39

Fecha de presentación: febrero, 2023
Fecha de aceptación: abril, 2023
Fecha de publicación: junio, 2023

COMPORTAMIENTO

DE LOS USUARIOS SOBRE LOS DELITOS INFORMÁTICOS EN LA CIUDAD DEL PUYO. LIMITACIONES ACTUALES EN LA LEGISLACIÓN Y NORMAS

BEHAVIOR OF USERS REGARDING COMPUTER CRIME IN THE CITY OF PUYO. CURRENT LIMITATIONS IN LAW AND STANDARDS

Miguel Eduardo Velastegui Córdova[1]
E-mail: direccionpuyo@uniandes.edu.ec
ORCID: https://orcid.org/0000-0003-1433-0839
Miguel Angel Velastegui Heredia[1]
E-mail: sp.miguelavh49@uniandes.edu.ec
ORCID: https://orcid.org/0009-0008-5681-7729
[1]Universidad Regional Autónoma de Los Andes Puyo, Ecuador.

Cita sugerida (APA, séptima edición)

Velastegui Córdova, M. E., Velastegui Heredia, M. A. (2023). Comportamiento de los usuarios sobre los delitos informáticos en la Ciudad del Puyo. Limitaciones actuales en la legislación y normas. *Universidad y Sociedad*, 15(S2), 344-353.

RESUMEN

La presente investigación tuvo como objetivo evaluar las actitudes y comportamientos de los usuarios en relación con la seguridad y confiabilidad en la realización de transacciones por medios electrónicos, así como analizar las limitaciones actuales en la legislación y normas que regulan estos delitos en el país. Para ello, se desarrollaron procesos de búsqueda de información y se aplicaron encuestas a profesionales del derecho, autoridades, estudiantes universitarios y actores del comercio local, con el objetivo de recolectar información de las variables de interés. La investigación mostró que un número preocupante de personas ha sido víctima de estafas y fraudes por medios electrónicos, evidenciando la necesidad de implementar medidas para prevenir estos delitos. Se observó un bajo nivel de conocimiento y falta de medidas de protección por parte de los encuestados. Se señaló la escasez de personal técnico y falta de leyes efectivas para regular y sancionar a los infractores informáticos en el país. Se observó la necesidad de actualizar las leyes y regulaciones, mejorar la educación y concienciación de los usuarios, implementar medidas preventivas, mejorar la capacitación en seguridad informática y abordar el creciente problema de los delitos informáticos en la ciudad del Puyo y en todo el país.

Palabras clave: Delitos informáticos; legislación; estafas; seguridad informática

ABSTRACT

The objective of this research was to evaluate the attitudes and behaviors of users in relation to security and reliability in carrying out transactions by electronic means, as well as to analyze the current limitations in the legislation and regulations that regulate these crimes in the country. For this, information search processes were developed, and surveys were applied to legal professionals, authorities, university students and local business actors, with the objective of collecting information on the variables of interest. The investigation showed that a worrying number of people have been victims of scams and fraud by electronic means, evidencing the need to implement measures to prevent these crimes. A low level of knowledge and lack of protection measures were observed on the part of the respondents. The shortage of technical personnel and the lack of effective laws to regulate and punish computer offenders in the country were pointed out. The need to update laws and regulations, improve user education and awareness, implement preventive measures, improve training in computer security, and address the growing problem of computer crime in the city of Puyo and throughout the country was noted.

Keywords: Computer crimes; legislation; scams; Informatics security

INTRODUCCIÓN

En la actualidad, el mundo digital se ha convertido en una parte integral de la vida moderna, brindando una gran cantidad de beneficios en términos de eficiencia y conectividad (Li & Takakuwa, 2016). La creciente dependencia de la tecnología también ha aumentado la cantidad de riesgos que deben enfrentar, a diario, los usuarios de la web. El procesamiento y la transmisión de información en línea han dado lugar a nuevos delitos, como las estafas cibernéticas, que pueden afectar tanto a individuos como a empresas.

De acuerdo con Saltos et al. (2021), los delitos informáticos se definen como acciones dolosas y antijurídicas que causan perjuicios a personas o entidades a través del uso de medios informáticos. Estos delitos implican el uso de dispositivos o programas informáticos con el objetivo de dañar o destruir ordenadores, medios electrónicos y redes de Internet.

Entre las características de los delitos informáticos, se pueden destacar las siguientes: en primer lugar, suelen ser acciones ocupacionales, lo que significa que son cometidos por personas que tienen conocimientos técnicos en informática. En segundo lugar, son operaciones de oportunidad, lo que significa que se aprovechan de situaciones o circunstancias específicas para cometer el delito. En tercer lugar, ofrecen posibilidades de tiempo y espacio, ya que pueden ser perpetrados desde cualquier lugar del mundo en cualquier momento del día.(Vereau, 2021)

Se conoce, además, que existen muchos casos de delitos informáticos que no son denunciados, lo que indica que la magnitud del problema puede ser mayor de lo que se piensa. Por otro lado, la comprobación de estos delitos puede ser muy compleja debido a la recurrente falta de evidencias físicas y a la complejidad técnica de los sistemas informáticos. Finalmente, estos delitos tienen una tendencia a proliferar cada vez más, lo que requiere de una respuesta efectiva por parte de las autoridades y la sociedad en general. (Santacruz & Hermoza, 2019)

