Cybercrimes and Cyberattacks: Legal Analysis in the Criminal Law of Ecuador

Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador

Autores:

Sarmiento-Chamba, Jose Andres
UNIVERSIDAD INTERNACIONAL DEL ECUADOR-UIDE
Egresado de la carrera de Derecho
Loja – Ecuador
josarmientoch@uide.edu.ec

https://orcid.org/0009-0009-6691-9400

Abg. Maldonado-Ruiz, Luis Mauricio Mg
UNIVERSIDAD INTERNACIONAL DEL ECUADOR-UIDE
Docente-Investigador
Loja – Ecuador
lumaldonadoru@uide.edu.ec

https://orcid.org/0000-0002-0956-7869

Fechas de recepción: 26-JUN-2024 aceptación: 26-JUL-2024 publicación:15-SEP-2024

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

El presente artículo científico aborda la creciente problemática de los delitos informáticos en Ecuador, analizando su impacto económico, psicológico y social. A través de un exhaustivo estudio de la legislación vigente, se evidencia la falta de conocimiento sobre la ilegalidad de ciertas acciones, como la violación de la intimidad y el reemplazo de identificaciones móviles, lo que ha llevado a consecuencias extremas, incluyendo suicidios. Se argumenta que el Código Orgánico Integral Penal (COIP) requiere reformas urgentes, ya que las penas actuales son desproporcionadas y carecen de sanciones económicas adecuadas. El artículo también destaca la necesidad de adherirse al Convenio de Budapest, que facilitaría la cooperación internacional en la lucha contra estos delitos. Se subraya la importancia de que tanto instituciones públicas como privadas actualicen sus sistemas de seguridad tecnológica, especialmente ante el avance de la inteligencia artificial, para proteger la información personal de los ciudadanos. Además, se discuten casos específicos de delitos informáticos, como el acceso no consentido a sistemas informáticos y la distribución de software malicioso, ilustrando cómo estas acciones afectan la privacidad y seguridad de las personas. En conclusión, el artículo llama a una mayor educación y concienciación sobre los delitos informáticos, así como a la implementación de medidas más efectivas para prevenir y sancionar estas conductas, asegurando así la protección de los derechos digitales en la sociedad ecuatoriana.

Palabras clave: Ciberseguridad; Privacidad; Suicidio; Robo, Extorsion

Abstract

The present scientific article addresses the growing issue of cybercrimes in Ecuador, analyzing their economic, psychological, and social impact. Through a comprehensive study of current legislation, the lack of awareness regarding the illegality of certain actions, such as invasion of privacy and mobile identification replacement, is highlighted. This has led to extreme consequences, including suicides. It is argued that the Comprehensive Organic Penal Code (COIP) requires urgent reforms, as current penalties are disproportionate and lack adequate economic sanctions. The article also emphasizes the need to adhere to the Budapest Convention, which would facilitate international cooperation in combating these crimes. The importance of both public and private institutions updating their technological security systems is underscored, especially in light of advancements in artificial intelligence, to protect citizens' personal information. Additionally, specific cases of cybercrimes, such as unauthorized access to computer systems and the distribution of malicious software, are discussed, illustrating how these actions affect individuals' privacy and security. In conclusion, the article calls for greater education and awareness about cybercrimes, as well as the implementation of more effective measures to prevent and punish these behaviors, thus ensuring the protection of digital rights in Ecuadorian society.

Keywords: Cybersecurity; Privacy; Suicide; Theft; Extortion

Introducción

La tecnología año tras año ha ido evolucionando de una manera veloz y poco a poco se ha ido introduciendo mucho más en la vida cotidiana de las personas, como por ejemplo, para el trabajo, educación, salud, entretenimiento, comunicación y un sin número de actividades, esto ha facilitado mucho la vida del ser humano, porque ayuda a realizar las actividades de manera rápida y eficaz, pero también existen personas que dan mal uso a la tecnología y la ocupan para realizar cosas ilegales como por ejemplo: hackear dispositivos móviles, portátiles, cuentas bancarias, etc. Esto es un problema que ha venido acarreando durante los últimos años, donde personas se han visto afectas de manera económica, psicológica e incluso hasta física.

El Ecuador, al igual que otros países, no está libre de los ataques cibernéticos. Cuando a las personas les hablan de un ataque cibernético o hackeo de cuentas, la primera impresión o idea que se tiene acerca de ciberataques es que proviene de banda delictivas u organizaciones mundiales de hackers. Si bien es cierto es correcto que los ciberataques provienen de aquellas organizaciones o bandas, en realidad muchas personas hacen ciberataques desde su casa con un ordenador de PC o incluso desde un celular sin pertenecer a bandas delictivas. En varios casos, tienden a hackear celulares u redes sociales para poder sacar información de personas, fotos de índole sexual, dinero a través de banca móviles de móviles; y eso tiene un fin, el cual es hacer chantajes o extorsión para así poder aprovecharse de las personas y sacar dinero o beneficios que requiera el autor de delito.

El objetivo de este artículo es hacer una investigación profunda que sea normativa y doctrinaria para saber si en verdad los ecuatorianos están protegidos por los delitos informáticos que hay en la actualidad. Para esto, empezaremos explicando que son delitos informáticos, ciberataques, se hará un análisis profundo del Código Orgánico Integral Penal (COIP), se analizará noticias acerca del tema y se hará una evaluación a cerca del marco jurídico actual del Ecuador para saber si en verdad los ordenamientos jurídicos fueron eficaces o fallaron a favor de los delitos informáticos.

¿Qué son delitos informáticos?

Los delitos informáticos, como lo dice la palabra, son delitos que se producen mediante la tecnología. Nos decía el autor PARKER que los delitos informáticos son situaciones que involucran sistemas informáticos donde la víctima experimentó o pudo haber experimentado perjuicios, y el autor actuó con la intención de obtener beneficios propios (Hernandez, 2009).

Miguel Ramallo y María Castillo nos dan la definición que el delito informático nos habla del accionar de manera dolosa que genera un daño, perjuicio o mal a personas jurídicas o naturales con lo cual hubo un dispositivo electrónico de por medio de la acción, con la finalidad de hacer tareas informáticas (Pino, 2016).

Luego de analizar dos conceptos muy importantes sobre la definición de delitos informáticos, podemos llegar a la conclusión que los delitos informáticos son actividades de manera perjudicial donde afectan a una persona natural, entidad pública o privada de manera dañina, donde hay de por medio un artefacto o dispositivo electrónico, el cual será la herramienta principal para que el actor del delito pueda sacar beneficios propios sobre la víctima.

¿Qué son ciberataques?

