UNIVERSIDAD METROPOLITANA DEL ECUADOR

FACULTAD DE CIENCIAS SOCIALES, HUMANIDADES Y EDUCACION

CARRERA: DERECHO

SEDE QUITO

ENSAYO DE TITULACION PREVIO A LA OBTENCION DEL TITULO DE ABOGADO DE LOS TRIBUNALES DE JUSTICIA DE EL ECUADOR

REGULACIÓN DE LOS CIBER DELITOS O DELITOS INFORMÁTICOS TIPIFICADOS EN EL CÓDIGO INTEGRAL PENAL (COIP)

AUTOR:

HENRY DANIEL CHILUISA VALENCIA

TUTORA:

DRA. ALICIA RAMÍREZ DE CASTILLO PhD.

QUITO - 2023

CERTIFICADO DEL TUTOR

En calidad de Tutor del trabajo de Investigación sobre el tema: "REGULACIÓN DE LOS CIBER DELITOS O DELITOS INFORMÁTICOS TIPIFICADOS EN EL CÓDIGO INTEGRAL PENAL (COIP) del Sr. HENRY DANIEL CHILUISA VALENCIA, Egresado de la Carrera de Derecho, de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Metropolitana del Ecuador, considero que dicho trabajo de Graduación reúne los requisitos y méritos suficientes para ser sometidos a la Evaluación del Tribunal de Grado. Consejo Directivo de la Facultad designe para su correspondiente estudio y calificación.

DRA. ALICIA RAMÍREZ DE CASTILLO, PHD

TUTORA

CERTIFICACIÓN DE AUTORÍA DE TRABAJO DE TITULACIÓN

Yo, HENRY DANIEL CHILUISA VALENCIA**,** estudiante de la Universidad Metropolitana del Ecuador "UMET", Derecho, declaro en forma libre y voluntaria que el presente Ensayo que versa sobre: **REGULACIÓN DE LOS CIBER DELITOS O DELITOS INFORMÁTICOS TIPIFICADOS EN EL CÓDIGO INTEGRAL PENAL (COIP)** y las expresiones vertidas en la misma, son autoría del compareciente, las cuales se han realizado en base a recopilación bibliográfica, consultas de internet y consultas de campo.

En consecuencia, asumo la responsabilidad de la originalidad de la misma y el cuidado al referirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto.

Atentamente,

Firmado electrónicamente por:
HENRY DANIEL
CHILUISA VALENCIA

HENRY DANIEL CHILUISA VALENCIA

C.I. 1719984732

AUTOR

CESIÓN DE DERECHOS DE AUTOR

Yo, HENRY DANIEL CHILUISA VALENCIA, en calidad de autor y titular de los derechos morales y patrimoniales del trabajo de titulación, **REGULACIÓN DE LOS CIBER DELITOS O DELITOS INFORMÁTICOS TIPIFICADOS EN EL CÓDIGO INTEGRAL PENAL** (COIP**)**, modalidad ENSAYO de conformidad con el Art. 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, cedo a favor de la Universidad Metropolitana del Ecuador una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo ami favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Metropolitana del Ecuador para que realice la digitalización y publicación de este trabajo de titulación en el repositorio virtual, de conformidada lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Atentamente

Firmado electrónicamente por:
HENRY DANIEL
CHILUISA VALENCIA

_____

HENRY DANIEL CHILUISA VALENCIA

CI: 1719984732

DEDICATORIA

A Dios, porque ni una sola hoja de los árboles se caería sin su voluntad, a mis queridos Padres, Luis Rene Chiluisa Mendieta y Margarita del Roció Valencia, quienes con su ejemplo y apoyo incondicional me impulsaron a alcanzar este importante logro en mi vida, a ellos le debo todo lo que soy ya que me supieron formar para la vida con amor y dedicación.

AGRADECIMIENTO

Agradezco a Dios por haber cuidado y guiado mi camino permitiendo alcanzar este logro de mucha importancia en mi vida, mi admiración y sincero agradecimiento para mi abuelita Norma María Mendieta Mendieta, de quien siempre obtuve apoyo y cariño incondicional, siempre tendré en cuenta sus consejos ya que me han ayudado para desenvolverme en la vida como un hombre de bien y en esta nueva etapa que empiezo como profesional espero seguir contando con sus valiosos consejos y su inmenso amor.

Un especial agradecimiento para mí querida Dra. Alicia Ramírez de Castillo, quien con su paciencia, dedicación y don de enseñanza me ha sabido guiar por este camino de la hermosa Carrera de Derecho las palabras son insuficientes para exaltar la labor de esta excelente docente que deja huellas imborrables en la memoria del corazón

ÍNDICE

RESUMEN

En el presente ensayo se analizó objetivamente los delitos informáticos desde la perspectiva sancionatoria de la legislación ecuatoriana con la norma contenida en el Código Integral Penal (COIP) que fue promulgado en 2014 en el mismo se integró normativa en referencia a delitos informáticos, se realizó el análisis de la conducta típica y antijurídica de los delitos informáticos que se encuentran normados en el COIP (Código Orgánico Integral Penal) identificado los sujetos procesales que intervienen en los mismos, así como la identificación y clasificación de los ciber delincuentes que son conocidos como "hackers" pero que tienen una clasificación de acuerdo a sus acciones y conocimientos, los ciber delincuentes no son criminales comunes, son personas u organizaciones que tienen un alto grado de conocimientos de las TIC's y que utilizan este conocimiento para realizar acciones delincuenciales tales como estafa, apropiación de datos, ciber terrorismo, ciber bullying, clonación de tarjetas, pornografía infantil, extorsión, oferta de servicios sexuales con menores de 18 años por medio de dispositivos electrónicos, etc. con la característica de que estos pueden ser cometidos desde cualquier parte del mundo utilizando dispositivos electrónicos y las TIC's, así como identificar los ciber delitos y los esfuerzos de la administración de justicia y sus operadores en la lucha contra el ciber crimen que ha incrementado sus operaciones a nivel mundial utilizando la tecnología como instrumento para el cometimiento de actos ilícitos cuyo objetivo es obtener datos de manera fraudulenta logrando así manipular, borrar, modificar y atacar sistemas informáticos, en el presente ensayo presentamos ideas de colaboración internacional con el objetivo de que se realice una lucha efectiva contra el ciber crimen a la vez que presentamos estadísticas alarmantes del acelerado e incontenible incremento de delitos informáticos en el Ecuador, el análisis de la presente investigación arroja como resultado que la normativa ecuatoriana es insuficiente y no se encuentra actualizada para la evolución de los delitos informáticos ya que es imperativo que el Ecuador suscriba acuerdo de cooperación internacional que le permitan controlar mitigar y erradicar el ciber crimen.