En el ámbito de los delitos informáticos, se pueden distinguir dos tipos: en primer lugar, aquellos que causan un mayor impacto en las organizaciones, como por ejemplo los fraudes y sabotajes. En segundo lugar, existen delitos que resultan más difíciles de detectar, ya que suelen ser cometidos por personas que trabajan dentro de la misma empresa y que tienen conocimientos sobre las configuraciones de las plataformas tecnológicas. En muchos casos, estos delitos son cometidos en colaboración con otros empleados o terceros.(Acosta et al., 2020)

Durante la pandemia del COVID-19, debido al incremento del uso de los medios de la informática, se produjo un aumento significativo de los fraudes y estafas por medios electrónicos, lo que generó una gran preocupación en la sociedad. En tal escenario, fue necesario destacar la importancia de tomar medidas preventivas para protegerse contra los delitos informáticos, especialmente en esos tiempos de crisis. (Pérez & Zaldaña, 2020)

En general, el fraude informático se refiere a la manipulación de sistemas informáticos con el fin de obtener un beneficio económico a costa de terceros. Según Mayer & Oliver (2020), este fraude consiste en una transferencia no consentida de cualquier activo patrimonial en perjuicio de un tercero, y suele involucrar manipulaciones telemáticas como correos electrónicos, redes sociales, mensajería instantánea, páginas web, entre otros. Es importante tener en cuenta que las estafas electrónicas, también conocidas como “scams”, son una modalidad cada vez más común de fraude, que utiliza diversas estrategias ingeniosas para engañar a las personas y obtener su información personal o su dinero.

Las estafas en línea pueden tener consecuencias devastadoras, lo que hace que sea imprescindible que los usuarios y las empresas comprendan los riesgos y tomen medidas preventivas para protegerse contra estas amenazas. En este sentido, resulta fundamental que los consumidores y las empresas conozcan las estrategias utilizadas por los delincuentes cibernéticos y estén preparados para combatir estas amenazas.

De esta manera, se propone la realización del presente estudio, que tiene como objetivo evaluar las actitudes, percepciones y comportamientos de los usuarios de dispositivos móviles y computadoras en relación con la seguridad y confiabilidad en la realización de transacciones por medios electrónicos, así como su conocimiento y experiencia en relación con los delitos informáticos y la denuncia de estos ante las autoridades competentes. Además, se busca analizar las limitaciones actuales en la legislación y normas que regulan estos delitos en el país, así como las posibles soluciones para mejorar la protección de los usuarios en línea y la prevención de delitos informáticos.

Ciberespacio

La comprensión del término “ciberespacio” requiere entender la creación de entornos artificiales por medio de herramientas informáticas y la inclusión de la inteligencia artificial, lo que se deriva de la “cibernética” de Norbert Wiener en 1940. Esta disciplina estudia las analogías entre los sistemas de comunicación y control de las máquinas y los seres vivos. El ciberespacio se refiere a una

realidad virtual construida digitalmente con ordenadores y no es un espacio físico que se pueda tocar.(Llinares, 2011)

El ciberespacio está relacionado con Internet, que es un conjunto de servicios desarrollados en la red. Estos incluyen sitios web, correos electrónicos, redes sociales, entre otros, y no tienen una ubicación específica en un país, excepto la de sus servidores y usuarios. Es importante señalar que, aunque algunas personas utilizan los términos ciberespacio e Internet como sinónimos, es incorrecto hacerlo, ya que el ciberespacio es un término más amplio y jerárquico que incluye a Internet como uno de sus componentes.

El ciberespacio presenta múltiples desafíos para los gobiernos que intentan regularizarlo, ya que se trata de una realidad virtual con características propias que dificultan la persecución y el juicio de los delitos que se cometen en él. A pesar de esto, algunos activistas defienden la independencia y la autonomía del ciberespacio y se oponen a la intervención gubernamental en forma de controles y censura (Del Campo et al., 2021). Para abordar estos problemas, se ha desarrollado el concepto de "ciberética" que busca regularizar el uso y la administración de la información en el ciberespacio. Es necesario que las leyes y las normas se actualicen para regularizar ciertas actividades en el ciberespacio y hacer frente a los delitos que se cometen allí.

Por otro lado, la web ha evolucionado rápidamente y se ha convertido en una herramienta esencial en la vida cotidiana de muchas personas. Los usuarios pueden interactuar masivamente y crear grandes grupos de personas que interactúan permanentemente. Internet se ha convertido en la red más grande y demandada en todo el mundo debido a la calidad de su contenido y los múltiples servicios que ofrece. Es importante seguir monitoreando y actualizando la regulación de la web para garantizar que se sigan respetando los derechos y las libertades de los usuarios mientras se protege la seguridad y la privacidad de la información.

A medida que han incrementado los servicios en la web, también han incrementado los delitos relacionados al uso de esta tecnología y medios de comunicación. Para Ojeda-Pérez et al. (2010) el delito informático puede ser definido como una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto sino también a la afectación de la información per se cómo bien jurídico tutelado, diferente de los intereses jurídicos tradicionales.

