su privacidad en línea. (Kaspersky, 2023).

En este contexto, esta investigación se centró en descubrir cómo impactan los ciberdelitos a la confianza digital de la sociedad ecuatoriana, mediante la identificación de sus principales formas, los factores que contribuyen a su proliferación y cómo estas actividades ilícitas afectan la confianza de la sociedad ecuatoriana en los entornos digitales.

El análisis de los ciberdelitos y su impacto en la sociedad ecuatoriana tiene una gran importancia, ya que el aumento de las tecnologías en Ecuador a raíz de la pandemia, ha ido acompañado de una mayor incidencia de delitos informáticos tales como el ciber espionaje, la divulgación de información privada, el phising (suplantación de identidad), virus informáticos, manipulación y ocultamiento de datos, skiming (robo en tarjetas de crédito), entre otros, que representan una amenaza a la seguridad y bienestar de los ciudadanos. (De La Torre Lascano & Quiroz Peña, 2023).

Dado que el 79,21% de los ecuatorianos tienen acceso a internet y 15,8 millónes de ciudadanos poseen cuentas en las redes sociales (Tamayo Benavides & Delgado Montenegro, 2023), al compartir información de forma constante, se ha vuelto necesario comprender el impacto de los ciberdelitos a nivel nacional, puesto que de tener un alto impacto podría afectar negativamente a la confianza a los ecuatorianos en los entornos digitales. Además, de actuar como un limitante para el desarrollo tecnológico y la innovación (Stanciu & Tinca, 2017).

3. Desarrollo

3.1. Marco teórico

Definición y tipos de ciberdelitos

Los ciberdelitos son actividades delictivas que se realizan en el ámbito digital y que abarcan una amplia variedad de prácticas ilícitas, los cuales se llevan a cabo utilizando las tecnologías de la información y la comunicación. Por lo general, son perpetrados por individuos o grupos con conocimientos avanzados en informática y

con acceso a recursos tecnológicos, los cuales buscan obtener beneficios económicos, políticos o personales. Dada su constante amenaza para la seguridad en línea, es crucial identificar esos delitos para evitar ser víctima de ellos (Cortés Borrero & Bibiana Ruiz, 2023). A continuación, se detallan los más comunes (Acosta, Benavides, & García, 2020; Rodríguez Almirón, 2023).

- **Cibersabotaje:** Implica el intento deliberado de dañar, interrumpir o destruir sistemas informáticos, redes o infraestructuras con el fin de causar daño o pérdida de información.
- **Ciberespionaje:** Consiste en infiltrarse en sistemas informáticos o redes con el objetivo de recopilar información confidencial, como secretos comerciales, datos financieros o información gubernamental.
- **Interferencias que comprometen la red:** Es cualquier acción destinada a comprometer la integridad, disponibilidad o confidencialidad de una red, como el bloqueo de tráfico legítimo o la manipulación de datos transmitidos.
- **Muleros:** Son aquellos individuos que son reclutados por ciberdelincuentes para llevar a cabo actividades ilegales de transferencia de dinero, como parte de una operación delictiva organizada.
- **Pharming:** Los atacantes redirigen el tráfico de un sitio web legítimo a uno falso, donde intentan obtener información privada.
- **Phishing:** Consiste en enviar correos electrónicos falsificados que parecen ser de instituciones legítimas para engañar a las personas y hacer que revelen información confidencial, como contraseñas o detalles de tarjetas de crédito.
- **Ransomware:** Es un tipo de malware que cifra archivos o bloquea el acceso a sistemas informáticos y luego exige un rescate a cambio de restaurar el acceso.
- **Smishing**: Es una variante del phishing que se realiza a través de mensajes de texto (SMS) en lugar de correos electrónicos. Los atacantes intentan engañar a las personas para que revelen información personal o descarguen algún tipo de malware en sus dispositivos.
- **Venta de datos corporativos:** Involucra la comercialización ilegal de información confidencial de empresas, como listas de clientes, datos financieros o secretos comerciales.

Historia y evolución de los ciberdelitos

Los inicios de los ciberdelitos se remontan a 1940, con la concepción de las primeras redes informáticas. En aquel entonces, estos eran realizados por aficionados para demostrar su habilidad técnica en el área. Sin embargo, su definición y relevancia se consolidaron después con la aparición del internet, el cual abrió un mundo de oportunidades tanto para el desarrollo tecnológico como para un nuevo tipo de delincuencia. (Cortés Borrero & Bibiana Ruiz, 2023).

En 1970, Bob Thomas desarrolló el primer virus conocido como Creeper, el cual se propagó dentro de la red ARPANET para imprimir el mensaje “Soy creeper. Atrápame si puedes” en múltiples computadoras. Aunque este virus no realizó modificaciones dañinas, despertó la necesidad de encontrar una solución a este problema. Fue entonces cuando Ray Tomlinson desarrolló el primer antivirus llamado Reaper, el cual se encargaba de encontrar y eliminar los Creepers. (Catalin Bugoi & Esquinas Puche, 2023).

En 1987, los virus comenzaron a comercializarse. Aunque los primeros virus, como los troyanos y gusanos, ya habían aparecido antes, fue en este año cuando su comercialización se intensificó. Por lo que, John McAfee decidió establecer la empresa McAfee y lanzó así el primer antivirus comercial llamado VirusScan. (Catalin Bugoi & Esquinas Puche, 2023). Este acontecimiento fue seguido por el crecimiento exponencial de los ciberataques, financiados en gran medida por grupos delictivos en las primeras décadas del siglo XXI, lo que llevó a los gobiernos a implementar medidas contra la ciberdelincuencia. (Paredes Puente de la Vega, 2021).

Conceptos fundamentales de la ciberseguridad

La ciberseguridad surge como un campo de suma importancia en esta era digital, donde la protección de datos sensibles se vuelve cada vez más esencial. Se basa en la unión de herramientas y tecnologías con el fin de proteger y defender las redes informáticas, servidores, dispositivos electrónicos, y sobre todo datos de carácter sensible ante posibles amenazas informáticas que se presenten o puedan presentarse en un futuro. A medida que avanza para contrarrestar estos actos, también lo hacen los delitos informáticos incrementando su complejidad. De esta manera, la ciberseguridad ha pasado de ser un tema secundario a convertirse en uno principal. (Candau Romero, 2021).