Palabras Clave: Informática, Delito, Ciber, Tecnología, Crimen, Tics

ABSTRACT

This essay objectively analyzed computer crimes from the punitive perspective of the Ecuadorian legislation with the norm contained in the Comprehensive Criminal Code (COIP), which was enacted in 2014 in the same regulation, was integrated in reference to computer crimes.

The analysis of the typical and ant juridical conduct of computer crimes that are regulated in the COIP (Organic Integral Penal Code) identified the procedural subjects involved in the same, as well as the identification and classification of cyber criminals who are known as "hackers" but have a classification according to their actions and knowledge.

Cyber criminals are not common criminals, they are people or organizations that have a high degree of knowledge of ICT's and use this knowledge to carry out criminal actions such as fraud, data appropriation, cyber terrorism, cyber bullying, card cloning, child pornography, extortion, offer of sexual services with children under 18 years of age through electronic devices, etc. with the characteristic that these can be committed from anywhere in the world using electronic devices and ICT's.

As well as identifying cybercrimes and the efforts of the administration of justice and its operators in the fight against cybercrime that has increased its operations worldwide using technology as a tool for the commission of illegal acts whose objective is to obtain data fraudulently thus managing to manipulate, delete, modify and attack computer systems.

In this essay we present ideas of international collaboration in order to carry out an effective fight against cybercrime while we present alarming statistics of the rapid and unstoppable increase of computer crimes in Ecuador, the analysis of this research shows that the Ecuadorian legislation is insufficient and is not updated for the evolution of computer crimes since it is imperative that Ecuador sign international cooperation agreements that allow it to control, mitigate and eradicate cybercrime.

Keywords: Computer Science, Crime, Cyber, Technology, Crime, Tics.

INTRODUCCIÓN

Delitos informáticos o ciber delitos con el desarrollo y auge de la tecnología a nivel global la forma de cometer delitos también cambio y la normativa penal tuvo que hacer ajustes en sus leyes para sancionar estos delitos en este ensayo identificaremos los tipos de delitos informáticos y sus sanciones de acuerdo al Código Integral Penal Art. 174 (COIP) (Ecuador, Asamblea Nacional, 2014)

Desde un punto de vista jurídico se define a los ciber delitos como toda conducta típica, antijurídica y culpable que utiliza medios electrónicos o tecnológicos que lesionan o ponen en peligro la libertad informática, afectando la integridad, confidencialidad y disponibilidad de los sistemas informáticos redes y datos.

Los delitos informáticos o ciberdelitos han sido objeto de un amplio estudio entre juristas y profesionales de la seguridad informática con esto permitiendo que diversas legislaciones a nivel mundial tipifiquen estas conductas delictivas en pro de mitigar las consecuencias de las mismas ya que con la globalización y el auge del internet han incrementado el porcentaje de actos delincuenciales mediante el uso de la tecnología.

En el presente ensayo, definiremos que son los ciberdelitos: los delitos informáticos son todas las acciones realizadas por un ciber delincuente de forma digital a través del uso de internet o dispositivos electrónicos con el fin de causar daños o perjuicios a terceras personas, por lo general este tipo de delitos son cometidos desde otro país con la ayuda de las TIC (tecnologías de la información)

En el Ecuador en los últimos años se ha visto un incremento de delitos informáticos de manera exponencial muchos de los cuales han quedado sin denuncia debido al desconocimiento de las victimas ya que en la mayoría de ocasiones no saben a dónde acudir o cuales son los delitos informáticos que tienen sanción dentro de nuestro ordenamiento jurídico.

Cabe recalcar que esta modalidad de delitos está en continua transformación y cada vez las mafias que se dedican a estas actividades ilícitas desarrollan nuevas técnicas de robar información, existen grupos que se dedican a promover la enseñanza de este tipo de actividades por lo que este ensayo se enfoca en la tipificación de estos delitos en nuestro ordenamiento jurídico y también analizaremos el trabajo de policía nacional, organizaciones internacionales y legisladores para mitigar las acciones criminales ya que es de suma importancia la unión de estos grupos para poder

realizar un frente de lucha contra la ciber delincuencia.

Precisamente la base de los ciber delitos se centra en el robo de información personal, datos bancarios o datos confidenciales para luego ser utilizados de manera ilegal por los llamados “hackers” que son personas o mafias organizadas que se dedican a esta actividad ilícita desde diferentes lugares del mundo y con la ayuda de un ordenador quizás esta es la principal característica de este tipo de delitos que en la mayoría de casos son realizados de manera en que la víctima sin darse cuenta otorga sus datos y el delito se comete con la mínima o nula violencia.

Entre las principales víctimas se encuentran personas adultas mayores y jóvenes que al sentirse atraídos por ofertas dentro del internet ingresan sus datos personales de manera voluntaria siendo así víctimas de múltiples delitos informáticos como estafas o extorsiones ya que los ciber delincuentes utilizan la mínima oportunidad para poder realizar sus acciones criminales,

En el Ecuador es el Código Integral Penal (COIP) quien se encarga de tipificar estas conductas antijurídicas sancionándolas con la privación de la libertad dependiendo el tipo penal las penas privativas de libertad van desde 1 año hasta 10 años como pena máxima, muchos delitos informáticos fueron incluidos con la reforma del código integral penal en el año 2014.

El objetivo del presente ensayo es identificar los delitos informáticos y sus sanciones en referencia al COIP (Código Orgánico Integral Penal), así como también las medidas que implementa el ordenamiento jurídico ecuatoriano para poder mitigar estas acciones delictivas que se han incrementado con ayuda de los avances tecnológicos y la globalización.

DESARROLLO

Como antecedente principal nos remontaremos a la década de los 70 con el nacimiento del internet que por años tuvo un crecimiento acelerado y con esto también nació un lado oscuro dando lugar a nuevos términos desconocidos al momento como ciber delitos que tuvo su aparición por primera vez en la década de los 90 en Francia, utilizado el internet como base para sus acciones delictivas, otro precedente importante es la aparición de las redes sociales como Facebook.

Que si es bien logro que las personas tengan un acercamiento a pesar de la distancia, pero también ocasiono que la información personal quedo expuesta tanto para amigos como para desconocidos es ahí en donde entra en auge los ciberdelitos ya que los delincuentes cibernéticos o hackers se aprovechan de la que la información esta vulnerable y realizan sus actividades ilícitas.

En el Ecuador con la promulgación del Código Integral Penal en 2014 se estableció la tipificación de los delitos informáticos en el artículo 190 aunque anteriormente ya se estableció una normativa en 1999 se promulgo la ley de Comercio Electrónico mensajes de Datos y firmas electrónicas la cual fue un gran avance para la época ya que implementaba sanciones que intentaban crear un sistema seguro para los usuarios de internet.