Existen diversas formas de fraude informático que se han vuelto recurrentes en internet a lo largo del tiempo, como el "*phishing*", el "*pharming*" y "*money-mules*". Estas técnicas buscan obtener información personal de los usuarios de internet con fines fraudulentos. Según Khonji et al. (2013), el "*phishing*" es un ataque de ingeniería social que explota debilidades en los procesos de un sistema, causados por los usuarios. Esto se logra a través de correos electrónicos masivos, que imitan el contenido e imágenes oficiales, para obtener información personal o credenciales de acceso, lo que permite la vulneración de sus cuentas bancarias personales.

Por otro lado, el "*pharming*" consiste en manipular las direcciones DNS (sistema de nombres de dominio) para que las páginas web visitadas por los usuarios no sean las auténticas, sino páginas web falsas creadas para obtener datos confidenciales, principalmente relacionados con la banca en línea, y así apoderarse del dinero o activos de la víctima. La principal diferencia entre ambas técnicas radica en los medios utilizados para obtener los datos personales. Mientras que el "*phishing*" utiliza técnicas de ingeniería social, el "*pharming*" utiliza un programa maligno en el servidor de internet del usuario para reconducirlo a una página web falsa.

Marco legal

De acuerdo con Zambrano & Ordoñez (2016) dice que los países latinoamericanos no tienen un marco legal homogéneo aplicable a los delitos de esta índole, por lo que generalmente, resulta muy complicado combatirlos. En el artículo 8 del Convenio de Europa sobre Ciberdelincuencia de 2001, se establece que:

''Artículo 8.- Estafa informática. – Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a.- cualquier introducción, alteración, borrado o supresión de datos informáticos;

b.- cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona".

En la región americana, uno de los tantos países que se vieron afectados por estafas en el periodo de pandemia por Covid-19 fue Argentina. Este país registró niveles elevados de estafas por medios informáticos. En Argentina diferentes provincias han realizado una reforma en las leyes procesales dejando a un lado normas legales procesales que reglamenten el problema de la evidencia digital y la incorporación de los medios tecnológicos a efectos de dotarlos de certeza, autenticidad y valor probatorio

durante los procesos judiciales. (Gendler & Andonegui, 2021)

Dentro de la reforma al Código Orgánico Integral Penal (COIP), artículo 190 se establece: el uso de un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de ésta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años (Ecuador Asamblea Nacional, 2014). Sin embargo, con el paso del tiempo han aparecido nuevos delitos informáticos que no están tipificados dentro del Código Orgánico Integral Penal, como los ciberataques, ventas ilegales, entre muchos otros que evidencian el ingenio de los delincuentes cibernéticos.

Ecuador, para la elaboración de la Ley de Comercio Electrónico, Mensaje de datos y Firmas Electrónicas, se basó en el modelo de ley establecida por UNCITRAL (The United Nations Commission on International Trade Law), gracias a esta ley permite modificar el COIP y sancionar delitos informáticos como: La obtención y utilización no autorizada de información (Art. 58), la estafa utilizando medios electrónicos o telemáticos (Art. 63).

La lucha contra los delitos informáticos, si bien ya tiene una base legal, aun se conoce de algunas falencias para una correcta protección a la información. (Campos, 2019) declara que es deber del Estado y en especial del Ministerio Público el de promover las dinámicas sociales, jurídicas, tecnológicas, policiales, o de cualquier otra índole para hacer frente de forma eficaz al problema de la delincuencia informática.

En la sección “Delitos contra el derecho a la propiedad”, el Artículo 186 del COIP hace referencia a la Estafa: La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. (Ecuador Asamblea Nacional, 2014)

Este es uno de los delitos más comunes que se desarrolla con gran magnitud en internet, e inclusive hasta en las redes celulares, ya que, a través de engaños, inducen a las víctimas a revelar información personal o patrimonial, en este caso revelación de cuantas, de usuarios, contraseñas, cuentas bancarias o tarjetas de crédito, para perjudicarse.

METODOLOGIA

La presente investigación parte de un análisis crítico-reflexivo sobre la problemática que conlleva las “estafas cibernéticas” y su incidencia en el ámbito comercial de la ciudad del Puyo, provincia de Pastaza. Los métodos empleados en la esta investigación corresponden a la modalidad “cuali-cuantitativa”, con la utilización de técnicas e instrumentos de investigación para la recolección de datos. Se tomó en cuenta los procesos delincuenciales aparentemente aislados, para formular una concepción más amplia de este tipo de delitos informáticos en la ciudad de Puyo.

Para contextualizar el tema de la investigación, se desarrollaron procesos de búsqueda selectiva de información en libros, artículos científicos, revistas y sitios de internet; para fundamentar el objeto de estudios de la presente investigación. Para poder extraer los datos de la realidad, se aplicaron instrumentos para la recolección de datos, con el objetivo de recolectar información de las variables de la presente investigación, mediante un cuestionario en línea con 15 preguntas relacionadas a la temática, aplicadas a los distintos actores con una muestra representativa, para conocer su opinión.

En tal sentido, se buscó indagar en el uso que los encuestados hacen de los dispositivos móviles y computadoras en sus actividades cotidianas. Además, se investigó sobre el uso de estos dispositivos para comunicarse, trabajar, estudiar, hacer negocios, compartir información y entretenimiento.

Se consultó sobre el conocimiento que los encuestados tienen acerca de los delitos de estafa y fraude informático, así como su experiencia personal o en su entorno familiar en cuanto a ser víctimas de estos delitos. También se indagó sobre la presentación de denuncias ante las autoridades competentes y la percepción de los encuestados acerca de la existencia de leyes y normas actualizadas que permitan combatir estos delitos. Finalmente, se consultó sobre la opinión de los encuestados en cuanto a la necesidad de reformar las leyes para frenar estos delitos y tener mayor seguridad en las transacciones por medios electrónicos.