En este contexto, es esencial comprender los pilares sobre los cuales se sustenta la ciberseguridad. Además de la protección constante de datos y sistemas, implica también la concienciación y educación de los usuarios para prevenir ataques y minimizar riesgos. La colaboración entre sectores público y privado también juega un papel crucial en la detección temprana y la respuesta efectiva a las amenazas cibernéticas. Asimismo, el desarrollo de normativas y regulaciones adecuadas se vuelve imperativo para establecer estándares de seguridad y promover la responsabilidad en el manejo de la información sensible. Por lo tanto, esta disciplina no solo se trata de defender redes y datos, sino también de promover una cultura de seguridad integral en la sociedad digital actual. (Ministerio de Telecomunicaciones y Sociedad de la Información, 2022).

Desafíos actuales y ventajas de la ciberseguridad

Hoy en día, la ciberseguridad enfrenta desafíos complejos, como el aumento de los delitos informáticos, la escasez de profesionales especializados en el área, fallos de seguridad en entornos laborales remotos y en el sector bancario, así como el constante crecimiento de la dark web que facilita las actividades ilegales, la evolución de nuevas modalidades de ciberdelitos, la implementación de tecnologías emergentes como el metaverso y la falta de conciencia sobre los riesgos digitales a los que están expuestos los usuarios. A pesar de estos desafíos, muchas organizaciones y gobiernos continúan generando medidas para mitigar las amenazas cibernéticas. (Harán, 2022).

Si bien la ciberseguridad enfrenta crecientes retos, es innegable que también ofrece una serie de beneficios como la protección de datos, esto a nivel empresarial trae como ventaja la confianza por parte de los clientes y permite mantener una buena reputación, mejor gestión de acceso mediante medidas como verificación y autenticación de usuarios evitando así el robo de información, el cumplimiento de los requisitos legales entorno al cuidado de los datos, mayor productividad al brindar tranquilidad respecto a la seguridad, control sobre el riesgo de pérdidas monetarias y constante disponibilidad de los sistemas. (Díez Huertas, 2020).

Impacto de los ciberdelitos

Los ciberdelitos han crecido de una forma tan exponencial que su uso ha traído consecuencias negativas a varios sectores, siendo el ransomware, que consiste en una forma de extorsión y secuestro de información, una de las principales amenazas a las que se enfrenta la ciberseguridad en la actualidad. Según la plataforma alemana Statista, se prevé que el tamaño del mercado en torno a la ciberseguridad aumentará a 345,4 mil millones de dólares para el 2026, dado que su rol se ha vuelto indispensable. (Nieto Rodríguez & Sánchez Rojas, 2023).

Considerando este panorama, es crucial destacar las diversas áreas donde los ciberdelitos representan una amenaza significativa. Por ejemplo, en el sector financiero, con la vulnerabilidad de los datos bancarios; en el ámbito sanitario, con la exposición de registros médicos y expedientes privados; en los servicios públicos, con el riesgo de acceso al control de la cadena de suministros; en el gobierno, con la visualización de información confidencial de los ciudadanos; en la educación, con la divulgación de los datos personales de los estudiantes; y en los medios de comunicación, con el ataque a la distribución de contenido. (Bidaidea, 2023).

En la vida cotidiana, los riesgos antes los ciberdelitos se hacen presente de forma constante, por lo que los usuarios han adoptado diversas prácticas para protegerse, tales como tener actualizado el antivirus y sistemas operativos en todos los dispositivos electrónicos, usar contraseñas seguras, evitar descargar aplicaciones de terceros o dar clics a enlaces que se encuentran en los correos spam, así como el uso de sitios webs seguros y la utilización de redes privadas para hacer movimientos financieros o cualquier otra actividad que incluya compartir datos importantes. (Navarro Uriol, 2020).

Tendencias y amenazas emergentes de la ciberseguridad

Se observa un creciente interés en la implementación de la inteligencia artificial en la ciberseguridad, ya que la IA es capaz de analizar patrones y así detectar comportamientos extraños, de forma que permite automatizar una respuesta ante posibles ciberataques. Además, la aplicación de la ciberseguridad se está extendiendo a los centros de datos híbridos, dado que las empresas y organizaciones buscan disminuir parte de su infraestructura local y realizar una transición hacia la nube, también se está empezando a utilizar los firewalls de malla híbrida que combinan varios tipos de firewall buscando proteger tanto la información de la nube como la local. (CheckPoint, 2023).

En contraste con estas innovaciones, están presentes los riesgos relacionados al internet de las cosas y a las ciudades inteligentes, junto con los ataques a los dispositivos móviles en el que se utilizan métodos como aplicaciones maliciosas, ataques a los sistemas operativos y mensajes que buscan engañar a los usuarios para robar información. (Vásquez López, 2021).

Ética y responsabilidad en la ciberseguridad

En el ámbito corporativo, la selección de profesionales en ciberseguridad es compleja debido a las diversas intenciones que existen entre ellos. Muchos de los expertos actuales han tenido experiencias previas con el hacking durante su juventud, lo que hace necesario distinguir entre aquellos que lo hicieron de manera constructiva para aprender y aquellos con intenciones maliciosas que hicieron actividades ilícitas. Esto subraya la importancia de no solo buscar habilidades técnicas, sino también profesionales con ética y responsabilidad. (Mendoza, 2016).

Los profesionales de ciberseguridad frecuentemente se enfrentan a dilemas éticos debido a la naturaleza de su trabajo. Por ejemplo, pueden encontrarse en situaciones donde descubren algún tipo de vulnerabilidad en un sistema que podrían explotar para obtener un acceso no autorizado y obtener algún tipo de beneficio. Sin embargo, en estos casos estos profesionales deben ejercer un buen sentido de la responsabilidad y la ética, eligiendo siempre proteger la integridad y seguridad de los datos. Por lo que, al final, lo que distingue a un profesional de la ciberseguridad de un ciberdelincuente son sus principios éticos y su responsabilidad hacia la protección de la información y la privacidad de las personas. (Mendoza, 2016).