Pero lamentablemente el auge de la tecnología no fue de la mano con la normativa legal y para el 2010 hubo una gran cantidad de delitos informáticos que quedaron impunes ya que muchas personas no sabían a dónde acudir o simplemente la falta de cultura de denuncia por parte de la ciudadanía, permitió que en muchas provincias del País se incremente los delitos informáticos ya que muchos de estos no eran denunciados

En el 2012 se hicieron modificaciones al Código Penal a fin de poder sancionar y este tipo de delitos entre los artículos más destacados está el articulo 200 numeral 1 que sancionaba a las personas que se apropien de información la divulguen o que intenten realizar actividades ilícitas con la información obtenida fraudulentamente la sanción o pena iba de seis meses a 1 año y multa pecuniaria de 500 a 1000 dólares.

En el actual código orgánico integral penal se aumentaron nuevos delitos y las sanciones también se hicieron más drásticas, esto es muy importante ya que tenemos una normativa que intenta abarcar en su mayoría los delitos cibernéticos y sancionarlos con penas representativas también se busca mitigar, educar y prevenir que más personas caigan en este tipo de delitos.

Definición delitos informáticos

El departamento de investigación de la Universidad de México señala como delitos informáticos todas "aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen un indebido uso de cualquier medio informático"

En torno al delito informático, (Camacho Losa, 1987) define al delito informático como: "Cualquier acción dolosa o culposa, es decir con o sin intención de causar daño ya sea a personas o a entidades de forma directa o inmediata la victima haciendo uso de forma activa de dispositivos utilizados en actividades informáticas". (pag.25)

El delito informático para (Suárez Sánchez, 2016), establece:

> En conclusión, el delito informático está vinculado no solo a la realización de una conducta delictiva 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 (págs. 44).

Ante lo expuesto realizaré mi definición de delitos informáticos, al realizar mi investigación puedo mencionar que los delitos informáticos son acciones ilícitas que se realizan mediante el mal uso de las TIC (Tecnologías de la Información), los actos ilícitos se han transformado de tal forma que antiguas formas de delinquir han sido adaptadas para cometerlas utilizando la tecnología.

Delitos Informáticos reconocidos en el COIP

En el actual Código Orgánico Integral Penal (COIP) están divididos en varias secciones los delitos informáticos y sus sanciones en un apartado de la sección cuarta de los de delitos contra la integridad sexual y reproductiva en el artículo 174 establece que tendrá una sanción de pena privativa de la libertad den 7 a 10 años toda persona que difunda contenido de oferta sexual con menores de 18 años por cualquier medio electrónico como chat, mensajería juegos electrónicos u otro medio electrónico. (Ecuador, Asamblea Nacional, 2014)

En la sección sexta artículo 178 delitos contra el derecho a la intimidad familiar y personal se tipifica la divulgación, reproducción, retención o difusión de información contenida en soportes informáticos sin la autorización de la otra persona y la sanción es la privación de la libertad de 1 a 3 años quedando exentos de esta pena la persona divulgue información en audio y video siempre y cuando la misma también intervenga.

En la sección novena delitos contra la propiedad articulo 186 numeral 2 La estafa mediante

el uso de dispositivos electrónicos que clonen la información de una tarjeta o la alteren o la modificación de cajeros electrónicos para alterar, capturar, almacenar o reproducir información para este delito la pena es de 7 años y puede ser de 10 años si los afectados son doso más personas o el monto de perjuicio de 50 salarios básicos

En el artículo 190 tenemos un delito informático propio ya que para que se considerado como tal el implicado debe tener un amplio conocimiento en informático lo que conocemos como hacker para que sea sancionado se deberá utilizar un medio electrónico para apropiarse sin autorización de un bien ajeno sea por transferencia no consentida de bienes, valores y derechos para este ciber delito la sanción va de 1 a 3 años.

Los artículos 191, 192, 193, 194 establecen una sanción de 1 a 3 años a todas las personas que alteren equipos terminales móviles con fines delictivos o para su comercialización con estos artículos se busca mitigar y frenar el robo de dispositivos móviles ya que en ocasiones los equipos son robados y alteran los IMEI y etiquetas de seguridad incrementando así la delincuencia ya que el robo de teléfonos celulares es uno de los delitos más cometidos en el Ecuador.

El artículo 195 también sanciona a las personas que tengan en su propiedad maquinas, dispositivos que o dispongan de infraestructura para el ilícito de igual forma la sanción para este ilícito va desde 1 a 3 años de privación de la libertad siendo así que se intenta reducir este tipo de delitos ya en ocasiones las personas que venden o tienen en su poder este tipo de dispositivos realizan el ilícito.

El articulo 211 castiga con pena de privación de libertad a la o las personas que mediante dispositivos móviles o programas informáticos modifiquen, cambien, alteren, supriman o añadan información personal incorrecta de otras personas o alteren su propia información personal con el fin de manipular o inducir al engaño a otras personas y de esta forma cometer ilícitos como falsificación de datos.

El articulo 229 sanciona con privación de libertad de uno a 3 años a quien revele información de base de datos sin consentimiento, este artículo no se cumple al pie de la letra ya que es común encontrar personas que comercializan bases de datos a call centers y empresas comerciales para que se encarguen de llamar a potenciales compradores y por otra parte también se venden estas bases de datos para realizar llamadas de estafa y de extorsión.

El articulo 231 sanciona con pena privativa de libertad de 3 a 5 años a las personas que realicen alteraciones en su activo patrimonial cambando así mediante softwares sofisticados sus cuentas bancaria o propiedades a su nombre o a nombre de terceras personas intentado mitigar así el lavado de activos y testaferrismo.

El Artículo 232 toda persona que vulnere o ataque la integridad de sistemas informáticos será sancionada con la pena privativa de libertad de 3 a 5 años, como hemos visto en los últimos años diferentes ataques a sitios web y sistemas informáticos estatales por hackers logrando así robar o modificar información confidencial de usuarios logando millonarias pérdidas al estado y a empresas particulares.

El Articulo 233 Delitos contra la información pública reservada legalmente las personas o grupos de hacker que incurran en este delito tendrán una sanción de 5 a 7 años de privación de libertad se impone la misma pena a quienes según el Artículo 234 realicen el acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

En el artículo 298 inciso 8 defraudación tributaria para quienes alteren libros o registros informáticos de contabilidad beneficiando o perjudicando dependiendo la información que se altere tal como asientos contables, registro de cuentas contables, nombres cantidades o nombres falsos tendrán una pena privativa de libertad de 1 a 3 años.

Principales causas de delitos informáticos en el Ecuador

Entre las principales causas para que las víctimas sufran de ciberdelitos es el descuido ya que en la mayoría de casos se ha originado por descuido de los usuarios al momento de ingresar información en redes sociales o ingresar información personal en redes no seguras en las cuales los hackers o ciber delincuentes aprovechan para y utilizan esta información para realizar múltiples delitos.