Al igual que los delitos informáticos los ciberataques son delitos que se producen mediante la tecnología. El objetivo principal de estos son dañar, acceder sin permiso o hackear los sistemas informáticos que pueden ser redes amplias o dispositivos. Estos ataques cibernéticos pueden ocurrir de varias maneras, como, por ejemplo, cuando existen los virus informáticos, envió de mensajes o correos no deseados o SPAM (Ureña, 2015).

A la fecha de hoy, año 2024, no se cuenta con datos que sean verídicos sobre cuantos delitos informáticos se ha convertido entre el año 2023 – 2024. Sin embargo, para darnos una idea, si hay datos confirmados que del año 2020 al año 2022 existió un numero de 3.183 delitos y hubo 682 casos. Estos datos son proporcionados por la Policía Nacional del Ecuador. Así mismo la Policía nos menciona que, mediante estudios, se ha confirmado que dentro del Ecuador hay un numero de 6 provincias donde son las principales víctimas de los delitos informales los cuales son: Pichincha, Guayas, Imbabura, Manabí, Azuay y Carchi (EL COMERCIO, 2020).

Así mismo la Policía Nacional del Ecuador, luego de un aproximado de 11 meses de investigación, pudieron revelar datos donde se visualiza que hay cinco delitos informáticos los cuales se comenten con mayor frecuencia que al resto, los cuales son: (EL COMERCIO, 2020)

1. Estafa en línea
2. Violación a la intimidad
3. El acceso no consentido a un sistema informático
4. El ataque a la integridad de sistemas informáticos
5. Apropiación fraudulenta por medios electrónicos. (EL COMERCIO, 2020)

Clasificación de estafas tipificado por la policía nacional del Ecuador

La policía nacional a lo largo de sus investigaciones sobre delitos informáticos ha podido llegar a la conclusión de dar tres definiciones sobre los tipos de estafa en general, para poder describir e identificar los tipos de delitos informáticos que se están cometiendo. El primer tipo de estafa es el Phishing, que ocurre cuando los ciberdelincuentes contactan a la víctima haciéndose pasar por una persona conocida por la misma o que este en el entorno de la víctima, con el fin de poder llegar a una conversación y a su vez sacarle toda la información posible para así poder usarla en su contra. La segunda definición nos habla de Spear Phishing, en este tipo de estafa nos define que los ciberdelincuentes investigan la vida privada de la víctima como por ejemplo donde vive, estudia o trabaja, cuáles son los pasatiempos, gustos musicales, donde viven los familiares de la víctima, con el fin de poder engañarlas para poder perjudicarlas, por esa razón es recomendable tener los perfiles de redes sociales privados, no publicar fotos de donde se encuentra la víctima en ese momento. Si se usaran todos esos filtros de seguridad, para los ciberdelincuentes fuera difícil poder investigar la vida de la víctima. La última definición es el Smishing que ocurre cuando existe una manipulación de los ciberdelincuentes hacia la victimas a través de mensajes de texto o su vez de llamada telefónicas. (Indio, 2021).

Después de analizar la clasificación de tipos de estafa según la Policía Nacional del Ecuador, he podido llegar a la conclusión que los tipos de estafa que son de manera virtual, estos vendrían hacer un indicio para poder cometer delitos informáticos.

También se desprenden varios delitos como por ejemplo el delito de extorción, secuestro, robo, asesinato y muchos delitos más, por la razón que los delincuentes al saber toda la información de la víctima, ellos se benefician para no solo cometer los delitos informáticos, sino muchos delitos más que atentan contra los bienes, la vida o los allegados a la víctima.

Material y Métodos

En la investigación sobre delitos informáticos en Ecuador se llevó a cabo mediante un enfoque metodológico que es cuantitativo y estudio de casos que combina un análisis normativo y doctrinario, así como la recolección de datos empíricos a través de encuestas. A continuación, se describen los materiales y métodos utilizados en el estudio:

Materiales:

- Marco Legal: Se reviso el Código Orgánico Integral Penal (COIP) y otras normativas relacionadas con la ciberseguridad y la protección de datos personales en Ecuador. Esto permitió identificar las disposiciones legales existentes y sus deficiencias.
- Literatura académica: Se consultaron artículos científicos, libros y estudios previos sobre delitos informáticos, cibercrimen y su impacto en la sociedad. Esto proporciono un contexto teórico y antecedentes relevantes para la investigación.
- Casos Prácticos: Se analizaron casos documentados de delitos informáticos en Ecuador y en otros países, lo que ayudo a ilustrar la gravedad y las consecuencias de estas acciones

Métodos:

- Análisis Documental: Se realizo un análisis exhaustivo de la legislación vigente y de la literatura académica para identificar las lagunas legales y las áreas que requieren reformas. Este análisis permitió establecer un marco de referencia para la discusión sobre la efectividad de las leyes actuales.
- Encuestas: Se diseño y aplico una encuesta a 70 personas para evaluar su conocimiento sobre delitos informáticos y la legislación que los protege. Las preguntas incluyeron temas como la violación de la intimidad, las sanciones por delitos informáticos y la percepción general sobre la ciberseguridad. Los

resultados de la encuesta proporcionaron datos cuantitativos sobre el nivel de conciencia y conocimiento de la población

- Estudio comparativo: Se realizo un análisis comparativo de la legislación ecuatoriana con la de otros países, especialmente aquellos que han implementado medidas efectivas contra el cibercrimen, para identificar mejores prácticas y posibles reformas

Tratados internacionales sobre delitos informáticos

Los tratados internacionales han sido una herramienta fundamental para poder solucionar problemas, proteger derechos, promover cooperación, etc., tienen muchos beneficios entre dos o más de dos sujetos de derechos internacionales. Con el paso de los años, los delitos informáticos o la ciberdelincuencia ha sido un problema para los ciudadanos, que ha ido afectándolos de diferentes maneras. Por esa razón el concejo de Europa creo un convenio el cual se nombra "Convenio de Budapest" el cual se creó en el año del 2001 para poder combatir los problemas de ciberdelincuencia, pero aquí el problema radica en que el Ecuador no está suscrito a este convenio y esto es un problema grande porque el país se limita tanto a hacer investigaciones sobre los delitos informáticos como combatirlos. El Ecuador se encuentra anexo a varios convenios como por ejemplo el convenio de Berna para sobre los derechos de autor, convenio internacional de telecomunicaciones, pero no son exactamente sobre delitos informáticos. (Campos, 2019).