Interrelación entre la ciberseguridad y confianza digital

La evolución de la ciberseguridad refleja un constante esfuerzo por proteger los datos, lo cual resalta la estrecha relación que existe entre esta disciplina y la privacidad. Ambos estando íntimamente vinculados, ya que sin medidas de ciberseguridad sería imposible garantizar la seguridad y privacidad de los datos, lo que podría terminar socavando la confianza de los usuarios. (Giménez Pérez, 2023).

La confianza digital termina jugando un papel crucial en la adopción y uso continuo de tecnologías digitales, de forma que cuando los usuarios confían en que sus datos están seguros y protegidos, están más dispuestos a participar en transacciones en línea, compartir información personal y utilizar servicios digitales. Por lo que, la ciberseguridad no solo es una cuestión técnica, sino también un componente fundamental para fomentar la confianza y la adopción de la tecnología en la sociedad. (Fundación Innovación Bankiter, 2021).

3.2 Metodología

Para alcanzar los objetivos establecidos, se utilizó la metodología de investigación descriptiva que se centró en el estudio de los ciberdelitos en Ecuador, donde se abarcó información desde 2016 hasta 2023, teniendo como objeto de estudio a los ciudadanos ecuatorianos. Se exploraron como variables independientes a los ciberdelitos, y como variables dependientes a la sociedad ecuatoriana, con el fin de comprender el alcance y las consecuencias que causan los delitos informáticos en la confianza digital de la población ecuatoriana.

Para llevar a cabo este estudio, se empleó el método documental, el cual consistió en la recopilación y revisión de una amplia variedad de fuentes. En la investigación se consultaron recursos como libros y tesis, que proporcionaron un enfoque bibliográfico a la investigación; artículos de revistas científicas y sitios webs confiables, que aportaron un enfoque hemerográfico; e informes y actas de instituciones públicas y privadas, que ofrecieron un enfoque archivístico, lo que permitió obtener una perspectiva más completa sobre los ciberdelitos en Ecuador y su impacto en la sociedad (Casasola Rivera, 2015). A continuación, se detallan los pasos seguidos para el proceso de recolección de información.

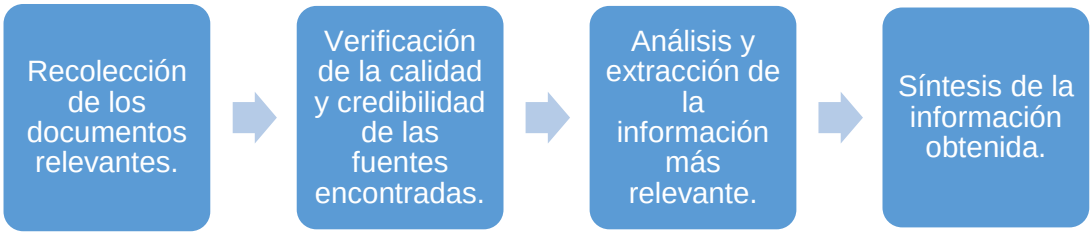

Figura 1. Proceso de recolección de información

Este proceso permitió obtener una extensa cantidad de información y datos provenientes de fuentes confiables sobre los ciberdelitos en Ecuador. Tras su recolección, se realizó un minucioso proceso de clasificación y categorización de la información recopilada, lo que enriqueció su análisis y facilitó una comprensión más profunda sobre el impacto de estos delitos en la ciudadanía ecuatoriana.

3.3. Artículos de revisión relacionados

Se realizó un análisis exhaustivo de los principales artículos científicos relacionados con esta investigación. Estos artículos fueron recopilados mediante consultas en las bases de datos científicas Scopus y ResearchGate. Utilizando los términos de búsqueda "cybercrime AND Ecuador" en Scopus, se obtuvieron 7 resultados, mientras que en ResearchGate se emplearon criterios como "(ciberdelito OR delitos informáticos) AND Ecuador", lo que arrojó 100 resultados. De esta recopilación, se seleccionaron los trabajos publicados a partir del año 2020 que hayan sido los más relevantes y estrechamente relacionados con nuestro tema de investigación. A continuación, se presenta una tabla con estos artículos.

Tabla 1

Artículos relacionados

Título	Autor	Año	Resumen
Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas.	Maldonado Fernando, Juca; Medina Peña, Rolando	2023	Esta investigación se enfocó en analizar los ciberdelitos en Ecuador y su impacto social, utilizando el análisis documental y la exegética para estudiar el marco legal relacionado. Se identificaron como las prácticas más comunes en Ecuador al robo de información, el fraude en línea, los ataques informáticos, la sextorsión y el ciberacoso, así como las estrategias utilizadas por los delincuentes. Se concluye que es necesario concientizar sobre la seguridad digital, fortalecer las respuestas del gobierno, promover la investigación, el desarrollo de tecnologías y las colaboraciones internacionales.
Ciberdelitos y su asociación en el cometimiento de fraudes financieros en la pandemia del Covid-19	De La Torre Lascano, Carlos; Quiroz Peña, Jaime	2023	Durante la pandemia del COVID-19, el cibercrimen y el fraude financiero experimentaron un aumento debido a la rápida adopción de las nuevas tecnologías, lo cual afectó a numerosas organizaciones. Este estudio se centró en una evaluación de la percepción de estas amenazas en las organizaciones, utilizando un enfoque descriptivo y cuantitativo. Los resultados revelaron que la manipulación de datos económicos y las estafas fueron los ciberdelitos más frecuentes, y como medidas preventivas, se implementaron auditorías y controles internos.
Delitos informáticos en Ecuador según el COIP: un análisis documental	Aparicio Izurieta, Viviana	2022	Este artículo se centró en realizar un análisis documental de los delitos informáticos más frecuentes en Ecuador y las sanciones establecidas en el COIP. Se incluyó una descripción teórica de cada delito y sus penalizaciones, así como los fines más comunes y los mecanismos tecnológicos utilizados. También se investigaron los métodos tiene el estado nacional para asegurar la seguridad y