La falta de cultura de denuncia también forma parte de las causas del incremento de delitos informáticos en el país ya que muchas víctimas no acuden a realizar una denuncia formal en fiscalía quedando así este delito impune ya que ante la falta de personas que denuncien estos actos ilícitos, fiscalía no puede actuar e intentar desmantelar las bandas criminales que se dedican a estas actividades, por otra parte los pocos usuarios que se han acercado a realizar la denuncia respectiva menciona que el trámite es engorroso y que no disponen de tiempo para continuar con el proceso abandonándolo y dejando que el delito quede impune.

En otra causa está el aceptar correos electrónicos de remitente desconocidos en donde realizan falsificación de páginas oficiales, aunque la dirección Url no es segura siendo así un claro descuido por parte del usuario al no verificar que la dirección web sea de una fuente confiable a esto se lo conoce con el termino en ingles phishing con esto los ciber delincuentes buscan que clonar las páginas oficiales de bancos a fin de obtener contraseñas bancarias para poder realizar sus acciones criminales y realizar robos o estafas bancarias.

Sujetos que intervienen en los delitos informáticos

Para el Derecho Penal las conductas típicas antijurídicas constan de dos sujetos un sujeto activo y un sujeto pasivo, los mismos pueden ser una o varias personas naturales o personas jurídicas, tenemos así que la persona que sufrió del daño es el sujeto pasivo y la o las personas que ejecutan el acto ilegal son el sujeto activo ya que realizan acciones típicas antijurídicas en contra del bien protegido que en este caso sería la información del sujeto pasivo o víctima.

El sujeto activo como ya lo definí es la persona que realiza el ilícito pero como diferenciamos a estos ciber delincuentes de los delincuentes tradicionales puedo identificar de manera clara que son personas que tienen un conocimiento avanzado acerca de sistemas informáticos o tiene contacto directo con información sensible por causas laborales o tienen habilidades con el uso de sistemas informáticos las cuales utilizan para el cometimiento de actos ilícitos con la ayuda de dispositivos electrónicos.

El sujeto pasivo es la persona titular del bien jurídico protegido que la ley intenta proteger y que sufre la actividad típica antijurídica del sujeto activo en otras palabras es la victima la cual a causa de diversas herramientas informáticas que utilizan los llamados hackers terminan entregando informaciones sensibles siendo víctimas de múltiples delitos.

El desafío de sancionar los delitos informáticos en el Ecuador

Como hemos expuesto en líneas anteriores resulta un desafío la lucha contra los ciber delincuencia ya que muchos de estos ilícitos en la mayoría de casos se cometen desde otros países ya que este tipo de delitos tienen la característica de que no es necesario estar en el mismo país ni en la misma ciudad para realizarlo siendo así que torna una tarea difícil seguir el rastro y poder sancionarlo.

La versatilidad que se presta para el cometimiento de este tipo de delitos pone en aprietos tanto a la policía nacional a jueces y organismos de justicia ya que si es bien con la reforma del

COIP del 2014 se establecieron las directrices para sancionar los múltiples delitos informáticos existentes, pero muchos de estos delitos escapan de la jurisdicción ecuatoriana y la falta de cooperación internacional ha impedido realizar un seguimiento efectivo ante estas bandas criminales.

Al mencionar que muchos de los delitos informáticos son cometidos de manera remota desde otros países no quiere decir que en el Ecuador no existan estas estructuras criminales ya que si las hay y han tenido un incremento sustancial en los últimos años realizando diferentes ataques cibernéticos tanto a personas particulares robando su información personal y bancaria y también las instituciones públicas han sido blanco de robo y alteración de información en beneficio de los ciber delincuentes que en muchos de los casos operan desde las diferentes cárceles del país.

Otro de los problemas que puedo mencionar al momento de juzgar un ciber delito es el poco conocimiento del tema por parte de fiscales, jueces y administradores de justicia ya que por lo general este tipo de delitos quedan impunes por que al momento de juzgar no tienen una idea clara de materia penal informática o en la mayoría de casos no aplican el tipo penal correspondiente al delito, la falta de conocimiento ha ocasionado que este tipo de delitos no sean juzgados quedando en su mayoría impunes.

La principal problemática radica en la poca o nula cooperación internacional ya que muchos países disponen de leyes obsoletas para combatir la forma de cometer los ciber delitos y como generalmente los delitos informáticos realizan una ruta que atraviesa algunos países antes del cometimiento del ilícito, entonces se vuelve una práctica difícil poder sancionar este tipo de delitos sumado que cada país tiene su propia legislación penal y no se quiere ceder en cuanto a la tipificación unánime que ayude a combatir la ciber delincuencia “ no se puede combatir la delincuencia del siglo XXI con leyes del siglo XX.

Propuesta para combatir la ciber delincuencia

Como he mencionado los delitos informáticos tienen como característica especial que en su mayoría no son cometidos “in situ” y que el rastro criminal puede atravesar varios países antes de concluir con el delito, teniendo en cuenta que los ciber delincuentes cada más se encuentran actualizados con la nueva tecnología y la nueva forma de cometer delitos seria imperativo la unión de los países y realizar una cooperación para crear leyes o un código.

Este código abarcaría una tipificación especial para los ciber delitos, pero lo importante o

especial seria que se pueda aplicar en todos los países para que al momento de poder juzgarlo y combatirlo no existan lagunas legales como las hay en la actualidad ya que cada país tiene su legislación y existen controversias al momento de poder sancionar los ciber delitos ya que de un a otro país la tipificación varia.

Tipos o clasificación de ciber delincuentes

Como ya he mencionado los ciber delincuentes son personas con un alto conocimiento en tecnología, redes y sistemas informáticos que utilizan este conocimiento para cometer actos ilícitos como estafas, defraudaciones fiscales y ataques a sistemas operativos con la intención de borrar, alterar o robar información, generalmente son conocidos como hackers, pero hay una clasificación ya que en su mayoría son personas que realizan acciones criminales, pero hay ciertas excepciones.

Los Hacker White Hat o hackers de sombrero blanco son personas u organizaciones con el conocimiento para hackear sistemas operativos, pero son contratados por empresas de ciber seguridad para detectar vulnerabilidades dentro de sus sistemas operativos y de esa forma realizar los respectivos ajustes a estos sistemas informáticos a fin de evitar sufrir ataques cibernéticos, este tipo de hackers trabajan conjuntamente con la policía o empresas privadas como públicas.

Los Hacker Black Hat o hackers de sombrero negro al igual que los hackers de sombrero blanco son expertos en informática, pero sus fines son completamente diferentes ya que sus actividades se centran en vulnerar sistemas informáticos para acceder a información confidencial y robar información, datos bancarios o información de acceso reservado de gobiernos y empresas privadas a fin de utilizarla para cometer actos ilícitos.