El Ecuador ha sido un blanco perfecto para los delitos informáticos en los últimos años, pero el país ha estado con muchas limitaciones para poder combatir esta problemática porque no está anexo a la convención de Budapest. Aunque no parezca relevante, el Ecuador debería adherirse lo más rápido posible a este convenio, porque al no estar adherido se complica el ámbito de investigaciones, no puede sancionar delitos informáticos a nivel mundial, no se podrá pedir, acceder o apoyarse en pruebas internacionales, el país está muy limitado al intercambio de información o apoyo internacional para poder combatir los delitos informáticos.

Código Orgánico Integral Penal

El Código Orgánico Integral Penal (COIP) es uno varios ordenamientos jurídicos que tiene el Ecuador donde existen un conjunto de normas jurídicas que ayuda a controlar y regular las penas y delitos de la materia penal, el COIP está organizado por ejemplo por: Principio generales, delitos, procedimiento penal y ejecución de penas. Pero la incógnita es, ¿Los ecuatorianos estamos protegidos por el COIP de los delitos informáticos?

El COIP en materia de delitos informáticos ha ido experimentando un proceso evolutivo, marcado por diversas modificaciones y actualizaciones, para poder adaptar las nuevas normas penales clásicas a las nuevas realidades del mundo digital. Un gran avance que tuvo el Ecuador en el ámbito digital fue cuando se dio por aprobada la ley de Comercio Electrónico, Mensajes de Datos y Firmas electrónicas. Esta ley proyectó un avance con muy buenos resultados en la búsqueda de un marco jurídico que garantizara seguridad al 100% a los usuarios de las tecnologías emergentes. En el año 2002 hubo modificaciones relevantes a esta ley, completando el panorama de los delitos informáticos y así fortaleciendo las herramientas legales para combatir dichos delitos. (Salgado, 2021)

En el COIP no existe un capítulo que sea específicamente dedicado para los delitos informáticos, pero podemos encontrar varios delitos a lo largo del texto legislativo que tipifican el tipo de conductas de varios delitos informáticos. A continuación, se mostrará una recopilación de todos los delitos informáticos que se encuentran en el texto legislativo penal:

ART. COIP	NOMBRE DEL ARTICULO	PENA
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	7 a 10 años
178	Violación a la intimidad	1 a 3 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
193	Reemplazo de identificación de terminales móviles	1 a 3 años
194	Comercialización ilícita de terminales móviles	1 a 3 años

229	Revelación ilegal de base de datos	1 a 3 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 contra la información pública reservada legalmente	5 a 7 años
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5 años

(Villacís, 2022)

Existe una lista de 13 delitos informáticos que están tipificados en el COIP, en la tabla visualizada sobre "delitos informáticos" se ha ordenado cada artículo desde el menor número hasta el mayor número, pero la pregunta es ¿De qué trata cada delito? a continuación se explicará cada definición según el COIP y se hará un análisis de cada delito.

Art.174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos: La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años (Código Orgánico Integral Penal [COIP], 2021)

En este delito existen varios factores que se deben que tomar en cuenta los cuales son: sujeto activo, sujeto pasivo, bien jurídico protegido, objeto material y conducta. El sujeto activo nos habla de la persona que comete el delito (autor), el sujeto pasivo es la persona que sufre en daño del delito, un menor de edad o persona con discapacidad (victima), el bien jurídico protegido nos habla de la integridad sexual y reproductiva y si lo vemos en segundo plano hablamos sobre la libertad de desarrollo que puedan tener los menores de 18 años y las personas que cuenten con una discapacidad y por último la conducta que nos habla sobre la acción u omisión derivada del delito. (Moncada & Guerrero, 2022)

Los niños, niñas y adolescentes van por sobre todas las cosas, ya que son un grupo que tiende a ser vulnerable ante los muchos peligros de la vida diaria y del internet, como lo mencionamos en la introducción, el internet cada vez se introduce en la vida cotidiana del ser humano porque es algo indispensable para la mayoría de actividades. El gobierno del Ecuador debería implementar en todas las escuelas y colegios una materia llamada o

referente a “educación sexual integral y seguridad en línea” para así poder capacitar y que estén preparados los niños, niñas y adolescentes por los peligros que tiene el internet. Así mismo hoy en día la inteligencia artificial (IA) ha tenido una avance impresionante y tenemos que usar esto a favor de la seguridad, el gobierno tiene que trabajar con empresas de tecnologías y plataformas para poder crear una IA que mediante el algoritmo haya un monitorio automático sobre las cuentas de los celulares de todos los menores de edad y bloquee toda clases de contenido sexual, por último el gobierno debería hacer análisis continuo sobre la actividad sexual de menores en línea y pueda comprender con más claridad este fenómeno y crear estrategias efectivas para la seguridad de todos los menores de edad.

Art. 174.- Violación a la intimidad: La persona que, sin contar con el consentimiento o la autorización legal, acceda, interprete, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionado con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal [COIP], 2021)

Cuando hablamos de la violación a la intimidad, hablamos de un tipo penal el cual es el resultado de una lesión y de una conducta al instante, es decir es pluriofensivo, para dejarlo un poco más claro, el termino pluriofensivo en el ámbito del derecho es aquel que ataca a más de un bien jurídico a la vez. La violación a la intimidad es pluriofensiva por la razón que, cuando se comete este delito no solo solo se viola o se ofende la libertad individual de cada ser humano, sino también se violenta la intimidad, la dignidad humana y la familia. Este delito también cuenta con varios factores como los sujetos activos, pasivos y objeto material, cuando hablamos de sujeto activo hablamos que el sujeto es singular e indeterminado, este sujeto intercepta comunicaciones de los sujetos que la emiten, generan o a su vez la envían y si esta información no es solicitada por alguna razón por las autoridades competentes, todo es ilegal, porque solo los sujetos dueños de su propia información deciden si se reserva o divulga su propio contenido. Cuando hablamos del sujeto pasivo hablamos que puede ser cualquier persona que se comunique con otra, el emisor y receptor tiene el derecho a la intimidad y a la privacidad, por lo tanto ambos sujetos pueden ser sujetos pasivos en la acción generada. Cuando hablamos del objeto material nos damos cuenta que todo apunta a que es la comunicación privada,

cuando existe comunicación entre dos personas por medios electrónicos como por ejemplo redes sociales, llamadas, mensajes de texto, correo electrónico y un sin número de manera de comunicarse que existen. (Gonzalez, 2017)

