Universidad tecnológica ECOTEC

Derecho y gobernabilidad

Título del trabajo:

El avance normativo del delito electrónico de estafa por medio de las tarjetas electrónicas desde la normativa jurídica en el 2020 y la dificultad para determinar su autoría

Línea de investigación:

Gestión de las relaciones jurídicas

Modalidad de titulación:

Trabajo de investigación

Carrera:

Derecho – Ciencias penales y criminológicas

Título a obtener:

Abogado

Autor (a):

María Fernanda Carrillo Vera

Tutor (a):

Roger Nieto Maridueña

Samborondón – Ecuador

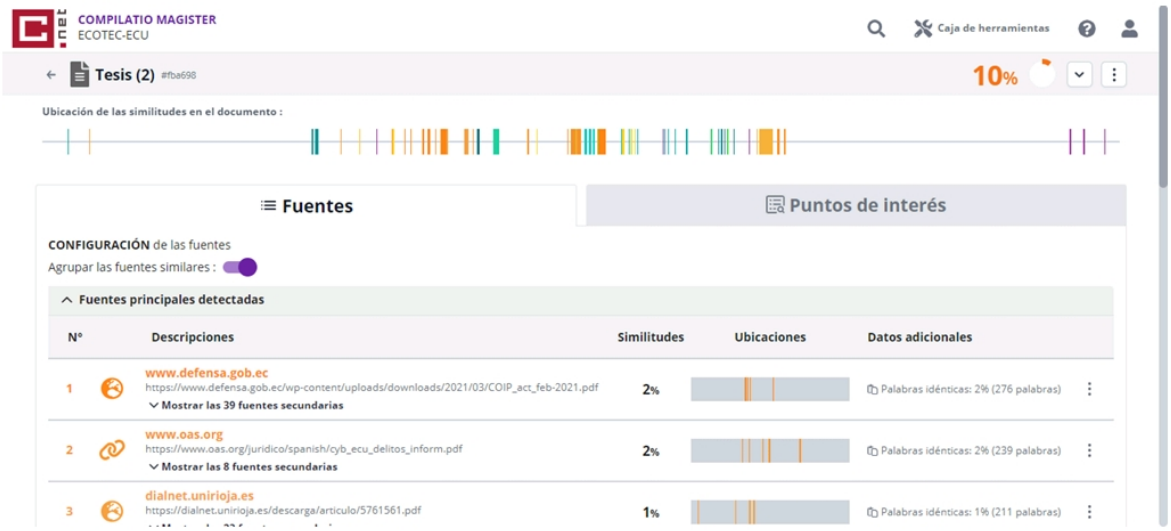
2023

ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado Roger Nieto Maridueña, tutor del trabajo de titulación El avance normativo del delito electrónico de estafa por medio de las tarjetas electrónicas desde la normativa jurídica en el 2020 y la dificultad para determinar su autoría" elaborado María Fernanda Carrillo Vera, con mi respectiva supervisión como requerimiento parcial para la obtención del título de Abogada.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias 10% mismo que se puede verificar en el siguiente link: (https://app.compilatio.net/v5/report/ca8fdb14eae2f613b8880833fd9a072cd9d5777d/sources). Adicional se adjunta print de pantalla de dicho resultado.



Firmado electrónicamente por:
ROGER HECTOR NIETO MARIDUENA

FIRMA DEL TUTOR
NOMBRES Y APELLIDOS DEL TUTOR

ANEXO N°16

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL

Samborondón, 11 de agosto del 2023

Magíster
Andrés Madero Poveda
Decano(a) de la Facultad
Facultad de Derecho y Gobernabilidad.
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: El avance normativo del delito electrónico de estafa por medio de las tarjetas electrónicas desde la normativa jurídica en el 2020 y la dificultad para determinar su autoría según su modalidad PROYECTO DE INVESTIGACIÓN; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **Carrillo Vera María Fernanda,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,

Firmado electrónicamente por:
ROGER HECTOR NIETO MARIDUEÑA

Mgtr/ PhD. Roger Nieto Maridueña

Tutor(a)

AGRADECIMIENTOS

Me gustaría agradecer primero a mis abuelos Imelda y Rodrigo quienes me han criado, cuidado y están guiando siempre mi camino, quienes me apoyan en cada una de mis etapas, a mi padre David, a mis hermanos Rodrigo y Anelisse junto con mi querido Ronald, por haber sido mi motivación e impulso durante este arduo camino.