Los Hacker Gray Hat al igual que los anteriores mencionados son expertos en informática y sistemas de ciber seguridad, pero su diferencia es que no utilizan su conocimiento ni para hacer el bien o el mal, ellos disfrutan y romper o vulnerar sistemas informáticos buscan lagunas o vacíos para poder ingresar a sistemas informáticos por diversión o pasatiempo son grupos que realizan estas actividades por hobbies.

Los Hacker Blue Hat son aficionados a la informática sin mucho conocimiento en sistemas informáticos pero que buscan realizar el mal ya que infectan sistemas con virus o intentan vulnerarlos sin mucho éxito ya que lo que intentan es alcanzar popularidad entre su comunidad, aunque sus conocimientos no son avanzados ni sus técnicas las mejores si se los puede considerar un grupo peligroso ya que sus intenciones son maliciosas e intentan realizar el mayor daño posible.

Los Hackactivistas son grupos de hackers anónimos que buscan vulnerar sitios web o sistemas informáticos gubernamentales para obtener beneficios económicos o políticos el grupo más reconocido a nivel mundial es el grupo Anonymous que esté presente en muchos países y que por lo general buscan exponer injusticas o actos de corrupción gubernamental o intentan ejercer presión política y mediática con la información obtenida.

Diferencias entre hackactivismo y Ciberactivismo

Mientras que los Hackactivistas utilizan cualquier medio ya sea ilegal o legal para acceder a sistemas operativos a fin de realizar sus actos de protestas sin causar danos severos, losciber activistas utilizan únicamente medios legales para realizar sus actividades de protesta sin alterar el normal funcionamiento de empresas u organizaciones ya que su principal fin es hacer escuchar sus peticiones, pero a través de software legales.

Delitos informáticos más cometidos en el Ecuador

El (El Comercio, 2022) menciona un informe estadístico de la unidad de ciber delitosde la policía nacional que entre el año 2020 a julio de 2022 se han registrado 3183 delitos informáticos en el año 2020 se registraron 682 casos en el año 2021 hubo un incremento a 1851y en los 6 primeros meses del año 2022 ya van más de 650 casos registrados. Teniendo así una tendencia al incremento sustancial en ciber delitos este informe de la policía nacional no cuenta con los casos no denunciados por la ciudadanía por lo que es un aproximado.

Los datos son alarmantes teniendo en cuenta que la tenencia es a incrementarse este tipo de delitos entre los más cometidos tenemos los fraudes bancarios, estafas por redes sociales, ofertas laborales fraudulentas, phishing, pornografía infantil, llamadas falsas, violación al derecho a la intimidad y extorsiones.

Los fraudes bancarios este tipo de delitos son los más comunes y su modus operandi aplica robando datos bancarios de las víctimas para acceder a sus cuentas bancarias y realizar transacciones no consentidas por el usuario, adicional utilizan dispositivos electrónicos que colocan en cajeros automáticos para realizar la clonación de tarjetas y realizar compras o débitos de las cuentas bancarias de las víctimas.

Las estafas por redes sociales para este delito los ciber delincuentes operan por redes sociales como Facebook y WhatsApp en las cuales ofertan productos y servicios a bajos costo o costos promocionales la víctima se deja atrapar por este tupo de ofertas y realiza la compra la cual

nunca llega ya que por lo general son cuentas falsas o nuevas que luego de haber cometido la estafa borran la cuenta y se pierde el contacto con el vendedor siendo así que nunca se recibeel producto, a pesar de ser un ciber delito muy común casi no es denunciado por lo cual las autoridades no pueden realizar un seguimiento efectivo a este ilícito.

Las ofertas laborales fraudulentas por internet para este tipo de delitos utilizan redes sociales y nombres falsos de empresas conocidas y prestigiosas ofertando vacantes laborales con sueldos llamativos y simulando procesos de contratación como si fueran las empresas verdaderas en el cual solicitan compra de uniformes o pagos para exámenes médicos o capaciones a lo que muchos incautos acceden por la falta de oportunidades laborales o porque le llama la atención la oferta salarial, luego se realizar el depósito o pagos solicitados estas empresas fraudulentas y falsas desaparecen.

El phishing para este delito los hackers utilizan el correo electrónico para enviar mensajes spam o basura simulan paginas falsas en las cuáles solicitan información personal o bancaria para luego realizar actos ilícitos como robo de dinero o falsificación de información, este ciber delito va tomando fuerza en el país ya que son constantes los correos electrónicos que envían a diario los ciber delincuentes para intentar apropiarse de información personal de las victimas que caen en este ciber delito quizás por desconocimiento o descuido.

Las llamadas de extorsión o estafa.

Aunque no es una práctica nueva si ha tenido un mayor auge en los últimos años, esta práctica consiste en que los ciber delincuentes realizan llamadas a las potenciales víctimas haciéndose pasar por supuestos familiares y solicitar dinero fingiendo un supuesto problema o accidente, este delito ha incrementado gracias a la tecnología sobre todo al poco cuidado de las personas a colocar información personal en sus redes sociales, información que es utilizada por ciber delincuentes y también delincuentes comunes que la utilizan para realizar estas llamadas.

También puedo mencionar las llamadas de extorsión se han incrementado con la crisis carcelaria en el País ya que muchos ciudadanos han denunciado ser víctimas de llamadas amenazantes solicitando dinero por supuesta protección o para que no les hagan daño esto ha tomado un término utilizado en Colombia llamadas “vacunas” las cuales han sido utilizadas por bandas criminales aprovechándose de la ola de inseguridad que vive en País.

Se considera al Tráfico de órganos como un ciber delito como establece el COIP en el

artículo 96 toda persona que fuera de los casos permitidos por la ley realice actos onerosos con órganos, tejidos, fluidos o componentes anatómicos por cualquier medio esto incluye también por medios o dispositivos informáticos ya que por la tecnología es fácil visualizar en internet la venta de órganos la pena privativa de libertad para este delito es de 10 a 13 años.

La pornografía Infantil como establece el artículo 103 Código Integral Penal, la persona que filme, grabe, produzca, transmita, edite materiales visuales y audiovisuales informáticos, electrónicos o de cualquier soporte físico o digital que contenga la representación visual de desnudos o semidesnudos reales o simulados de niños, niñas y adolescentes con connotación sexual será sancionado con pena privativa de libertad de 13 a 16 años, este delito ha tomado un preocupante incremento ya que el internet y redes sociales han permitido que crezca estas acciones repudiables y recriminables. (Ecuador, Asamblea Nacional, 2014)

Este delito es considerado como ciber delito ya que también se realiza a través de internet está tipificado en el artículo 178 del COIP es la violación de la intimidad en la cual sanciona con pena privativa de la libertad de uno a tres años a quien sin autorización divulgue, reproduzca almacene o exponga información personal, aunque la norma es clara existe un gran problema al momento de sancionarlo ya que hay muchas personas que exponen su vida públicamente en redes sociales y su información es de libre acceso aunque las personas que las comercializan o hacen uso de la misma no tienen su consentimiento.