RESULTADOS Y DISCUSION

La recolección, procesamiento y análisis de los datos, permiten la obtención de resultados relevantes en cuanto al uso de dispositivos electrónicos y seguridad en línea. En este sentido, en cuanto al uso de dispositivos

electrónicos, se puede observar que la gran mayoría de los encuestados (el 66,7%) utilizan todo el tiempo sus dispositivos móviles o computadoras para realizar sus actividades cotidianas, lo que indica una alta dependencia de estos dispositivos. Además, se puede notar que los dispositivos móviles son utilizados principalmente para comunicarse y trabajar, así como para fines de entretenimiento.

Respecto a la percepción de confiabilidad de las ofertas de bienes, productos y servicios en línea, los resultados muestran que más de la mitad de los encuestados (el 51,5%) las considera moderadamente confiables, mientras que el 30,3% no las considera muy confiables. Sin embargo, un porcentaje significativo (el 9,1%) indica que no las considera confiables. Ver Figura 1.

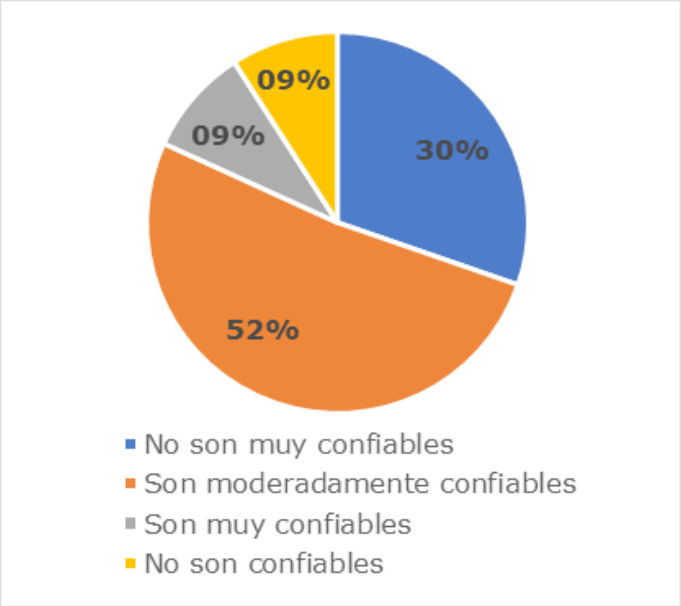

Figura 1. Nivel de confianza sobre publicidad en Internet.

Fuente: Elaboración propia

En cuanto a las compras y ventas en línea, los resultados indican que el 27,3% de los encuestados realizan compras o ventas electrónicas, mientras que el 21,2% lo hace a menudo y el mismo porcentaje lo hace rara vez. Sin embargo, un porcentaje importante (el 21,2%) nunca ha realizado compras o ventas en línea. Además, la mayoría de los encuestados (el 54,5%) indica que sí utilizan algún método de comprobación para verificar la autenticidad de las compras en línea. Ver Figura 2.

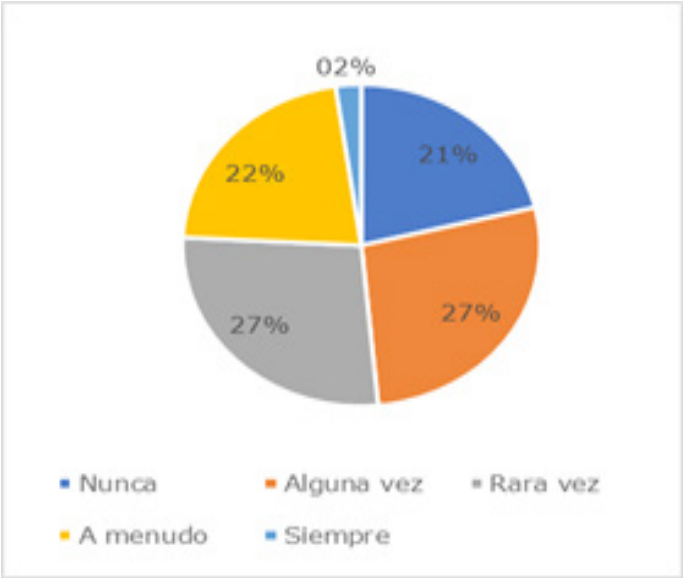

Figura 2. Frecuencia de compras o ventas realizadas por medios electrónicos.

Fuente: Elaboración propia.

En cuanto a la pregunta dirigida a los encuestados acerca de si han utilizado algún método de comprobación para verificar la autenticidad de una compra realizada por medios electrónicos, se observa que el 54,5% de los encuestados afirmó haber utilizado métodos de verificación, mientras que el 45,5% restante indicó no haber utilizado ninguno. Esta información evidencia una tendencia hacia la utilización de medidas preventivas por parte de los usuarios al momento de realizar compras en línea.

Asimismo, los métodos de verificación más utilizados por los encuestados que afirmaron haberlos utilizado incluyen la verificación del vendedor, la revisión de comentarios sobre el producto publicado, la comprobación de la seguridad del sitio, la realización de investigaciones en línea y la verificación del certificado de seguridad del sitio. Estos métodos resultan de gran utilidad para los usuarios al momento de realizar transacciones por medios electrónicos, ya que les permite asegurarse de la autenticidad y seguridad de la transacción.