Este delito es uno de los más frecuentes entre jóvenes hoy en día, por la razón que con el paso del tiempo se ha ido normalizando enviarse fotos, videos o algún índole similar de la intimidad entre dos personas, este delito es muy grave, porque puede tener muchas consecuencias como nos dice el autor González, no solo se viola la intimidad, sino también la dignidad humana, han existido muchos casos en la actualidad donde adolescentes se han quitado la vida por culpa de las personas que las extorsionan con publicar sus fotos intimas o reciben acoso de las demás personas por la filtración de imagines intimas, por ejemplo en el periódico llamado “INFOBAE” nos encontramos titulares como “ Dos menores de edad se quitan la vida por el acoso que se recibe por la filtración de sus fotos intimas” o en “UNIVISION” donde se encuentran titulares como “Una joven se quita la vida por un video que su novio filtro” o diarios como “SEMANA” donde titula “ Un joven se suicida por ser extorsionado con su contenido intimo” lo similar que tienen todas las noticias relacionadas al tema es que los jóvenes entran en una depresión al no saber que hacer, a quien acudir, como solucionar, pensar que su reputación esta por los suelos y un sin números de razones. Esto es una problemática que se tiene que solucionar lo antes posible, porque muchos jóvenes y adultos mayores han vivido este tormento y muchas personas lo van a vivir a futuro, pero la pregunta es:

¿Por qué sucede esto?, La respuesta es simple y es porque todas las personas están mal informadas o no tienen conocimiento que esto es un delito, si todas las personas o al menos el 75% de la población tuviera conocimiento que violar la intimidad es un delito, al menos la mayoría de personas lo pensarían dos veces antes de difundir contenido íntimo de otra persona, ¿Cómo solucionar esto? El gobierno tiene que encargarse de hacer campañas contra la violación a la intimidad, hacer seminarios, capacitar a los profesores para poder enseñar en las escuelas, colegios y universidades sobre las consecuencias de filtrar contenido íntimo, una estrategia muy buena que se tiene que aplicar es que el gobierno debería pagar publicidad en distintos sitios web donde ponga información sobre como ir a denunciar, que hacer si estas pasando por ese problema, con quien acudir y un montón de información para así poder ayudar a muchas personas que están siendo víctimas de la violación a la intimidad.

Art. 190.- Apropiación fraudulenta por medio electrónicos: La persona que utilice fraudulentamente 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 esta 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. (Código Orgánico Integral Penal [COIP], 2021)

En este delito encontramos varios factores como lo son el sujeto activo, sujeto pasivo, bien jurídico protegido y objeto material. Cuando se habla del sujeto activo tenemos que saber que puede ser cualquier persona, la comisión del delito de apropiación fraudulenta por medio electrónicos nos cita que el sujeto activo puede ser cualquier persona, no necesariamente alguien con conocimientos sobre tecnología que sea avanzada. Es común que las personas que comenten este delito sean hábiles en el campo de la tecnología, pero también existe una posibilidad que la persona que quiera cometer este delito contrate a otra persona que sea experto en tecnología para poder comer el delito, por lo tanto, podemos decir que en efecto cualquier persona puede ser el sujeto activo del delito. El sujeto pasivo al igual que el activo puede ser cualquier persona en general, pero esta definición es amplia, ya que la víctima en este caso podrían ser personas naturales y jurídicas que utilicen sistemas informáticos y o plataformas digitales para el uso de su funcionamiento. El bien jurídico protegido es acertado que es el patrimonio y la propiedad, ya que el articulo al ser apropiación ilícita, el principal derecho que se atenta, es el derecho a la propiedad, pero también existen varios bienes jurídicos que se pueden afectar como la intimidad de la persona pasiva, en caso de ser persona jurídica, la seguridad nacional, etc. Por último, el objetivo material de la infracción son los bienes, valores o derechos de la naturaleza digital dentro del ámbito de sistemas informáticos. (Torres, 2022)

En la actualidad los delitos informáticos son cada vez más comunes y sofisticados y el delito de apropiación fraudulenta por medios electrónicos no es la excepción, es una problemática que ha ido afectando a varias personas a lo largo de tiempo, como lo dijimos en el apartado de tratados internacionales, el Ecuador si quiere empezar a combatir contra estos delitos y tener una mayor eficacia para resolverlos, debería estar adherido al

convenio de Budapest ya que esto proporcionaría un marco jurídico internacional unificado para poder combatir los delitos informáticos, facilitaría la cooperación internacional entre autoridades judiciales y lo más importante, se equilibra la lucha contra la ciberdelincuencia con la protección de derechos humanos. Todas las entidades jurídicas al proporcionar el acceso a personas naturales a sistemas informáticos donde corren peligro los bienes tanto personales como de trabajo, se debería dar una capacitación de prevención, responsabilidad y compromiso de las personas, porque muchas personas confían la información a otra persona como por ejemplo a sus cónyuges, hijos, hermanos, amigos, etc., y a las personas que se les comparte la información, puede ser mal utilizada o compartirla sin saber las consecuencias que puede tener a futuro.

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles: La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionado con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal [COIP], 2021)

El articulo mencionado es complejo de entender, por ello vamos a explicarlo de manera general, cuando el articulo nos habla de reprogramación, nos habla del cambio del software o parámetros generales del terminal móviles, cuando se habla de modificación hablamos de cambiar o alterar los datos base que tienen el trabajo de identificar el dispositivo como lo es el IMEI, esto para explicarlo en palabras no técnicas, es como decir el número de cedula de un celular, es lo que nos garantiza la autenticidad del terminal móvil. A continuación, un ejemplo del articulo:

Carlos se graduó en tecnología y sistemática y tiene mucho conocimiento a cerca de electrónica y software, Carlos le compra un celular a un amigo suyo porque los vende más baratos que el precio normal y al momento de usarlo se da cuenta que el celular está bloqueado, al ingresar su tarjeta SIM se da cuenta que no puede utilizar la red de su operador móvil y en lugar de contactar a la compañía del servicio para desbloquear el celular de manera legal, Carlos toma la decisión de reprogramar el celular por su propia cuenta para poder usar libremente el celular.

Generalmente estos casos ocurren cuando los celulares han sido robados y la persona que fue afectada llama a la operadora del celular para bloquearlo y que no pueda ser usado, sin embargo, estos individuos estafan a las personas vendiendo los celulares bloqueados, para evitar eso tipo de estafas se recomienda no comprar celulares a personas extrañas de la calle, ni comprar celulares móviles usados o de reventa.