¡Gracias universidad ECOTEC! por transmitirme tus conocimientos y las grandiosas experiencias junto con recuerdos que me llevo y quedaran plasmados por siempre en mi memoria.

DEDICATORIA

Esto va dedicado a mis padres: Imelda, Rodrigo y David quienes creyeron en mí y son mi claro ejemplo a seguir, personas que me han acompañado de forma incondicional desde el primer momento.

RESUMEN

El fraude informático es un delito que acarrea consecuencias graves para la seguridad jurídica de los ecuatorianos y a su vez sigue en ascenso independientemente de cual se la forma en la que este se produce, se planteó el objetivo de analizar el fraude informático junto con la protección que posee el denominado bien jurídico en. Cuanto a materia penal se trata desde una perspectiva teórica, enfrascado en la metodología de la revisión bibliográfica y entrevista a expertos en el tema cuyos resultados evidenciaron el fraude informático se encuentra tipificado como un delito contra la propiedad, debiéndose destacar la relevancia vital que posee la sanción conforme a lo expuesto por la Convención dada por el Consejo de Europa sobre Cibernética, en el cual se trató este tema entre otros, instalado principalmente en el desarrollo de la la tecnología dentro del siglo XXI, motivo a la legislación penal introducir sanciones a quienes intenten adueñarse de la propiedad de terceros por medios engañosos para conseguirlo. En conclusión, en el Ecuador se ha legislado la penalidad en el fraude informático como un delito contra los bienes por lo que radica la importancia en los juzgadores a la hora de impartir la sanción contra quienes lo cometan.

Palabras clave: Fraude, Documentos, Informática, Protección, Bien Jurídico, Penal.

ABSTRACT

Computer fraud is a crime that carries serious consequences for the legal security of Ecuadorians and in turn continues to rise regardless of the form in which it occurs, the objective of analyzing computer fraud together with the protection that has the so-called legal property in Ecuador was raised. As far as criminal matters are concerned from a theoretical perspective, the methodology was based on a bibliographic review and interviews with experts on the subject, the results of which showed that computer fraud is typified as a crime against property, highlighting the vital relevance of the sanction in accordance with the provisions of the Convention on Cybernetics of the Council of Europe, which dealt with this issue among others, installed mainly in the development of technology in the XXI century, which motivated the criminal legislation to introduce penalties for those who attempt to take ownership of the property of others by deceptive means to achieve it. In conclusion, in Ecuador the criminality of computer fraud has been legislated as a crime against property, so the importance lies in the judges when it comes to imparting the penalty against those who commit it.

Key words: Fraud, Documents, Computer, Protection, Legal Property, Criminal.

Contenido

Introducción

Debido a la creciente ola en delitos electrónicos, a raíz de la pandemia del Covid 19 surgida a principios de año, en marzo del 2020, es propicio analizar los factores que influyeron en esto y cual o cuales son las penas con las que el estado ecuatoriano sanciona este tipo de delitos, puesto que pese a no ser una modalidad nueva para delinquir se conoce poco sobre la materia en cuestión.

Hoy en día por el aumento de la inseguridad que se vive en el país, sobre todo en la zona 8, la mayoría de ciudadanos optan por la utilización de tarjetas a la hora de realizar pagos, ya sean estas de débito o crédito, puesto que lo ven como un método más práctico y seguro al momento de utilizar el dinero por los beneficios que las mismas le brindan, no obstante, no conocen los peligros que esto supone, puesto que la estafa informática y el fraude por medio de tarjetas electrónicas es un delito que va en aumento por el desconocimiento y los avances tecnológicos.