Respecto a los delitos informáticos, la mayoría de los encuestados (el 81,8%) indica que tiene conocimientos sobre el tema, pero un porcentaje significativo (el 18,2%) lo desconoce. Además, el 78,8% de los encuestados ha sido víctima de algún tipo de estafa o fraude por medios electrónicos. Ver Figura 3.

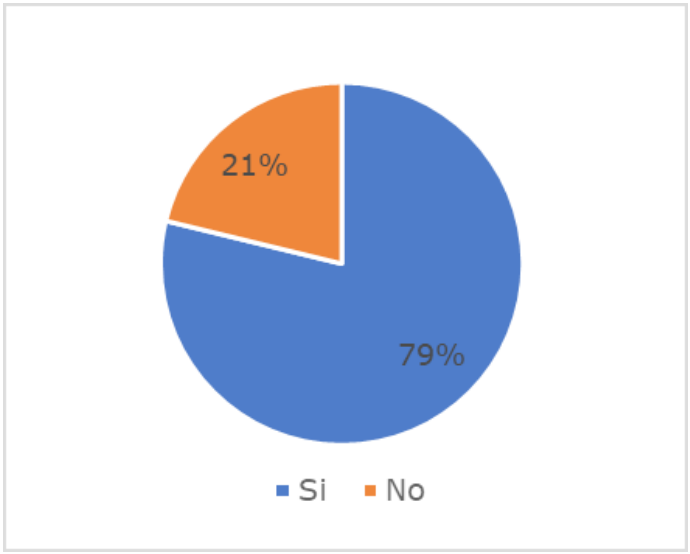

Figura 3. Víctimas de estafas o fraudes informáticos.

Fuentes: Elaboración propia.

En relación con la experiencia de los encuestados y su entorno con respecto a ser víctima de estafas o fraudes por medios electrónicos, el 78.8% de los encuestados afirmó haber sufrido este tipo de delitos, mientras que el 21.2% no reportó haber experimentado tal situación. En cuanto a los medios utilizados para perpetrar estas acciones, los encuestados afectados mencionaron, en orden de frecuencia decreciente, la publicidad en redes sociales relacionada con un determinado producto o servicio, seguido por llamadas telefónicas y mensajes de correo electrónico. También se mencionaron mensajes de WhatsApp y Messenger, así como sorteos o rifas en vivo.

Es evidente que la incidencia de los delitos informáticos en la sociedad actual es alarmante y debe abordarse desde múltiples perspectivas, incluyendo medidas preventivas y de seguridad efectivas, así como una actualización de las leyes y normativas que regulan estas prácticas en el ámbito cibernético.

En este sentido, los resultados muestran que la mayoría de los encuestados (el 72,7%) no ha presentado denuncias ante las autoridades competentes, a pesar de haber sido víctimas de delitos informáticos. Y de aquellos que sí presentaron denuncias, el 90,9% indica que no ha habido un debido proceso. Ver Figura 4.

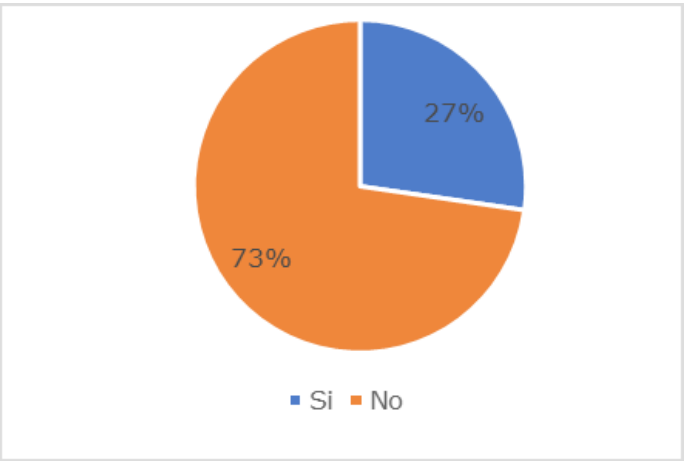

Figura 4. Debido proceso investigativo.

Fuente: Elaboración propia

En cuanto a la presentación de denuncias ante las autoridades competentes, solo el 9.1% de los encuestados informa haber tenido un debido proceso, mientras que el 90.9% afirma que no lo ha tenido. Este resultado sugiere una preocupante falta de eficacia en la respuesta de las autoridades a los delitos informáticos reportados. Además, esto puede tener un efecto desalentador en las víctimas, que pueden sentir que no tienen ninguna posibilidad de recuperar sus pérdidas o de ver que se haga justicia.

Por otro lado, en cuanto a la percepción de las leyes y normas para combatir delitos informáticos en el país, la mayoría de los encuestados (el 63,6%) considera que en el Ecuador no se cuentan con leyes y normas actualizadas para combatir estos delitos, mientras que el 15,2% indica que si y el 21,2% desconoce esta realidad. Ver Figura 5

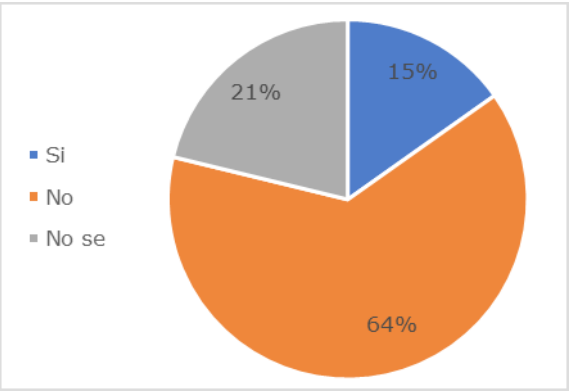

Figura 5. Percepción sobre las leyes y normas para combatir los delitos informáticos.