Art. 192: Intercambio, comercialización o compra de información de equipos terminales móviles: La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal [COIP], 2021)

Con el paso del tiempo la compra y venta de información de personas se ha transformado en un negocio rentable, por lo general en este negocio participan personas individualmente y empresas, estas funcionan de manera ilegal, sin ser supervisadas o reguladas por las autoridades correspondientes, los proveedores de internet abusan de los historiales de navegación, datos, ubicación móvil e informaciones sensibles del usuario, por lo tanto es importante establecer reglas lo antes posible para evitar este tipo de problemas. Existen empresas que su objetivo principal es limpiar, organizar y recopilar datos de uso personal para poder vender la información para el uso publicitario (TORRES, 2022)

Este delito en la actualidad es de los que más afecta a las personas, porque por este delito se despliegan muchos más como el robo, extorción, hurto, amenazas, asesinato, etc. Se despliegan varios delitos por que los principales compradores de esta información son sujetos que quieren obtener datos sobre una persona especifica, para así poder sacar provecho sobre la víctima y usar la información obtenida a su favor, al igual que el anterior artículo, las recomendaciones son que cuando una persona deje de usar un terminal móvil o se deñe, no hay que botarlos, venderlos o venderlos por piezas sino que habría que guardarlos, reciclarlos o irlos a dejar o vender a empresas que son certificadas como por claro, movistar, CNT, etc. Para poder evitar el robo de información por personas. Al igual que muchas empresas sin certificación recopilan toda la información robada para vendérsela a otras empresas y te puedan vender productos mediante publicidad en base a tu información.

Art. 193.- Reemplazo de identificación de terminales móviles: La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal [COIP], 2021)

El articulo cuando habla de reemplazo de identificación de un terminal móvil, se refiere a la acción de quitar o cambiar etiquetas originales que tiene cada terminal móvil, estas etiquetas contienen información como el número de serie del terminal móvil, el IMI (International Mobile Equipment Identity) y muchos más datos, sirven para dar autenticidad a cada terminal móvil y son únicos para cada dispositivo, al momento de colocar o reemplazar nuevas etiquetas el terminal móvil, terminara con identificación falsa o diferente al original, un ejemplo para poder entender este delito es el siguiente: Pablo se dedica a robar celulares para así poder venderlos más baratos, pero Pablo sabe que al momento de robar los celulares, las personas llaman a sus respectivas compañías para bloquear y rastrear el celular, Pablo para evitar este tipo de cosas opta por cambiar la información de identificación de los terminales móviles para que no puedan ser rastreados, bloqueados y recuperados y así venderlos a otras personas como si fuera otro celular totalmente limpio.

Art. 194.- Comercialización ilícita de terminales móviles: La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal [COIP], 2021)

Como en la mayoría de los delitos, existe el sujeto activo y pasivo, en este caso no es la excepción, ya que el sujeto activo es la persona que comercializa los terminales móviles y la persona pasiva es aquel que los adquiere, si bien la persona pasiva pueden ser personas naturales o jurídicas porque la comercialización ilícita en la actualidad se ha convertido en un negocio beneficioso para los individuos y emprensas grandes, porque deciden adquirir estos productos para poder ahorrar dinero en la compra de terminales móviles.

Un ejemplo muy práctico para entender este delito es: Luis tiene un local de aparatos electrónicos y decide importar terminales móviles de una empresa no autorizada, los terminales móviles (celulares) no cumplen con las regulaciones establecidas por la autoridad competente de telecomunicaciones del Ecuador y aun así Luis decide vender los celulares en su local. Esto es algo perjudicial porque primero están violando las disposiciones emitidas legalmente y segundo los consumidores al comprar un producto no saben si es original, esta robado, clonado o tiene piezas dañadas que puedan hacer explotar el celular y poner en peligro la integridad del consumidor en que este caso la persona pasiva.

Art. 229.- Revelación ilegal de base de datos: La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, base de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializado voluntaria e intencionalmente la violación de secreto, la intimidad y la privacidad de las personas, será sancionado con pena privativa de libertad de uno a tres años (Código Orgánico Integral Penal [COIP], 2021).

En este artículo hay como desglosar 6 acciones para poder interpretar claramente el articulo como, por ejemplo: la acción prohibida: Es la revelación de la información registrada; medio de información: Son los archivos, base de datos, ficheros, sistema informático del usuario, etc.; canales de revelación: Sistemas informáticos, electrónicos, telecomunicaciones o telemáticos; intención: Intencional o voluntaria; protección: Intimidad y privacidad de personas, sanción: 1 a 3 años de cárcel.

Un ejemplo para poder entender este artículo es: Mateo trabaja en una institución y el maneja los datos personales de todos los usuarios, como por ejemplo los nombres, números de teléfono, direcciones, información acerca de tarjetas de crédito o débito, saldos, etc. Mateo para poder sacar ingresos extra copia toda la información del usuario y las vende a una empresa que se dedica a marketing o a una persona común y corriente y todo eso lo hace sin el consentimiento del usuario

En este articulo hay una falla de redacción o de explicación, porque nos habla que cuando se comete el delito, hay una pena privativa de libertad de uno a tres años lo que relativamente vendría a ser una pena leve, esto es algo erróneo porque no se distingue o se diferencia la información que se difundió, ya que nos habla solo de la información confidencial y se pasa por alto la información reservada. (Ruiz, 2016)

El análisis que hace la autora Ruiz es muy acertado, porque si una persona revela información de base de datos de alguna compañía es grave, pero si una persona entra a alguna base de datos del ejército, fiscalía o policía y revela información como por ejemplo de alguna investigación reservada o algún operativo secreto y la difunde, esto puede generar un problema nacional, internacional, criminal, etc. Estas personas que cometen ese delito de manera grave como el ejemplo que acabamos de ver debería tener una pena privativa de libertad mucho más alta porque será un acto más grave que el normal.

Art. 230.- Interceptación ilegal de datos: Sera sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvié, grabe u observe, en cualquier forma un dato informático en su origen, destino o en interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible
2. La persona que ilegalmente diseñe, desarrolle, venda, ejecute, programe o envié mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder
3. La persona que posea, venda, distribuya o de cualquier otra forma, disemine o introduzca en uno o más sistemas informáticos, dispositivos electrónicos, programas u otros contenidos digitales destinados a causar lo descrito en el número anterior
4. La persona que a través de cualquier medio copie, clone comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que este soportada en las tarjetas de crédito, débito, pago o similares

5. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior (Código Orgánico Integral Penal [COIP], 2021).