El acoso sexual o "Grooming" artículo 173 del COIP consiste en el contacto con finalidad sexual con menores de 18 años mediante medios electrónicos y la pena privativa de libertad para este delito está establecida entre 1 y 3 años, esta práctica se ha vuelto común yaque las redes sociales han contribuido para que cada vez más menores de edad accedan a este tipo de contenido sin supervisión.

La oferta de servicios sexuales a través de medios electrónicos o "sexting" como establece el artículo 174 del COIP se sancionara con pena privativa de la libertad de 7 a 10 años quienes oferten servicios sexuales con menores de 18 años a través de medios digitales o electrónicos, este delito ha utilizado la tecnología para corromper a menores de edad y hacerles víctimas de este delito y aunque puede ser confundido como pornografía infantil tiene una clara diferencia ya que en este delito se ofertan los servicios sexuales y no solo contenido grafico explícito en el que intervienen menores de 18 años.

Derechos de Autor afectados por los Ciberdelitos

Quizás el grupo más afectado por la ciber delincuencia son artistas, escritores, y todo tipo de persona que interviene en procesos de invención e innovación estas personas han visto vulnerado sus derechos de propiedad intelectual ya que debido al avance vertiginoso de la tecnología muchas de sus obras han sufrido de ciber ataques causando grandes pérdidas para sus creadores que han visto que sus creaciones han sido replicadas sus obras sin recibir reconocimiento moral o económico.

Las leyes que protegen la propiedad intelectual son insuficientes y no son amparadas en el nuevo marco de tecnología de la información, aunque el internet ha ayudado que muchos autores puedan impulsar sus creaciones y generar ganancias por las mismas también se presenta un lado oscuro en la cual no se puede mantener control de las copias y distribución ocasionando en su mayoría pérdidas significativas para sus autores.

Con la promulgación Del Código Orgánico de la Economía Social de los conocimientos, creatividad e innovación se buscó proteger los derechos de autor y de propiedad intelectual y aunque su normativa abarca extensivamente dicha protección aún resulta insuficiente ante la excesiva y acelerada expansión de la ciber delincuencia ya que al no contar con una normativa penal y administradores de justicia preparados para afrontar esta ola de criminalidad que evoluciona a pasos agigantados.

En el Ecuador las normas que intentan proteger los derechos de autor en todas las áreas de invención y también impulsar la creatividad otorgando protección ante la nuevas formas de ataques de ciber delincuentes que merman sus ganancias o beneficios debido a la piratería que prolifera en la actualidad ya que los llamados “piratas” o “hackers” utilizando la innovación tecnológica se encargan de realizar copias sin autorización de los autores y las reparten a nivel mundial generando pérdidas millonarias en regalías. (Ecuador, Asamblea Nacional, 2016)

Las pérdidas por incumplimiento de derechos de autor son millonarias, pero también atacan a autores que recién van empezando y que no cuentan con los medios suficientes para impulsar sus obras y en muchas ocasiones el mundo se pierde de grandes obras e invenciones porfalta de protección, quizás esta es la consecuencia luego de los perjuicios económicos que afectan a los derechos de autor perdiéndonos de grandes obras e invenciones ya que al no existir una seguridad jurídica cada vez son menos las personas que se dediquen a crear invenciones y obras.

Cuadro No 1. Delitos Informáticos reconocidos por la ONU

Delitos Informáticos reconocidos por la ONU (Organización de las Naciones Unidas)	
Fraudes cometidos por computadora	Transferencia de fondos
Falsificaciones informáticas	Destrucción de datos
Daños o modificaciones de programas o sistemas informáticos	Vulneración de datos
Narcotráfico	Terrorismo
Terrorismo	Pornografía Infantil
Ciber bullying	Phishing
Estafas electrónicas	Trata de personas
Ataques a plataformas gubernamentales	Violación a la intimidad

Fuente: (Nacionas Unidas, 2015)

Cabe recalcar que todos estos delitos son reconocidos por la ONU como delitos informáticos ya que su principal característica es que son cometidos a través de dispositivos móviles realizado por personas con alto conocimiento de TIC's, realizo esta aclaración ya que se suele confundir que el narcotráfico no es un ciber delito y en parte se tiene razón, pero la forma como ha cambiado la forma de cometer este ilícito utilizando la tecnología permite que la ONU lo considere como un delito informático.

Adicional cabe recalcar que estos delitos con cometidos por personas que tienen un alto conocimiento de las TIC's y de informática y que se les diferencia por esta razón de los criminales comunes ya que por lo general a los ciber delincuentes los conocemos como delincuentes de cuello blanco.

Cuadro N°2 Estadísticas de ciber delitos en el Ecuador

Artículo del COIP	Tipo penal	Año 2017	Año 2018	Año 2019	Año 2020	Año 2021	Total
103	Pornografía utilizando niñas, niños adolescentes.	103	104	91	113	95	496
104	Comercialización de pornografía utilizando niños, niñas, adolescentes	26	9	17	18	15	85
173	Contacto con finalidad sexual con menores de 18 años por medios electrónicos	158	202	165	152	152	829
174	Oferta de servicios sexuales con menores de 18 años por medios electrónicos	12	14	16	/	/	/
178	Violación a la intimidad	1660	2062	2038	1985	1346	9091
186	Estafa	13911	14268	16918	18415	16272	79784
190	Apropiación fraudulenta por medios electrónicos	959	1448	1744	2280	3962	10393
192	Intercambio, comercialización o compra de información de equipos terminales móviles.	0	0	0	1	1	2
193	Reemplazo de identificación de terminales móviles	4	2	0	0	3	9
194	Comercialización ilícita de terminales móviles.	24	14	7	285	10	240
195	Infraestructura ilícita	0	5	7	0	0	12
211	Supresión, alteración o suposición de la identidad y estado civil.	52	81	54	23	28	238
229	Revelación ilegal de base de datos.	22	44	34	30	23	153
230	Interceptación ilegal de datos	63	41	86	73	35	296
231	Transferencia electrónica de activo patrimonial	54	37	50	76	170	387
232	Ataque a la integridad de sistemas informáticos	85	86	111	95	86	463
233	Delitos contra la información pública reservada legalmente	14	12	5	5	4	40
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	218	236	242	295	274	1265
366	Terrorismo	12	120	65	13	17	227

Fuente: (Ecuador, Fsicalia General del Estado, 2021)

Como se observa en los datos la tendencia de ciber delitos ha crecido exponencialmente en los últimos años debido a los avances tecnológicos, el uso de redes sociales sumado a la poca educación digital por parte de los usuarios que no tienen cuidado en ingresar sus datos personales en sitios web de fácil acceso a información importante o sitios web poco seguros o no verificados.