Fuente: Elaboración propia

En última instancia, el 93.9% de los individuos encuestados manifestaron su conformidad con la necesidad de modificar las leyes para mitigar la incidencia de delitos y reforzar la seguridad en las transacciones electrónicas, mientras que solamente un 6.1% expresó su desacuerdo. Esta estadística sugiere una alta disposición de la población hacia la implementación de cambios legales en pos de una mayor protección en el ámbito de las operaciones por medios digitales. Ver Figura 6.

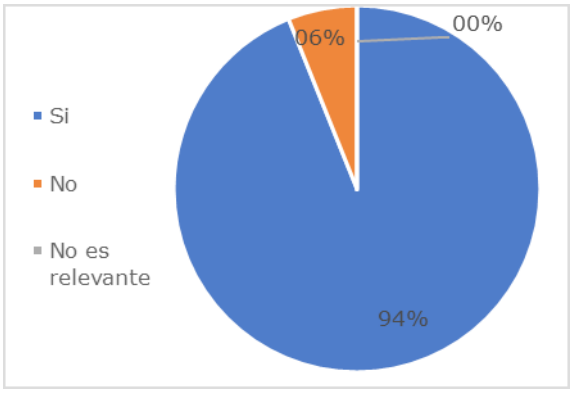

Figura 6. Reformas de leyes para frenar delitos informáticos.

Fuente: Elaboración propia

De manera general, se puede concluir que existe una alta dependencia de dispositivos electrónicos en la población encuestada, así como una gran cantidad de personas que han sido víctimas de delitos informáticos y que no han presentado denuncias. Además, se evidencia la necesidad de contar con leyes y normas actualizadas para combatir estos delitos y mejorar la seguridad en línea.

Teniendo en cuenta los resultados obtenidos, la Tabla 1 muestra un resumen de las principales estrategias que se proponen en vistas a mejorar la situación actual existente.

Tabla 1. Estrategias propuestas para ayudar a mejorar la situación existente en relación con la seguridad y confiabilidad en las transacciones electrónicas, así como a prevenir y combatir los delitos informáticos en la ciudad de Puyo.

• Fortalecimiento de la legislación y normativas: Es necesario revisar y actualizar las leyes y normativas existentes para adaptarlas a los avances tecnológicos y a las nuevas modalidades de delitos informáticos.	• Realizar una revisión exhaustiva de la legislación existente relacionada con delitos informáticos y transacciones electrónicas para identificar lagunas y áreas de mejora. • Establecer penas más severas y proporcionales para los delincuentes cibernéticos con el objetivo de disuadir y sancionar eficazmente estas actividades ilegales. • Promover la colaboración entre los legisladores, expertos en seguridad cibernética y representantes del sector privado para desarrollar enmiendas y actualizaciones en la legislación que reflejen los avances tecnológicos y las nuevas modalidades de delitos informáticos. • Establecer mecanismos ágiles y eficientes para la denuncia y persecución de los delitos informáticos, incluyendo la capacitación y asignación de recursos adecuados para las autoridades competentes.
• Mejora de la respuesta y atención a las víctimas: Es fundamental que las autoridades competentes brinden una respuesta eficiente y efectiva a las denuncias de delitos informáticos.	• Establecer unidades especializadas dentro de las fuerzas de seguridad y los organismos encargados de hacer cumplir la ley de la ciudad para investigar y perseguir los delitos informáticos. • Proporcionar capacitación continua y actualizada a los agentes encargados de atender las denuncias de delitos informáticos para mejorar sus habilidades técnicas y conocimientos legales. • Potenciar las líneas de atención telefónica y canales de comunicación en línea para que las víctimas de delitos informáticos puedan reportar los incidentes y recibir asesoramiento y apoyo adecuados. • Colaborar con organizaciones de apoyo a las víctimas para garantizar que se les proporcione asistencia emocional, legal y financiera durante todo el proceso de denuncia y recuperación.

• Colaboración público-privada: Es importante promover la colaboración entre el sector público y el sector privado, incluyendo a empresas de tecnología, instituciones financieras y proveedores de servicios en línea.	• Fomentar la colaboración entre el sector público y el sector privado a través de alianzas estratégicas y acuerdos de cooperación en la lucha contra los delitos informáticos. • Establecer foros y grupos de trabajo donde representantes del gobierno, empresas de tecnología, instituciones financieras y proveedores de servicios en línea puedan compartir información sobre amenazas y vulnerabilidades, así como desarrollar soluciones conjuntas de seguridad. • Promover el intercambio de mejores prácticas y conocimientos entre el sector público y el sector privado para fortalecer las capacidades de detección, prevención y respuesta ante los delitos informáticos. • Establecer programas de recompensas o incentivos para aquellos individuos o empresas que contribuyan significativamente a la identificación y prevención de delitos informáticos.
• Desarrollo de tecnologías de seguridad: Se debe fomentar la investigación y desarrollo de tecnologías de seguridad más avanzadas para proteger a los usuarios en línea.	• • Fomentar la investigación y el desarrollo de tecnologías de seguridad avanzadas que puedan detectar y prevenir de manera proactiva los delitos informáticos, como sistemas de detección de intrusiones, análisis de comportamiento y autenticación multifactorial. • • Promover el uso de herramientas de encriptación y autenticación robustas para proteger la integridad y confidencialidad de las transacciones electrónicas. • Establecer estándares de seguridad y certificaciones para los proveedores de servicios en línea y las plataformas de comercio electrónico, con el fin de garantizar que cumplan con los requisitos mínimos de seguridad y protección de datos.