Este artículo es muy importante para la protección de datos personales porque desde que la información está en un dispositivo electrónico que tenga vinculación con internet ya se corre un peligro como que la información se robada o difundida, gracias a este articulo está protegida la privacidad de las comunidades digitales de las personas, asegurando que no sean interceptados o chantajeados sin autorización judicial, pero algo que se tiene que tomar en cuenta es que la definición de contenido digital o sistema informático es algo ambigua porque pueden ser interpretados de manera amplia, lo que puede llevar a dificultades en su aplicación prácticas y en la redacción puede resultar en interpretaciones inconsistentes por parte de los jueces al momento de dar un veredicto, a continuación se dará un ejemplo de cada inciso para poder tener más claro el articulo:

1. Juan instala un programa de software espía en la computadora de lucia que es su compañera de trabajo para así poder entrar a sus correos electrónicos, Facebook, Instagram y obtener información confidencial para su beneficio personal
2. Pablo es hacker y crea una página web que es idéntica a la de una institución bancaria y empieza a mandar correos falsos y fraudulentos a los clientes de ese banco para que ingresen sus datos en la página falsa y así obtener acceso a los datos personales del cliente.
3. Carlos distribuye o vende un software dañino con virus que cuando se instala o simplemente se abre la aplicación el dispositivo electrónico automáticamente pasa a ser controlado por Carlos y así podrá robar la información
4. Un delincuente utiliza un skimmer (El skimmer es un dispositivo fraudulento que se coloca sobre el lector de las tarjetas de cajeros automáticos o terminales de pago para robar la información de las tarjetas de crédito o débito cuando los usuarios las insertan) (Corbino, 2016) para copar la información de las bandejas magnéticas de las tarjetas de crédito o débito de los clientes de un cajero automático y luego utiliza esa información para realizar compras fraudulentas.
5. Una persona fabrica dispositivos de skimming y los vende a otros delincuentes que los utilizan para clonar tarjetas de crédito en cajeros automáticos.

Art.- 231: Transferencia electrónica de activo patrimonial: La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensajes de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionado con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal [COIP], 2021).

El articulo 231 nos describe un delito relacionado con los delitos informáticos contra el activo patrimonial en este articulo tenemos que analizar 5 acciones las cuales son el verbo rector, bien jurídico protegido, sujeto activo, sujeto pasivo y consecuencia jurídica. El verbo rector son las palabras "alterar, manipular o modificar" un sistema informático no autorizado para obtener una transferencia o apropiación de un activo patrimonial; el bien jurídico protegido es el activo patrimonial como los bienes o recursos de valor que pertenecen a una persona; el sujeto activo es la persona que manipule el sistema informático no consentido; el sujeto pasivo es la persona natural o jurídica del activo patrimonial que es objeto de la transferencia no consentida y la consecuencia jurídica es la pena privativa de libertad de tres a cinco años.

A este delito lo vamos a nombrar como "un delito de moda" porque se ha cometido mucho los últimos 4 años, desde que las instituciones bancarias crearon las aplicaciones nombradas "banca virtual" han existido muchos robos, de 20 delitos informáticos que se comenten 1 persona puede salvar su dinero que fue robado, pero el problema aunque no se lo nombra directamente es un problema de las instituciones bancarias, porque ellos podrían impedir de 10 robos, al menos salvar el dinero de 7 o hasta 8 personas.

En el diario El Comercio publica una noticia acerca de un robo de transferencia electrónica de un activo patrimonial, nos relata una señora llamada Gisell de 35 años de edad que cuando salió de su trabajo una tarde cualquiera como todos los días, le empezaron a llegar mensajes de texto donde se notificaba el código de ingreso a la banca móvil y en otros mensajes el código para la confirmación de una transacción electrónica, nos relata que reviso el saldo de su cuenta y era de 728, 43 dólares y que todo parecía normal, pero pasando una hora le llegaron nuevos mensajes que decía que la contraseña fue cambiada con éxito, la usaría llamo a la institución bancaria para que le ayude con urgencia a que no se haga la transferencia, pero le comentaron que para ayudarle tenían

que validar sus datos y pasar el protocolo de seguridad, pero hasta realziar esos procesos la el dinero ya habría sido robada de la cuenta de la usaría. (EL COMERCIO, 2020)

El problema circula en que las instituciones bancarias siempre que ocurre un problema de transferencia bancaria ilegal, los usuarias preocupados y desesperados llaman a sus respectivos bancos para que se pueda ofrecer una solución, pero siempre existe el problema que se demoran excesivamente por comprobar los datos de verificación del usuario, está bien que tengan que seguir y respetar el protocolo de verificación de datos, pero en casos de crucial importancia no debería ser así, deberían crear algún programa de emergencia, para que cuando ocurran este tipo de situaciones solo necesiten hacer una videollamada para asegurar que es la persona propietaria de la cuenta y posterior a eso detener la cuenta, bloquear o quitar el dinero para que no se pueda hacer el robo a través de transferencia bancaria.

Art.- 232: Ataque a la integridad de sistemas informáticos: La persona que distribuya, dañe, borre, deteriore, altere suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal [COIP], 2021).

Se hizo una calificación al COIP por parte de expertos donde se pude manifestar que la calificación es media, porque hay delitos por el cual la pena privativa de libertad es muy alta y otros delitos por los cuales la pena privativa de libertad es muy baja, además donde nos comentan que algunos artículos están mal explicados como por ejemplo nos dicen que en este articulo el 232, tiene que tener excepciones los casos de investigación que tengan como objeto verificar la seguridad de los sistemas informáticos, siempre y cuando cuenten con la autorización correspondiente, nos dice también que los términos que se encuentran redactados en el artículo los cuales dice borrar, alterar, distribuir y entre todos los palabras, deberían estar junto a los términos "Con el objetivo de perjudicar o causar daño" como lo estipulan otros artículos (Tixi, 2022)

Art.- 233: Delitos contra la información pública reservada legalmente: La persona que destruya o inutilice información clasificada de conformidad con la ley, será sancionada con pena privativa de libertad de cinco a siete años

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal [COIP], 2021).

Este articulo como todos tiene una sujeto activo y conducta tipificada, pero en este caso se divide en dos partes, la primera es el sujeto activo que puede ser cualquier persona y la conducta típica es la distribución o inutilización de información clasificada, la segunda es el sujeto activo el cual en este caso vendría a ser un servidor público y la conducta tipificada es la obtención de información clasificada por medios electrónicos o informáticos, si hablamos de los elementos de tipo penal, tenemos que saber que existen dos, el cual es el elemento objetivo lo cual nos habla de la acción de destruir o inutilizar la información que ha sido clasificada según la ley, en este caso la información pública reservada legalmente, el otro elemento es el subjetivo el cual nos habla del Dolo el cual es la intención que tiene la persona de obtener la información sabiendo que es de clasificación legal.

Para poder entender este articulo vamos a explicarlo con un ejemplo; un empleado público de una institución del Estado Ecuatoriano, consciente de que esta accediendo a información clasificada, utiliza su acceso autorizado al sistema informático de la agencia para copiar documentos clasificados y los guarda en una memoria USB con la intención de tener la información y venderla. Para poder evitar este tipo de problemas todas las instituciones públicas deberían hacer que la información pública reservada solo la tengan las personas que son directivos o funcionarios públicos que en realidad sea necesario que tengan que trabajar con esa información, como es de conocimiento al entrar a una institución a trabajar se tiene mucha información a la mano de un funcionario, además que se debería instalar un software de seguridad en todas las computadoras de la institución para que no se puedan descargar, trasladar o no se puedan reconocer dispositivos de como USB para que así la información no sea sustraída de las computadoras.