			confidencialidad de la información, además de analizar la existencia de organismos especializados o leyes que protejan a los sistemas informáticos y a los ciudadanos afectados.
Implicaciones para las ciencias sociales del análisis de estafas y pederastia en línea en Ecuador	Pérez Martínez, Armenio; Rodríguez Fernández, Aimara	2023	Este trabajo se enfocó en analizar las implicaciones para las ciencias sociales que presentan los delitos en línea, tales como la estafa y la pederastia, en Ecuador. La metodología utilizada se basó en revisiones sistematizadas, donde se emplearon diversas bases de datos. Las conclusiones señalaron la necesidad de incrementar las investigaciones sobre estos delitos desde las ciencias sociales, así como fomentar políticas públicas y el estudio de la interdisciplinariedad con otras ciencias del comportamiento.
Preparación policial para responder al delito informático en Ecuador	Tamayo Benavides, Santiago; Delgado Montenegro, Mauricio	2023	Este estudio pretende explorar la preparación del personal policial ecuatoriano frente al delito informático, para lo cual se aplicó una encuesta para analizar la frecuencia de participación en capacitaciones, el nivel de confianza individual y organizacional para afrontarlos, y la percepción sobre cómo mejorar su respuesta. Además, se revisó la complejidad de las investigaciones de delitos informáticos y la preparación policial para abordar estos casos. En la conclusión, se sugiere que los policías ecuatorianos pueden beneficiarse de una mayor capacitación en habilidades básicas relacionadas con el delito informático.
Sobreexposición de adolescentes a ciberdelitos en el Ecuador	Quezada Sarmiento, Pablo; Suárez Tinoco, Edwin; Coloma Cuenca, André; Ruiz Salazar, Ramiro; Pinos Chamorro, Byron; Espinoza Lara, Edison; Arrobo Ordoñez, Christian; Martínez Campaña, Christian	2022	El trabajo propuesto se centró en analizar las causas y efectos de la sobreexposición de los adolescentes ecuatorianos a los ciberdelitos, destacando la falta de prevención y de atención previa de esta situación en otras investigaciones. Además, se identificó que la vulnerabilidad de los adolescentes ante estos riesgos en línea se debe en gran medida a la falta de control y supervisión por parte de sus padres y/o tutores, a quienes el desconocimiento tecnológico no los exime de su responsabilidad de cuidado, sino que implica un mayor esfuerzo por actualizarse y protegerlos.

A partir de la revisión bibliográfica realizada, se ha podido constatar que hay una tendencia por parte de los autores en el análisis de los ciberdelitos dirigido tanto al ámbito social como al legal y policial, donde los métodos de investigación que más se repiten son el documental y las revisiones sistematizadas, lo cual refleja la necesidad de recopilar la información y difundirla. Aunque no hay problemas en común puesto que cada uno analiza esta problemática en distintos escenarios, esta divergencia refleja una preocupación multifacética por entender y enfrentar los desafíos asociados a los delitos informáticos desde distintas perspectivas. En estas investigaciones, se propusieron soluciones que involucran la participación de varios actores, como padres para proteger a sus hijos ante los delitos informáticos,

empresas para salvaguardar su información y gobiernos para implementar leyes y capacitaciones que aborden eficazmente este problema creciente.

3.4. Diagrama de proceso

En nuestra investigación sobre los ciberdelitos en Ecuador, se desarrolló un diagrama de proceso que permitió visualizar de forma clara las diferentes etapas a seguir, lo que facilitó mantener un camino claro considerando los objetivos de investigación. A continuación, se detalla el diagrama de proceso.