Fuente: Elaboración propia

En este punto es importante destacar que la implementación exitosa de estas medidas requerirá de la colaboración y el compromiso de todos los actores involucrados, incluyendo a los ciudadanos, el sector privado, las organizaciones de la sociedad civil y las autoridades gubernamentales. Los ciudadanos deben tomar conciencia de los riesgos y desafíos de la seguridad en línea y adoptar medidas de protección personal, así como denunciar cualquier incidente de delito informático que experimenten o presencien. Las empresas y proveedores de servicios en línea tienen la responsabilidad de garantizar la seguridad de sus plataformas y sistemas. Por su parte, el gobierno tiene la responsabilidad de establecer y aplicar leyes y regulaciones adecuadas para combatir los delitos informáticos. Esto implica fortalecer la legislación existente, desarrollar estrategias nacionales de seguridad cibernética y asignar recursos adecuados para la investigación y persecución de los delincuentes cibernéticos.

Los resultados obtenidos confirman la alarmante expansión de los delitos informáticos, especialmente en el contexto de pandemia y postpandemia. Como han destacado diversos autores, la tecnología y su evolución constante presentan dificultades en la comprobación y verificación de estos delitos, lo que ha provocado un aumento significativo de las estafas y fraudes por medios electrónicos en todo el mundo (VASYUKOV et al., 2022).

Un ejemplo concreto de este aumento en los delitos informáticos es el caso de los ataques de phishing, que consisten en el envío de correos electrónicos fraudulentos con el objetivo de obtener información personal y financiera de los usuarios. Estos correos electrónicos falsos suelen incluir enlaces que redirigen a páginas web fraudulentas donde se solicita información personal o financiera. Según un estudio reciente, los ataques de phishing aumentaron en un 65% desde 2019, lo que demuestra la magnitud de este problema. (Alkhalil et al., 2021)

En comparación con otros estudios similares, los resultados obtenidos en esta encuesta muestran una tendencia similar en la preocupación de los usuarios por la seguridad en las transacciones electrónicas y la necesidad de reformas legales para combatir los delitos informáticos. En un estudio Cañas et al. (2021), se encontró que al menos el 32% de los encuestados había sido víctima de algún tipo de delito informático durante su vida. Estos resultados son similares a los obtenidos en la encuesta anteriormente mencionada, lo que sugiere que la preocupación por los delitos informáticos es una tendencia global y persistente.

En el caso específico de Ecuador, las estadísticas de la Fiscalía General muestran un incremento del 70% en los delitos de estafas y fraudes informáticos con respecto al año anterior, lo que indica la necesidad urgente de actualizar las leyes y regulaciones para combatir esta creciente amenaza.

En este marco, la actualización de las leyes y regulaciones es fundamental para combatir la creciente amenaza de los delitos informáticos en Ecuador. Aunque existen leyes que abordan estos delitos, no hay normas que regulen y sancionen estas conductas antijurídicas que se desarrollan en el ámbito cibernético, lo que genera un vacío legal que debe ser abordado.

Asimismo, es importante señalar que las personas que utilizan los medios electrónicos de forma permanente deben ser conscientes de la necesidad de tomar medidas de prevención y utilizar mecanismos de seguridad para evitar exponer información sensible que pueda ser utilizada por los estafadores digitales. Varios estudios señalan que la falta de conciencia y medidas de seguridad por parte de los usuarios de medios electrónicos es una de las principales causas del aumento de los delitos informáticos. (Graell, 2022)

Al uso de medios electrónicos y fomentar el uso responsable y seguro de la tecnología. Asimismo, es importante que las instituciones gubernamentales y privadas implementen medidas de seguridad adecuadas para garantizar la privacidad y seguridad de la información de sus usuarios y clientes.

CONCLUSIONES.

El presente estudio ha permitido al equipo investigador recopilar datos valiosos para determinar la incidencia de los delitos informáticos en la ciudad del Puyo, Provincia de Pastaza. La investigación se realizó en una muestra significativa de la población, que incluyó profesionales del derecho, autoridades, estudiantes universitarios y actores del comercio local. Los resultados indican que un número preocupante de personas han sido víctimas de estafas y fraudes por medios electrónicos, lo que demuestra la necesidad de implementar medidas para prevenir estos delitos. Además, se observó un bajo nivel de conocimiento por parte de los encuestados en relación con las nuevas formas de operación de los ciberdelincuentes, así como la falta de conocimiento sobre medidas de protección.