En la estafa informática se suelen dar dos casos que son la clonación de la tarjeta y la duplicación de la misma. En la clonación el objetivo es obtener la información de la misma que se encuentra guardada en la banda magnética por lo que se da el uso de dispositivos electrónicos encargados de alterar, modificar o clonar a los dispositivos originales de un cajero automático para así con esto almacenar la información, copiarla, guardarla de la tarjeta original para así en otra tarjeta en blanco reproducirla, en la duplicación se da la creación de la réplica o reemplazo de la misma de forma ilegal para realizar las operaciones.

Johanna Palacios nos cuenta que la falta de información acerca de los consumos no autorizados, además las barreras presentes en la accesibilidad dentro de las agencias bancarias y ausencia de turnos preferenciales son entre otras algunas de las innumerables situaciones a las que se enfrentan los usuarios con discapacidad ante percances como es la clonación de la tarjeta de crédito (2022).

En un mundo donde la información personal se encuentra sumamente indefensa, las personas deben estar alertas de la inseguridad a la que se encuentran expuestas. El abogado Beltrán nos detalla que aún sigue subsistiendo cierto índice en cuanto a corresponsabilidad entre las mismas agencias bancarias en conjunto con los proveedores de servicios, sus clientes y el estado. Explica que es necesario que todos estos involucrados hagan su parte para disminuir las estafas y los robos (Chejín, 2021).

Según las autoridades, estos estafadores solían enfocarse en personas de la tercera edad, quienes no estuvieran actualizados.” Aunque estas no son sus únicas víctimas. Se registró que el número de denuncias fue en aumento por delitos informáticos, el de estafas cambió de ser de 26.785 en el año 2019 a 27.322 y cintinuó en acenso con 39.147 en 2020 y el 2021” según la Fiscalía General del Estado (2022)

Juan Andrés Guerrero-Saade nos relata un caso sucedido por un turista en Brasil” cuando se encontraba en el aeropuerto a punto de irse, decidió comprar una camiseta de la selección de fútbol. La transacción no fue breve debido a que el empleado de la tienda argumentaba que le denegaban la tarjeta de crédito, por lo que tenía que llevarla a otro datafono ubicado en la parte de atrás de la tienda, una técnica frecuentemente utilizada para ganar tiempo y poder clonar una tarjeta de crédito ajeno a la vista del propietario.” (2014). le robaron 30.000 dólares, pero por suerte el propietario estaba afiliado a un banco americano y pagaba una cuota anual por un seguro contra fraude. Por lo tanto, hicieron honor a sus políticas progresistas que mitigaba su responsabilidad

Muchas veces las personas que sufren este tipo de delito no saben exactamente qué ocurrió o cómo, cuando han oído hablar de esta conducta delictiva generalmente se piensa que la estafa informática es de un solo tipo y solo trata de la sustracción ilegal de dinero por lo que es imprescindible el abordar este tema para despejar dudas y aclarar la importancia de conocer para prevenir y estar informados, dado que cuando es una cuestión de electrónica la ciudadanía se encuentra extraviada en qué esperar.

Planteamiento del problema

El objeto del trabajo de estudio es el investigar el crecimiento normativo que tiene la legislación ecuatoriana en este tipo de delitos, enfocado en la estafa informática, cual es la sanción impuesta por el estado.

Actualmente bastante parte de la población desconoce sobre los delitos electrónicos y con la nueva ola de avances que surgieron en el país con impacto producto de la pandemia producida muchos se encuentran desconcertados sobre el tema, puesto que se desconoce el trámite, tiempo o como son los procesos que se siguen, por lo cual la necesidad es de conocimiento en el tema, por eso la problemática nos plantea si ¿en Ecuador las leyes establecidas en el COIP son suficientes a la hora de sancionar delitos electrónicos?