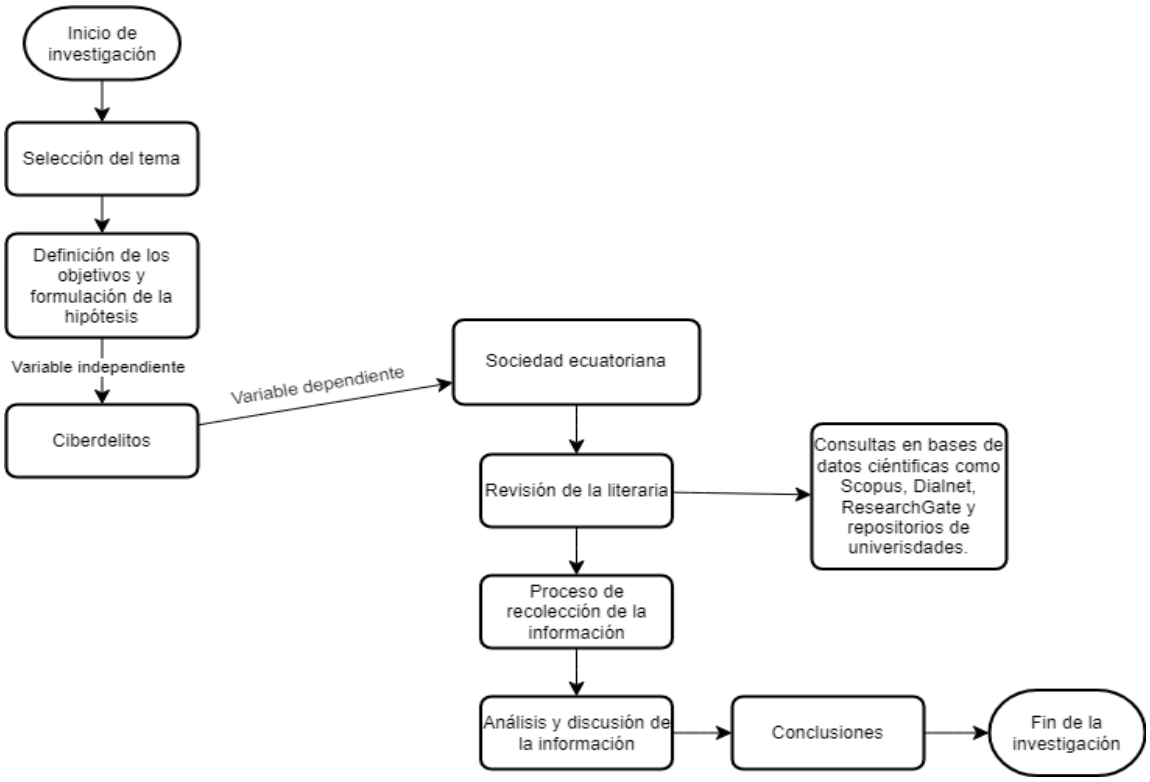

Figura 2. Proceso de investigación

4. Análisis y discusión

Para adentrarnos en el tema de los ciberdelitos, es esencial comprender el panorama actual de esta problemática. En Latinoamérica, según la empresa Kaspersky, tan solo entre el 2022 y 2023 se registraron más de dos millones de ataques cibernéticos, siendo Brasil, México y Ecuador los países más afectados. (Cañizares, 2023). Además, en este estudio, se reveló un aumento de ataques a dispositivos móviles, donde se destacan varias amenazas como adwares, spyloans, troyanos bancarios y aplicaciones legítimas utilizadas con fines poco éticos, que representan riesgos significativos para la seguridad de los usuarios en la región. (Kaspersky, 2023).

Los adware, que constituyen más del 70% de las amenazas detectadas, muestran publicidad intrusiva y recopilan datos de los usuarios. En cambio, el spyloan ofrece préstamos y bloquea el dispositivo si no se realiza el pago correspondiente o si se retrasa. Asimismo, los troyanos bancarios, especialmente los originarios de Brasil como Banbra, Brats y Basbanke, representan cerca del 60% de los intentos de infección en dispositivos móviles en América Latina, están diseñados para robar datos financieros como credenciales bancarias y números de tarjetas. Por

otro lado, Cerberus, que es una aplicación legal que se utiliza para el espionaje, ha sido identificada como una amenaza especialmente en casos de acoso a las mujeres. (Kaspersky, 2023).

Ciberdelitos en Ecuador

En los últimos años, en Ecuador ha surgido una creciente preocupación por la ciberseguridad debido al aumento de los ataques cibernéticos. Por lo que, resulta fundamental identificar los ciberdelitos más frecuentes en el país. A continuación, se detallarán las amenazas cibernéticas más comunes detectadas en Ecuador, según la Fiscalía General hasta el 2020. (Departamento de Seguridad de las TIC, 2020).

Figura 3. Los ciberdelitos más cometidos en Ecuador hasta el 2020.

De igual forma, con el objetivo de obtener un panorama más amplio sobre la frecuencia y evolución de los ciberdelitos en Ecuador, se han elaborado dos tablas que recopilan las denuncias realizadas entre el 2016 hasta el 2023, utilizando datos proporcionados por la Fiscalía General del Ecuador. A continuación, se presentan las tablas correspondientes.

Tabla 2

Delitos informáticos consumados

Delitos	2016	2017	2018	2019	2020	2021	2022	2023
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	145	217	234	238	287	414	351	486
Apropiación fraudulenta por medios electrónicos	1042	951	1423	1705	2233	5177	3113	3425

Aprovechamiento ilícito de servicios públicos	184	101	125	189	97	103	210	102
Ataque a la integridad de sistemas informáticos	76	85	87	108	92	125	199	175
Comercialización ilícita de terminales móviles	1	24	14	6	285	14	1	33
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	102	158	195	165	151	214	179	174
Delitos contra la información pública reservada legalmente	3	13	12	5	5	8	5	5
Estafa	15.028	13.906	14.187	16.559	17.675	23.386	22.329	24.016
Infraestructura ilícita	4	-	5	7	-	1	-	-
Intercambio, comercialización o compra de información de equipos terminales móviles	-	-	-	-	1	2	1	1
Interceptación ilegal de datos	78	61	42	82	71	66	76	61
Reemplazo de identificación de terminales móviles	5	4	2	-	3	-	-	1
Revelación ilegal de base de datos	24	21	46	29	29	27	62	29
Supresión, alteración o suposición de la identidad y estado civil	96	52	82	55	23	27	26	15
Transferencia electrónica de activo patrimonial	47	54	36	46	76	211	115	162
Violación a la intimidad	1.497	1.648	2.050	2.014	1.978	1.858	1.707	1.677
Total	**18.332**	**17.295**	**18.540**	**21.208**	**23.006**	**31.633**	**28.374**	**30.362**

Nota. (Sistema Integrado de Actuaciones Fiscales, 2024).

Tabla 3

Delitos informáticos tentativos

Delitos	2016	2017	2018	2019	2020	2021	2022	2023
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	2	2	2	3	5	4	2	2
Apropiación fraudulenta por medios electrónicos	10	8	27	36	47	57	25	23
Aprovechamiento ilícito de servicios públicos	2	-	2	2	1	-	-	-
Ataque a la integridad de sistemas informáticos	-	2	1	1	-	-	1	1

Comercialización ilícita de terminales móviles	-	-	-	1	-	-	-	-
Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	6	3	4	3	4	2	4	-
Delitos contra la información pública reservada legalmente	-	1	-	-	-	-	-	-
Estafa	179	161	121	335	592	526	384	305
Infraestructura ilícita	-	-	-	-	-	-	-	-
Intercambio, comercialización o compra de información de equipos terminales móviles	-	-	-	-	-	-	-	-
Interceptación ilegal de datos	4	1	1	4		1	3	
Reemplazo de identificación de terminales móviles	-	-	-	-	-	-	-	-
Revelación ilegal de base de datos	-	1	1	2	1	-	1	-
Supresión, alteración o suposición de la identidad y estado civil	-	1	-	-	1	-	1	-
Transferencia electrónica de activo patrimonial	1	-	2	2	1	1	1	1
Violación a la intimidad	20	22	22	18	25	19	14	7
Total	**224**	**202**	**183**	**407**	**677**	**610**	**450**	**339**

Nota. (Sistema Integrado de Actuaciones Fiscales, 2024).