Por otro lado, la investigación también señala la escasez de personal técnico especializado para realizar investigaciones sobre delitos informáticos y la falta de leyes y normas efectivas para regular y sancionar a los infractores informáticos en el país. Los resultados de esta investigación muestran la necesidad de una actualización de las leyes y regulaciones para combatir la proliferación de los delitos informáticos en Ecuador, así como la importancia de la educación y concienciación de los usuarios de medios electrónicos para prevenir y combatir estos delitos. Se recomienda mejorar la capacitación y formación en materia de seguridad informática, así como la implementación de medidas preventivas y la actualización de las normativas y leyes para abordar el creciente problema de los delitos informáticos en la ciudad del Puyo y en todo el país.

REFERENCIAS BIBLIOGRAFICAS:

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. https://biblat.unam.mx/es/revista/revista-venezolana-de-gerencia/articulo/delitos-informaticos-impunidad-organizacional-y-su-complejidad-en-el-mundo-de-los-negocios

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060. https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full

Campos, N. J. O. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. ***Revista Científica Hallazgos21, 4***(1), 100–111. https://dialnet.unirioja.es/servlet/articulo?codigo=7148227

Cañas Quiroga, M. C., Cuellar Sosa, A. L., & Marín Aguirre, A. P. (2021). Delitos informáticos que afectan los consumidores financieros del Banco Davivienda. Fundación Universitaria Los Libertadores. https://repository.libertadores.edu.co/bitstream/handle/11371/4905/Cañas_Cuellar_Marin_2021.pdf?sequence=1&isAllowed=y

Del Campo, E. A. P., Alvis, S. P., Acevedo, M. E. S., & Aguirre, C. M. (2021). Estado y soberanía en el ciberespacio. ***Via Inveniendi Et Iudicandi,16***(1), 1–46. https://www.redalyc.org/journal/5602/560268690006/560268690006.pdf

Ecuador Asamblea Nacional. (2014). Código Orgánico Integral Penal, COIP. In Registro Oficial No. 180 de 10-feb.2014. https://tbinternet.ohchr.org/Treaties/CEDAW/Shared Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf

Gendler, M. A., & Andonegui, F. (2021). El COVID-19 y las regulaciones digitales en Argentina. Controversias y Concurrencias Latinoamericanas, 12(22), 175–2020.

Graell, R. D. G. (2022). Prevención de delitos informáticos en los sistemas virtuales educativos en Panamá. ***Revista Saberes APUDEP, 5***(1), 518–534. https://revistas.up.ac.pa/index.php/saberes_apudep/article/view/2652

Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: a literature survey. IEEE *Communications Surveys & Tutorials, 15*(4), 2091–2121. https://ieeexplore.ieee.org/abstract/document/6497928/

Li, T. L., & Takakuwa, R. (2016). Análisis de confiabilidad y validez de un instrumento de medición de la sociedad del conocimiento y su dependencia en las tecnologías de la información y comunicación. *Revista de Iniciación Científica, 2*(2), 64–75. https://revistas.utp.ac.pa/index.php/ric/article/view/1249

Llinares, F. M. (2011). La oportunidad criminal en el ciberespacio. Revista Electrónica de Ciencia Penal y Criminología, 7, 1–7. https://www.academia.edu/download/59907219/la_oprtunidad_crimial_en_el_ciberespacion_LLINARES20190701-9258-1sx7oe7.pdf

Mayer Lux, L., & Oliver Calderón, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología, 9*(1), 151–184. https://www.scielo.cl/scielo.php?pid=S0719-25842020000100151&script=sci_arttext

Ojeda-Pérez, J. E., Rincón-Rodríguez, F., Arias-Flórez, M. E., & Daza-Martínez, L. A. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de Contabilidad, 11(28), 41–66. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

Pérez, F. V. N., & Zaldaña, B. C. (2020). Ciberdelincuencia en tiempos de covid-19:¿ La vulneración a derechos constitucionales? Lumen, 16(1), 93–100. https://revistas.unife.edu.pe/index.php/lumen/article/view/2287

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (2021). Análisis conceptual del delito informático en Ecuador. Conrado, 17(78), 343–351. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343

Santacruz, H. B., & Hermoza, M. M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. *Revista Ibérica de Sistemas e Tecnologias de Informação, E20*, 391–400. https://search.proquest.com/openview/fc081b269b3464d67367cafb7a4b1d66/1?pq-origsite=gscholar&cbl=1006393

VASYUKOV, V. F., BOCHAROV, A. V., KASHINA, E., & SINGILEVICH, D. A. (2022). CYBERSTALKING AS A TYPE OF CYBERCRIME: COUNTERACTION OPPORTUNITIES IN RUSSIAN AND INTERNATIONAL LEGISLATION. Relações Internacionais No Mundo, 2(35). https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=15189368&AN=157579375&h=okgQLSuk6a97Vv8OlVvagxN6P0lp8G9jcJQ%2Foa7eL%2FpDZRLitxzmEQ8rkRsH1Z9Ha6RUe%2FOktT2TyKryRy311w%3D%3D&crl=c

Vereau, R. V. (2021). Los delitos informáticos y su relación con la criminalidad económica. Ius Et Praxis, 053, 95–110. https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995

Zambrano, K. I. D., & Ordoñez, L. M. M. (2016). Delito Informático. Procedimiento Penal en Ecuador. Dominio de Las Ciencias, 2(2), 204–215. https://dialnet.unirioja.es/servlet/articulo?codigo=5761561