Fomentar una cultura de seguridad digital

La Unidad Nacional de Ciberdelitos de la Policía Nacional se ha encargado de realizar charlas, capacitaciones y talleres preventivos a la ciudadanía buscando educar a las personas para que tengan las herramientas necesarias para enfrentarse a los ciber delitos que han incrementado con los años, la idea es prevenir a la ciudadanía para que no sean víctimas de estafas y delitos informáticos, cabe recalcar que muchos de estos delitos son cometidos por el desconocimiento o descuido de las personas por lo cual la labor de la unidad de ciber delitos en tema de prevención es fundamental y juega un rol claro para luchar contra la ciber delincuencia.

Otra medida que la Unidad de Ciberdelitos de la Policía Nacional recomienda para combatir estos tipos de delitos es que las victimas denuncien el hecho para que así la policía nacional pueda hacer las pericias pertinentes, recordemos que el Ecuador mantiene acuerdos con la Interpol y debido que la mayoría de estos delitos son cometidos en otros países remotamente la denuncia es la única forma de luchar contra los ciber delincuentes e impedir que nuevas personas sean víctimas de estos hechos delictivos.

Dentro de la cultura digital se debe realizar capacitaciones a jueces y fiscales en materia de delitos informáticos ya que los ciber delitos al estar en continuo cambio y actualización el conocimiento de los operadores de justicia deben ir de la mano para poder combatir de manera efectiva estos actos ilícitos y evitar que los mismos queden impunes, logrando que las víctimas se sientan seguras y acudan a denunciar.

Cuerpos Normativos en la legislación ecuatoriana para la protección contra delitos informáticos.

1. Constitución de la República del Ecuador
2. Código Orgánico Integral Penal
3. Ley de Comercio Electrónico, Firmas Electrónicas y mensaje de Datos
4. Código Orgánico de la Economía Social de los Conocimientos, Creatividad eInnovación
5. Ley de Protección de Usuarios del Sistema Financiero

6. Código Monetario

Convenio de Budapest

> Es un convenio que se firmó en el 2001 y entro en vigencia en el año 2004 en Hungría precisamente en Budapest de ahí toma su nombre este es considerado el primer tratado internacional creado con el objetivo de proteger a la sociedad de los delitos informáticos, mediante la promulgación de leyes adecuadas para combatir la ciber delincuencia mejorando lastécnicas de investigación e impulsando la cooperación internacional. (Consejo Nacional De Europa, 2021)

En la actualidad más de 50 países se han adherido a este convenio, cada año más países buscan poder adherirse a este convenio ya que la lucha contra la ciber delincuencia es necesaria la cooperación internacional ya que la versatilidad para cometer estos delitos así lo amerita, este convenio nace de la necesidad de la protección legitima de datos informáticos, así como intentar regular el uso adecuado de las TIC's ya que con el desarrollo del internet y las redes sociales los datos quedan expuestos y vulnerables a ataques informáticos.

Al momento es el único convenio internacional que centra sus esfuerzos en la lucha contra el ciber delitos con mayor énfasis en las acciones ilícitas como delitos de odio, pornografía infantil, fraude electrónico e infracciones contra derechos de autor, el convenio de Budapest integra todos sus esfuerzos en la lucha eficaz en contra de los ciber delitos, facilitandosu detección, investigación y sanción tanto a nivel nacional e internacional, integrando accioneseficaces y confiables para una cooperación internacional rápida y fiable.

Este convenio mantiene en cuenta otro tipo de convenios ya existentes y busca integrarlos al igual respetando las leyes penales de sus países miembros ya que su objetivo es incrementar la eficiencia de las investigaciones y procedimientos penales relativos a ciber delitos en síntesis el convenio de Budapest es el instrumento más efectivo en pro de la lucha contra la ciber delincuencia.

Integración de Ecuador al convenio de Budapest

La Fiscalía General del Estado consciente que toda ayuda es válida en pro de la lucha contra los delitos informáticos resalto la importancia de pertenecer a instrumentos internacionales que permitan mantenerse actualizados en materia penal informática siendo así necesario que el Ecuador se adhiera al convenio de Budapest, en este sentido el Ministerio de Relaciones Exteriores y movilidad Humana del Ecuador solicito a la Secretaria del Consejo de Europa poder adherirse a

este instrumento internacional de lucha y erradicación del ciber crimen.

Para poder ser parte de este convenio la secretaria solicito los siguientes requisitos:

1. Contar con legislación que penalice los ciber delitos, además de otorgar facultades investigativas a servidores policiales a fin de poder investigar y obtener evidencia de delitos informáticos.

2. Una vez que se cuente con la legislación solicitada el Gobierno el Ecuador deberá enviar una carta al secretario general del Consejo de Europa en donde exprese su intención de adherirse al tratado.

3. La solicitud queda en consideración de ambas partes y posterior a eso se enviaráuna carta con la invitación para acceder a este convenio.

¿Es importante la adhesión de Ecuador al Convenio de Budapest?

Más que importante a mi consideración es necesario poder ser un País suscriptor del convenio de Budapest ya que la ciber delincuencia ha rebasado la justicia ecuatoriana y al no contar con las herramientas necesarias para combatirlas ha permitido que los ciber delincuenciahaya incrementado en los últimos anos, al ser parte del convenio de Budapest, El Ecuador a través de sus operadores de justicia entiéndase a los mismos como jueces, fiscales y policía nacional reciban la capacitación y herramientas necesarias para la lucha contra el ciber crimen.

Consecuencias de los ciber delitos

Las consecuencias producto de ser víctima de los delitos informáticos son muy drásticas ya que la mayoría de ciber delitos centran sus ataques en contra del patrimonio de las víctimas entre las principales consecuencias esta la alteración del patrimonio pues al ser víctimas de fraude o estafas se realiza perdidas monetarias, en cuanto a los delitos que atacan al derecho a la intimidad sus consecuencias son determinantes ya que pueden dañar el honor y buena honra de las personas derivando en problemas de salud mental como depresión y aislamiento.

Los ataques que se centran en sistemas informáticos de bancos y páginas informáticas que contienen información reservada causas estragos a nivel económico ya que generan pérdidas millonarias ya que inhabilitan sus servicios dejándolos inservibles por un tiempo, tiempo en el cual sus operaciones financieras recaen sumando al nerviosismo colectivo por parte de clientes que ven afectado su patrimonio

El ciber terrorismo tiene como principal objetivo causar inestabilidad en los países que sufren sus ataques informáticos por lo general atacando plataformas informáticas gubernamentales logrando desestabilizar a gobiernos a fin de poder presionar para que accedan a sus peticiones que en mayoría son a nivel político.

A nivel de delitos como la pornografía infantil y oferta de servicios sexuales con menores de 18 años se menciona como principal consecuencia el incremento en los últimos años de estas mafias dedicadas a este delito que aprovechando la innovación de la tecnología la utilizan para cometer actos ilícitos y reprobables con menores de edad.