En las tablas presentadas, se observa que durante el 2023 tanto en los delitos consumados como los tentativos, hubo una tendencia al alza en los delitos de estafa, con un total de 24,321 denuncias, seguido por la apropiación fraudulenta por medios electrónicos, con 3,448 denuncias, y la violación a la intimidad, con 1,684 denuncias. Por otro lado, los delitos menos frecuentes incluyen el reemplazo de identificación de terminales móviles, con solo una denuncia, el intercambio, comercialización o compra de información de equipos terminales móviles, también con una sola denuncia, y los delitos contra la información pública reservada legalmente, con un total de 5 denuncias.

Dificultades para combatir el aumento de los ciberdelitos

El panorama de los ciberdelitos en Ecuador ha experimentado cambios significativos como consecuencia de la pandemia del COVID-19, la cual impulsó una rápida transformación digital que terminó revelando vulnerabilidades subestimadas en la infraestructura cibernética nacional, lo que resultó en un aumento alarmante de estos actos delictivos. A pesar de los esfuerzos actuales para abordar este problema, persisten varios desafíos que dificultan su completa mitigación. (De La Torre Lascano & Quiroz Peña, 2023).

Una de las principales dificultades en la lucha contra los ataques cibernéticos es la falta de distinción conceptual entre los delitos informáticos y los cibercrímenes por parte de los encargados del sistema de justicia penal. (Salazar Méndez, Torres Maldonado, & Rodriguez Tapia, 2021). Los delitos informáticos, también conocidos como ciberdelitos, abarcan actos que ocurren a diario que van desde el fraude en línea

y las calumnias en un perfil falso hasta la piratería informática, mientras que los crímenes cibérneticos implican acciones más serias, como el daño intencionado a personas o propiedades a través de medios digitales. (Temperini, 2018).

Otro desafío significativo es la calificación simplificada de estos delitos basada únicamente en criterios formales, lo que puede subestimar su gravedad real. Además, la falta de estadísticas confiables dificulta el desarrollo de políticas y estrategias efectivas de ciberseguridad, así como la colaboración internacional en esta lucha. (Salazar Méndez, Torres Maldonado, & Rodriguez Tapia, 2021).

Las víctimas de cibercrímenes enfrentan obstáculos para acceder a la justicia debido al estigma asociado con ser víctima de un ataque cibernético y a los desafíos para presentar pruebas digitales en un tribunal. Asimismo, la falta de normativas claras sobre los datos informáticos y la carencia de capacitación y herramientas adecuadas para la obtención y análisis de evidencia digital también dificultan la investigación y persecución efectiva de los delitos cibernéticos. (Salazar Méndez, Torres Maldonado, & Rodriguez Tapia, 2021).

Finalmente, la falta de armonización normativa entre los estados obstaculiza la investigación y persecución conjunta de los delitos cibernéticos, especialmente aquellos de alcance transnacional, ya que la divergencia de leyes y procedimientos entre diferentes países dificulta la cooperación internacional en la lucha contra el cibercrimen. (Salazar Méndez, Torres Maldonado, & Rodriguez Tapia, 2021).

Efectos de los ciberdelitos en la confianza de la sociedad ecuatoriana

Los ciberdelitos han tenido un impacto significativo en la confianza de la sociedad ecuatoriana, como lo muestran las cifras alarmantes de denuncias registradas en el primer semestre del 2023. Con 1,488 denuncias por apropiación fraudulenta por medios electrónicos en ese periodo, la seguridad en las transacciones en línea se ve comprometida. (Ramos, 2023). Asimismo, Ecuador se posiciona como el cuarto país de Latinoamérica con mayor cantidad de ciberataques, con un promedio de 84 por minuto en 2022. Esta situación ha generado preocupación en todas las generaciones, desde los centennials hasta los adultos mayores, quienes comparten inquietudes sobre la seguridad en línea. (Jumbo, 2023).

Según la encuesta realizada por la empresa multinacional Paysafe, se pudo observar que, aunque los centennials muestran una mayor aceptación de los métodos de pago en línea debido a su familiaridad con la tecnología digital, el 50 % de ellos se sienten más cómodos al utilizar métodos de pago con varios pasos de verificación de identidad para resguardar sus datos financieros, siendo así que tanto ellos como la Generación X comparten una creciente preocupación por la ciberseguridad. Por lo que, a medida que el comercio en línea continúa expandiéndose en Ecuador, es esencial que las empresas implementen medidas efectivas de ciberseguridad para proteger los datos de los usuarios y restaurar su confianza en el mercado digital. (Ramos, 2023). Además, esta encuesta indicó que un 73 % de los ecuatorianos prefieren utilizar métodos de pago que no requieran compartir sus datos financieros con los comerciantes en línea, lo que subraya la preocupación generalizada por la seguridad de la información personal. (Lundh Castro & Velasco Sánchez, 2024).

A pesar de que los reclamos por fallos en la ciberseguridad representan una fracción pequeña del total de transacciones digitales en el país, la percepción del riesgo de fraude en línea sigue siendo una preocupación. Por ello, es fundamental que todas las empresas de comercio en línea implementen medidas robustas de seguridad

para proteger los datos de los usuarios. Afortunadamente, los esfuerzos coordinados entre el gobierno, el sector privado y los ciudadanos han contribuido a reducir la incidencia de los ciberdelitos en un 27 % en el 2023 con respecto al 2022, demostrando que la colaboración puede marcar la diferencia en la lucha contra la delincuencia cibernética. (Movistar, 2024).

5. Conclusión

El análisis detallado de los ciberdelitos en Ecuador reveló un panorama marcado por un aumento significativo en la incidencia de los delitos como estafa, apropiación fraudulenta por medios electrónicos y violaciones a la intimidad, lo que resalta la necesidad urgente de abordar los desafíos que enfrenta la sociedad ecuatoriana en materia de ciberseguridad, incluyendo la falta de distinción conceptual entre delitos informáticos y cibercrímenes, la necesidad de estadísticas confiables y la implementación de medidas efectivas para proteger los datos de los usuarios. Además, se destacó en la investigación el impacto negativo de los ciberdelitos en la confianza de los ciudadanos ecuatorianos en el mercado digital, lo que subraya la importancia de fortalecer la colaboración entre el gobierno, el sector privado y los ciudadanos para combatir la delincuencia cibernética y promover un entorno en línea seguro y confiable para todos los ecuatorianos.