Art.- 234: Acceso no consentido a un sistema informático, telemático o de telecomunicaciones: La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo el contra de la voluntad de quien tenga el legítimo derecho, para explorar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de

tráfico de datos o voz u ofrecer servicios legítimos, será sancionada con pena privativa de libertad de tres a cinco años (Código Orgánico Integral Penal [COIP], 2021).

Este artículo nos define de manera general el del delito informático ya que nos dice cuando exista el acceso no consentido a un sistema informático, telemático o telecomunicaciones, dentro de esta definición encontramos cuatro acciones el cual se divide en: Verbo rector, sujeto activo, sujeto pasivo y consecuencia jurídica. Cuando hablamos del verbo rector definimos que es la palabra "acceder" ya que el articulo nos dice que la persona que acceda, entonces ese es el verbo a identificar de manera principal porque si no existe la acción de acceder no existe el delito; cuando se habla del sujeto activo se menciona a la persona que acceda a un sistema informático no autorizado que haga esta actividad para un beneficio propio o para beneficios de tercer personas; el sujeto pasivo es la persona que está siendo afecta ya que es dueño del sistema informático que ha sido invadido ilegalmente y por último la consecuencia jurídica que viene a ser la pena privativa de libertad de tres a cinco por la ejecución del delito de acceder a un sistema informático, telecomunicaciones o telemático sin consentimiento e ilegalmente (VILLACRESES, 2024)

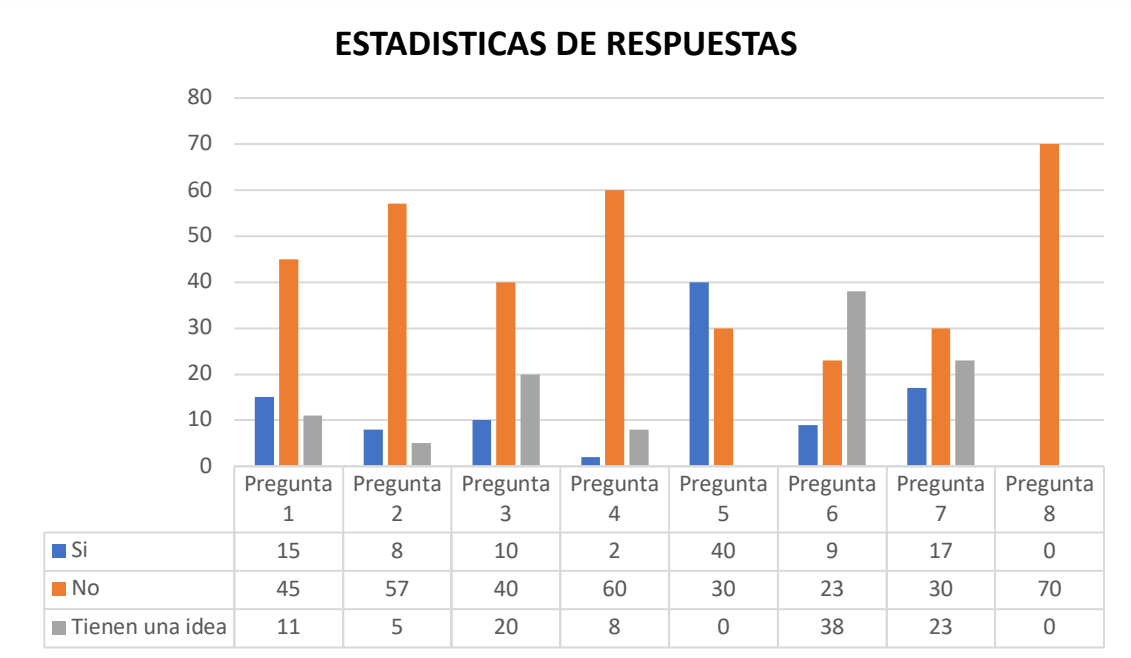
Se ha hecho una comparativa entre varias legislaciones de países como Ecuador, Venezuela y Perú acerca de los delitos informáticos y la diferencia de Ecuador con los otros países es que en las otras legislaciones cuando se comete un delito de índole informático además de la pena que se debe cumplir, existe una sanción económica para los autores del delito, lo cual en el Ecuador no existe. Desde mi punto de vista me parece erróneo que no exista ese tipo de sanciones en el COIP porque como es de conocimiento la mayoría de los delitos informáticos se hacen con un objetivo que es el económico como por ejemplo vender, retener o manipular información con el objetivo de beneficiarse a sí mismo, se debería imponer una sanción económica muy grande y retener las cuentas bancarias de quien comete el delito, como lo analizamos en un artículo anterior, hoy en día los delitos informáticos se han convertido en un negocio rentable económicamente.

Resultados y Discusión

En base a toda la investigación acerca de los delitos informáticos, se crearon incógnitas y he formulado preguntas claves para realizar a los ciudadanos para poder saber si realmente están informados sobre los delitos informáticos.

Preguntas:

1. ¿Sabes que son los delitos informáticos?
2. ¿Sabías que existe una normativa que te protege de los delitos informáticos?
3. ¿Sabes que significa violación a la intimidad?
4. ¿Sabías que hay cárcel para las personas que filtran tus fotos o videos íntimos?
5. ¿Has sido víctima alguna vez de hackeo?
6. ¿Sabías que si te transfieres dinero de una banca virtual a otra hay cárcel?
7. ¿Sabes que si te descargas información reservada del sistema de una institución pública o privada sin consentimiento hay cárcel?
8. ¿Sabes que si un celular está bloqueado como robado y le cambias la identificación del celular para que se desbloquee y poder usarlo es un delito?



	Pregunta 1	Pregunta 2	Pregunta 3	Pregunta 4	Pregunta 5	Pregunta 6	Pregunta 7	Pregunta 8
Si	15	8	10	2	40	9	17	0
No	45	57	40	60	30	23	30	70
Tienen una idea	11	5	20	8	0	38	23	0

Se encuesto a 70 personas en total, donde cada una fueron dando su respuesta acorde a sus conocimientos básicos, según la estadística nos podemos dar cuenta claramente que existe una falta de conocimientos acerca de los delitos informáticos, hay personas como se puede ver que tienen una idea del tema, no es por que conocen el tema a fondo o lo han estudiado alguna vez, sino supieron manifestar que es porque alguna vez lo escucharon en las noticias o solo por lógica básica.