Detallando todos los delitos informáticos en su mayoría crean problemas de índole económica, social, patrimonial y gubernamental por lo cual es necesario fortalecer la lucha contra la ciber delincuencia que a la fecha actual esta inmiscuida en todas las esferas de la sociedad a nivel mundial, como ya habíamos mencionado los criminales utilizaron y utilizan la tecnología para cambiar la forma de cometer delitos entonces los ordenamientos jurídicos y naciones deben realizar lo mismo a fin de poder frenar y erradicar la delincuencia informática.

Análisis a la propuesta de reforma al art 232 del COIP

La investigadora (Echevería Mera, 2015) en su tesis sobre los delitos informáticos y el derecho constitucional a la seguridad publica propone reformar el artículo 232 del Código Orgánico Integral Penal (COIP) el cual expresa que toda persona que dañe, borre, altere, suspenda, trabe, cause malfuncionamiento, suprima datos con la intención de causar perjuicios y daños las sanciones máximas serán de 5 a 7 años como máximo, la propuesta es aumentar la pena privativa de la libertad a quien incurra en este delito con la intención de realizar chantajes y extorsión a la víctima solicitando así que la pena máxima sea de 9 años.

El objetivo de esta propuesta es que los ciber delincuentes no lucren con el sufrimiento de la víctima ya que en muchas ocasiones debido a los ataques perpetrados las víctimas se sienten en indefensión y a esto sumarle el daño psicológico que sufre la víctima de extorsión o chantajes, esto ayudaría a brindar una seguridad jurídica y una investigación eficaz por parte de las autoridades y organismos competentes.

Me parece excelente la propuesta de la autora de a tesis lo que yo podría sumar o aportar a la propuesta es brindar ayuda y soporte psicológica a las víctimas de este tipo de ciber delitos y también brindar seguridad y protección personalizada a fin de instar a la víctima a denunciar ya

que las víctimas de chantaje y extorsión muy pocas veces acuden a fiscalía a poner la respectiva renuncia por miedo a las represalias.

Consideraciones Finales

Es necesaria la capacitación y educación en materia de TIC's tanto para administradores de justicia como ciudadanía en general con el objetivo de prevención y erradicación de los delitos informáticos, así como también urge la cooperación internacional a fin de poder crear una normativa que proteja a todas las jurisdicciones ya que los ciber delitos tienen como principal característica que pueden ser cometidos remotamente desde cualquier parte del mundo atravesando en su ITER CRIMINIS por varios países hasta concluir con su objetivo ilícito.

A nivel institucional es necesaria de todos los organismos de justicia como fiscalía, Consejo de la Judicatura, jueces integren sus conocimientos a fin de crear un sistema jurídico confiable para las víctimas logrando que cada vez sean más personas quienes se animen a denunciar los actos criminales de los cuales hayan sido víctima.

La Asamblea Nacional a través de sus legisladores debe emprender sus esfuerzos en la creación de un código que abarque de manera más amplia los delitos informáticos a través de leyes que vayan a la par de la innovación y avances tecnológicos que utilizan los ciber delincuentes para cometer sus actos ilícitos en contra del patrimonio de sus víctimas

CONCLUSIONES

1. El Ecuador aún se encuentra relegado en materia de derecho informático ya que no han podido lograr una actualización conforme ha evolucionado las formas de cometerdelitos de los ciber delincuentes.
2. Es claro que hay un gran cambio en la forma de cometer delitos ya que en la actualidad se realizan los mismos delitos existentes en años anteriores solo que hoy esmuy común que realicen con la ayuda de las TIC's.
3. Se debe capacitar a jueces, fiscales, policía nacional y operadores de justicia en materia de Derecho Penal informático ya que en muchas ocasiones el desconocimiento por parte de estos órganos de justicia ha ocasionado que muchos delitos queden impunes ya que por lo general han sido tipificados de manera errónea
4. La Asamblea Nacional del Ecuador a través de sus legisladores deben proponer, discutir y promulgar proyectos de ley que vayan acorde a la realidad tanto de nuestro país y la constante transformación de la tecnología y los conocimientos avanzados que utilizan los ciber delincuentes.
5. Se debe crear un reglamento que contenga todos los tipos penales contenidos en el COIP, pero de manera clara y sencilla para que pueda ser entendido por personas con conocimientos avanzados y para la ciudadanía en general logrando así crear una cultura de denuncia ya que cada vez más personas víctimas de ciber delitos se animen y decidan acudir a fiscalía a interponer la respectiva denuncia.

RECOMENDACIONES

- Se recomienda no ingresar datos personales en páginas web que no tienen una conexión segura
- Se recomienda tener contraseñas diferentes o seguras para aplicaciones bancarias y redes sociales
- Se recomienda que cuando se ha sido víctima de un delito de carácter informático ponerla respectiva denuncia en fiscalía.
- Se recomienda utilizar un antivirus actualizado y con licencia original
- Se recomienda que elimine correos de remitentes desconocidos o sospechosos nodescargue el contenido adjunto a estos correos ya que suele ser malware.
- Controlar el uso de dispositivos móviles y electrónicos en menores de edad

BIBLIOGRAFÍA

Camacho Losa, L. (1987). *Delito Informático.* Madrid: Gráficas Condor.

Consejo Nacional De Europa. (12 de 12 de 2021). *Convenio sobre la ciberdelincuencia.* Recuperado el 15 de Febrero de 2023, de https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Echevería Mera, A. G. (2015). *Los delitos informáticos y el derecho constitucional a la seguridad publica.* Obtenido de Universidad Tecnica de Ambato: https://repositorio.uta.edu.ec/jspui/bitstream/123456789/10034/1/FJCS-DE-802.pdf

Ecuador, Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* Quito: Registro Oficial N° 180 del 10 de febrero de 2014.

Ecuador, Asamblea Nacional. (2016). *Código orgánico de la economía social de los conocimientos, creatividad e innovación.* Quito: Registro oficial N° 899 del 9 de diciembre del 2016.

Ecuador, Fsicalia General del Estado. (14 de 12 de 2021). *Ciberdelitos perfil criminológico*. Recuperado el 3 de diciembre de 2022, de https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

El Comercio. (25 de Julio de 2022). 3183 delitos informáticos se han registrado en el Ecuador, desde el 2020. pág. 3. Recuperado el 17 de Febrero de 2023, de https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Nacionas Unidas. (12 de 04 de 2015). *DPI: Departamento de informacion Publica*. Recuperado el 15 de 12 de 2022, de https://www.un.org/youthenvoy/es/2013/09/dpi-departmento-de-informacion-publica/

Suárez Sánchez, A. (2016). *Manual de delito informatico en colombia analisis dogmatico de la ley 1273 de 2009.* Bogotá: Universidad Externado.