Referencias

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89), 351-368. Recuperado el 28 de Marzo de 2024, de https://biblat.unam.mx/hevila/Revistavenezolanadegerencia/2020/Vol.%2025/No.%2089/22.pdf

Bidaidea. (14 de Septiembre de 2023). *¿Qué sectores tienen más probabilidad de sufrir un ciberataque?* Recuperado el 20 de Marzo de 2024, de Bidaidea | Empresa de ciberseguridad e inteligencia: https://ciberseguridadbidaidea.com/sectores-vulnerables-ciberataques/#Sector_Financiero

Candau Romero, J. (2021). Ciberseguridad. Evolución y tendencias. *Boletín IEEE*(23), 460-494. Recuperado el 31 de Marzo de 2024, de https://dialnet.unirioja.es/servlet/articulo?codigo=8175398

Cañizares, E. (21 de Septiembre de 2023). *Ecuador es uno de los tres países latinoamericanos con más ciberataques*. Recuperado el 7 de Marzo de 2024, de El Universo | Diario: https://www.eluniverso.com/noticias/ecuador/ecuador-es-uno-de-los-tres-paises-latinoamericanos-con-mas-ciberataques-nota/#:~:text=Según%20el%20informe%2C%20los%20países,%2C%20Argentina%2C%20Perú%20y%20Chile.

Casasola Rivera, W. (2015). *El taller de la investigación: cómo realizar fácilmente una investigación documental.* San José, Costa Rica: Ediciones Didácticas Nexo. Recuperado el 30 de Marzo de 2024, de

https://www.researchgate.net/profile/Wilmer-Casasola-Rivera-2/publication/343945276_El_taller_de_la_investigacion_Como_realizar_facilmente_una_investigacion_documental/links/5f492c58299bf13c504a0fbb/El-taller-de-la-investigacion-Como-realizar-facilmente-u

Catalin Bugoi, R., & Esquinas Puche, P. (2023). Sitio web seguro frentte a ciberataques. (I. García Magariño, Ed.) *Universidad Complutense de Madrid*. Recuperado el 31 de Marzo de 2024, de https://docta.ucm.es/rest/api/core/bitstreams/d0496fa4-17e0-4f55-9538-636d7260600b/content

CheckPoint. (30 de Diciembre de 2023). *Las 7 principales tendencias en ciberseguridad en 2024*. Recuperado el 20 de Marzo de 2024, de CheckPoint | Líderes en ciberseguridad: https://www.checkpoint.com/es/cyber-hub/cyber-security/top-7-cyber-security-trends-in-2024/

Cortés Borrero, R., & Bibiana Ruiz, C. (15 de Julio de 2023). Los ciberdelitos y la ciberseguridad: una cuestión de género. *Revista Iberoamericana de derecho informático*(13), 73-84. Recuperado el 31 de Marzo de 2024

Cruz Estrada, I., & Miranda Zavala, A. M. (8 de Septiembre de 2023). Elementos relacionados con la satisfacción del consumidor del m-commercede la ciudad de Tijuana. *Revista de Alimentación Contemporánea y Desarrollo Regional, 33*(62). doi:https://doi.org/10.24836/es.v33i62.1336

De la Fuente, G., & Contreras Caballol, D. (Mayo de 2021). Transparencia con Sentido, fomentando la reutilización de la información pública. Aprendizajes y Desafíos. (P. U. Aballai, Ed.) *Carta Magna Digital: Sociedad de la Información y Tercera Ola de Datos Abiertos*, 61-67. Recuperado el 27 de Marzo de 2024, de https://flacsolab.cl/wp-content/uploads/2021/08/Carta-Magna-Digital.pdf

De La Torre Lascano, C. M., & Quiroz Peña, J. I. (2023). Ciberdelito y su asociación en el cometimiento de fraudes financieros en la pandemia de la COVID-19. *Revista Venezolana de Gerencia, 28*(102), 609-628. doi:https://doi.org/10.52080/rvgluz.28.102.11

Departamento de Seguridad de las TIC. (2020). *Delitos informáticos en Ecuador.* Policía Nacional del Ecuador, Dirección Nacional de Tecnologías de la Información y Comunicación. Recuperado el 9 de Abril de 2024, de https://www.policia.gob.ec/wp-content/uploads/downloads/2020/10/delitos-info-ecuador.pdf

Díez Huertas, L. (2020). Arquitectura y diseño de seguridad de aplicaciones en la nube pública. (M. J. Mendoza Flores, Ed.) *Universidad Oberta de Catalunya*. Recuperado el 31 de Marzo de 2024, de http://hdl.handle.net/10609/118427

Fundación Innovación Bankiter. (Marzo de 2021). Confianza en la era digital. *Future Trends Forum*, 3-14. Recuperado el 3 de Abril de 2024, de https://www.fundacionbankinter.org/wp-content/uploads/2021/09/Publicacion-PDF-ES-FTF_ConfianzaDigital-1.pdf

Giménez Pérez, V. (2023). Responsabilidades de un encargado de tratamiento de datos en relación a las normas relatiivas a ciberseguridad. (J. V. Oltra Gutiérrez, Ed.) *Universidad Politécnica de Valencia*. Recuperado el 31 de Marzo de 2024, de https://riunet.upv.es/handle/10251/197866

Harán, J. M. (3 de Noviembre de 2022). *10 importantes desafíos que tiene la ciberseguridad por delante*. Recuperado el 19 de Marzo de 2024, de WeLiveSecurity by ESET | Noticias de seguridad en internet: https://www.welivesecurity.com/la-es/2022/11/03/desafios-mas-importantes-ciberseguridad/