Conclusiones

Culminada la investigación sobre los delitos informáticos se ha podido llegar a las siguientes conclusiones:

1. Las personas no están siendo informadas sobre los delitos informáticos, pero ¿esto porque sucede? Porque en las escuelas, colegios y trabajos no están siendo puntos claves para que todas las personas puedan ser informadas. Si desde antes se empezaran a topar estos temas, las personas sabrían lo que están haciendo y cuáles son las consecuencias de sus actos, pero como las personas nos están informadas correctamente sobre los delitos informáticos y cuáles son las penas, tanto las personas que están cometiendo delitos informáticos como las personas que están siendo víctimas de estos delitos, no harán nada al respecto como dejar de hacer ciertos actos o denunciar los actos. Aunque este tema no parezca de alta relevancia en el análisis que se hizo acerca de cada artículo nos podemos dar cuenta que los delitos informáticos afectan de manera, económica, psicológica y física, en el artículo específicamente 178 acerca de violación a la intimidad, en el análisis nos pudimos dar cuenta que en ciertos casos ha existido hasta la muerte.

   Esto ocurre porque la víctima y el autor del delito están conscientes de las consecuencias que puede tener a futuro cometer este delito, igualmente existen personas que no saben que están cometiendo un delito como es el 193 que nos habla de reemplazar la identificaciones móviles, al momento de realizar la encuestas las personas pudieron manifestar que no tenían idea que realizar ese acto era totalmente ilegal y una vez más comprobamos que es por falta conocimiento que jamás se dio en instituciones tanto sea educativas como de trabajo.
2. El COIP tiene que ser reformado, según el análisis que se realizó se puede visualizar que existen fallas dentro del mismo como, por ejemplo: existen penas para delitos que son muy bajas o muy altas de acuerdo a cada delito cometido, hay redacciones de delitos que necesitan completar con ciertas palabras para poder identificar que se cometió el delito con el objetivo de perjudicar a una persona.

En un análisis citado acerca de comparativa de la legislación de varios países se pudo visualizar que Ecuador era uno de los países que en al momento de sancionar los delitos informáticos solo tenía pena privativa de libertad y no una sanción económica, esto es algo que se debe rectificar y aplicar una sanción económica de acuerdo al caso investigado y con qué objetivo se realizó, porque si contratan un hacker para robar la información de una institución pública y le pagaron el valor de 200.000 dólares, y logran arrestar a la persona responsable, al actor del delito correspondería una pena de 3 a 5 años y luego saldría a disfrutar el dinero que lo consiguió gracias a cometer el delito.

3. El Ecuador para poder combatir de mejor manera los delitos informáticos tiene que adherirse al Convenio de Budapest en contra de los delitos informáticos, aunque parezca que estos delitos solo pueden afectar a las personas naturales, también pueden afectar a un país entero como meterse al sistema de gobierno y manipular los votos para la elección de presidentes y muchas cosas negativas, si el Ecuador decide adherirse a este convenio facilitaría mucho más la gestión para combatir estos delitos.
4. Instituciones públicas y privadas tiene que actualizarse en el ámbito tecnológico, como lo dijimos en el principio de la investigación conforme pase el tiempo los seres humanos cada vez dependen más de la tecnología y ahora en la actualidad con la creación de la inteligencia artificial se tienen que usar a favor, como creando softwares de seguridad para que sea mucho más difícil el robo de información o ingresar a paginas donde se puede acceder fácilmente, así mismo las empresas de internet deben poner barras de seguridad para poder controlar más a las personas que son menores de edad, porque en el internet podemos encontrar un sin números de peligros.

Referencias bibliográficas

Campos, N. J. (8 de Febrero de 2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos*, 103.

Código Orgánico Integral Penal [COIP]. (2021). Registro Oficial Suplemento 180.

Corbino, M. (2016). Skimming. *REPOSTIRIO INSTITUCIONAL DE LA UNLP*.

EL COMERCIO. (2020). 3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020. *EL COMERCIO*, 1.

EL COMERCIO. (2020). Delincuentes cibernéticos ingresaron a su cuenta bancaria y le robaron su dinero; una víctima cuenta su historia. *EL COMERCIO*.

Gonzalez, P. (2017). *De la violacion a la intimidad, reserva e intercepciones de comunidades.* Bogota.

Hernandez, L. (2009). El delito informatico. Obtenido de https://addi.ehu.es/bitstream/handle/10810/24953/18-Hernandez.indd.pdf?sequence=1

Indio, Y. T. (Junio de 2021). Delitos informaticos frecuentes en el Ecuador: casos de estudio. *Repositorio Institucional de la Universidad Politécnica Salesiana*. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/20942/1/UPS-GT003389.pdf

Moncada, I., & Guerrero, A. (2022). Contacto y embaucamiento con finalidades sexuales a menores de edad a través de medio electronicos. *Polo del Conocimiento: Revista científico-profesional*, 10, 11, 12.

Pino, S. A. (2016). *Google Academico.* Obtenido de http://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/599/1/Delitos%20Inform%c3%a1ticos.%20generalidades.pdf

Ruiz, O. (2016). "Análisis jurídico práctico del delito de revelación ilegal de base de datos por parte de un servidor público, en el código orgánico integral penal". *Repositorio Institucional UNIANDES*, 47.

Salgado, M. F. (2021). Analisis conceptual del delito informatico en Ecuador. *Scielo*.

Tixi, S. (2022). "Análisis dogmático jurídico respecto a los delitos informáticos en el código orgánico integral penal". *REPOSTORIO INSITUCIONAL UNIANDES*.

TORRES, C. (2022). La anomia jurídica en el artículo 192 del código orgánico integral penal que vulnera la información de identificación de equipos terminales móviles. *REPOSITORIO INSTITUCIONAL UNIANDES*, 35- 36.

Torres, M. P. (2022). Delito de apropiacion fraudulenta por medios electronicos bajo la modalidad de Phising dentro del marco juridico ecuatoriano. *REPOSITORIO INSTITUCIONAL*, 47- 48.

Ureña, F. (2015). Ciberataques, la mayor amenaza actual. *ieee.es*. Obtenido de file:///C:/Users/cedetech/Downloads/Dialnet-CiberataquesLaMayorAmenazaActual-7684551.pdf

Villacís, R. P. (2022). Ciberseguridad y Ciberdefensa: Perspectiva de la. *Revsita Tecnológica Ciencia y Educación Edwards Deming*.

VILLACRESES, K. (2024). Estudio comparado a las normas de Ecuador, Venezuela y Perú con relación a las consecuencias jurídicas por acceso no autorizado a sistemas informáticos. *UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA*.

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.