Jumbo, B. (23 de Junio de 2023). *Ecuador, cuarto país latino con intentos de ataque cibernético por minuto*. Recuperado el 9 de Abril de 2024, de El Comercio | Diario: https://www.elcomercio.com/actualidad/negocios/ecuador-cuarto-pais-latino-con-intentos-ataque-cibernetico-por-minuto.html

Kaspersky. (20 de Septiembre de 2023). *Brasil, México y Ecuador: los principales blancos de ataques a dispositivos móviles en la región* . Recuperado el 9 de Abril de 2024, de Kaspersky | Empresa de ciberseguridad: https://latam.kaspersky.com/about/press-releases/2023_brasil-mexico-y-ecuador-los-principales-blancos-de-ataques-a-dispositivos-moviles-en-la-region

Kaspersky. (2023). *Kaspersky Security Bulletin 2023.* Boletín. Recuperado el 29 de Marzo de 2024, de https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/11/28102415/KSB_statistics_2023_en.pdf

Lundh Castro, E. G., & Velasco Sánchez, H. E. (2024). Análisis del uso de las billeteras electrónicas en Guayaquil: Desafíos y oportunidades. (K. R. Vallejo León, Ed.) *Universidad Politécnica Salesiana*. Recuperado el 9 de Abril de 2024, de http://dspace.ups.edu.ec/handle/123456789/27565

Mendoza, M. Á. (20 de Septiembre de 2016). *Ética, el factor humano más importante en el ámbito de la ciberseguridad*. Recuperado el 20 de Marzo de 2024, de WeLiveSecurity by ESET | Noticias de seguridad en internet: https://www.welivesecurity.com/la-es/2016/09/20/etica-en-ciberseguridad-factor-humano/

Ministerio de Telecomunicaciones y Sociedad de la Información. (Agosto de 2022). Estrategia de ciberseguridad del Ecuador. 7-9. Recuperado el 3 de Marzo de 2024, de https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

Movistar. (9 de Febrero de 2024). *Security Forum, de Movistar Empresas, analizó el escenario y tendencias de ciberseguridad en el país*. Recuperado el 09 de Abril de 2024, de Fundación Telefónica Movistar: https://www.telefonica.com.ec/security-forum-de-movistar-empresas-analizo-el-escenario-y-tendencias-de-ciberseguridad-en-el-pais/

Navarro Uriol, C. (2020). Estrategias de ciberseguridad: el caso de la pequeña y mediana empresa. (I. C. Escario Jover, Ed.) *Universidad de Zaragoza*.

Recuperado el 31 de Marzo de 2024, de https://zaguan.unizar.es/record/101988?ln=es

Nieto Rodríguez, C. O., & Sánchez Rojas, A. L. (12 de Mayo de 2023). Riesgos cibernéticos en el sector financiero colombiano situación actual y tendencias. *Fundación Universitaria del Área Andina*. Recuperado el 31 de Marzo de 2024, de https://digitk.areandina.edu.co/handle/areandina/5022

Paredes Puente de la Vega, M. G. (2021). Ciberterrorismo: Un nuevo desafío para el Derecho Internacional. (F. M. Novak Talavera, Ed.) *Pontificia Universidad Católica del Péru*. Recuperado el 31 de Marzo de 2024, de http://hdl.handle.net/20.500.12404/20374

Ramos, X. (25 de Julio de 2023). *73 % de los ecuatorianos prefieren utilizar un método de pago que no los obligue a compartir sus datos financieros con los comerciantes cuando compran en internet, según encuesta*. Recuperado el 9 de Marzo de 2024, de El Universo | Diario: https://www.eluniverso.com/noticias/informes/tarjetas-estafa-delitos-informaticos-ecuador-nota-2/

Rodríguez Almirón, F. (Julio de 2023). El delito de estafa informática. ¿Es posible determinar la responsabilidad civil de la entidad financiera en base al artículo 120.3 del código penal como consecuencia del phising? *Revista de Derecho Penal y Criminología, 3*(30), 273-304. doi:https://doi.org/10.5944/rdpc.JUNIO.2023.37387

Salazar Méndez, D., Torres Maldonado, M., & Rodriguez Tapia, B. (Diciembre de 2021). Ciberdelitos: Perfil Criminológico. (L. Monteros Arregui, & A. Lasso Ruiz, Edits.) *Revista Científia de Ciencias Jurídicas, Criminología y Seguridad, 30*. Recuperado el 9 de Abril de 2024, de https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Saura García, C. (Agosto de 2022). El lado oscuro de las GAFAM: monopolización de los datos y pérdidas de privacidad. *Veritas: revista de filosofía y teología*(52), 9-27. Recuperado el 28 de Marzo de 2024, de https://dialnet.unirioja.es/servlet/articulo?codigo=8958072

Sistema Integrado de Actuaciones Fiscales. (2024). *Estadísticas de denuncias del 2016-2023.* Informe estadístico, Fiscalía General del Estado | Ecuador, Dirección de Estadística y Sistemas de información. Recuperado el 9 de Abril de 2024

Stanciu, V., & Tinca, A. (2017). Explorando el cibercrimen - Realidades y desafíos. *Revista de Sistemas de Información de Gestión y Contabilidad, 16*(4), 610-623. doi:http://dx.doi.org/10.24818/jamis.2017.04009

Tamayo Benavides, S. M., & Delgado Montenegro, M. G. (2023). Preparación policial para responder al delito informático. *PODIUM*(44), 17-36. doi:https://doi.org/10.31095/podium.2023.44.2

Temperini, M. (2018). Delitos informáticos y cibercrimen: Alcances, conceptos y características. *Revista de Pensamiento Penal*, 49-68. Recuperado el 07 de Abril de 2024, de https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Vásquez López, F. E. (2021). Análisis de soluciones debido a la generación de información por dispositivos inteligentes de domótica en el internet de las cosas. *Centro Universitario Tecnológico CEUTEC*. Recuperado el 31 de Marzo de 2024, de https://repositorio.unitec.edu/xmlui/handle/123456789/11704