Investigar el delito desde cualquiera de las aristas es sin duda alguna una tarea compleja. Las dificultades que se presentan a la hora de tratar de instaurar el método científico a la delincuencia transnacional, al igual que al crimen organizado, estos mismos ya fueron estipuladas cuando se realizaron estudios previos, no obstante, cuando se desea o se requiere de enfrentar a este tipo de delincuencia en todo nivel es una ardua labor la que batalla y se expone el Ministerio Público por medio del mandato constitucional y la disposición legal. Y bien, el fenómeno que fue expuesto ahora últimamente ha tenido una visible creciente y esto tomando en consideración la manifestación que posee la globalización, esta que únicamente no solo se ha beneficiado, sino que por el contrario la misma ha contribuido en toda la masificación de este tipo de delitos y tecnificado a otra clase cómo son los catalogados delitos informáticos (Pino).

Según Luís Enrique (2021) “Por otra parte, queda al descubierto la falta de preparación de la administración de justicia ecuatoriana en cuanto a delitos cibernéticos. Las acciones equivocadas de la fiscalía no deberían repetirse en el futuro, sobre todo considerando la acelerada transformación digital que vivimos”. El Ecuador tiene ya antecedentes nefastos en cuanto a la protección de los derechos humanos de los ecuatorianos en entornos digitales, entre ellos, el caso de la empresa italiana *Hacking Team,* empresa que brindaba servicios de hacking a varios Gobiernos latinoamericanos, incluido el ecuatoriano. La información de este caso fue revelada en el año 2015, y puede ser consultada de manera abierta en el portal wikileaks.

Hasta ahora se conocen los diversos tipos de delitos electrónicos, su categoría, las características del mismo, de que tratan estos junto con el bien jurídico protegido que estos atacan y su respectiva sanción.

El ataque se realiza desde cualquier sector del planeta, lo que le brinda al ciberdelincuente diversos beneficios". Según Centeno "Si examinamos estas ventajas podemos destacar lo siguiente: el ciberatacante se siente tranquilo, ya que este no se expone físicamente frente a su víctima y menos a la posible participación de las fuerzas de seguridad, dado que se produce a distancia brinda sensación de paz e impunidad, al saber que existen lagunas legislativas a nivel internacional por lo que varios de los delitos cometidos quedan impunes" (J & Centeno, 2015)

A partir del desarrollo acelerado de internet, también sale el lado oscuro y se presentan nuevos términos como cibercriminal, ciberdelito o ciberdelincuencia, lo que puntualiza de forma genérica o amplia los aspectos ilícitos cometidos en el ciberespacio, que presentan características específicas: "el fácil cometimiento; requieren pocos recursos con relación al perjuicio que provocan; se pueden cometer en una jurisdicción sin estar presente en el territorio y por ende estos son quienes han salido favorecido de la existencia de las catalogadas lagunas de punibilidad que puedan estar presentes en determinados y diversos estados, estos han sido llamados paraísos cibernéticos, por la escaza o nula voluntad política que poseen para tipificar y sancionar estas conductas delictivas" (Subijana Zunzunegui, 2008)

Se dice que el cibercrimen a sido un término que a sido ampliamente discutido y tratado desde diferentes enfoques tanto teóricos como tecnicos técnicos, en el derecho, en la criminología, en la informática, en la sociología y otros diversos análisis que han intentado de poder encasillarlo en categorías como el delito transnacional, el ciberespacio, la ciberseguridad y por último la sociedad de la información. Esta es una figura tanto social como global que aumenta con gran velocidad, de tal forma que igusala a las tecnologías de la información, por ende, sus desafíos globales han concluido solamente en discusiones académicas en torno de los temas de identificación, jurisdicción, regulación y tratamiento (Marcillo, 2021)

Falta mayor información sobre el tema, en lenguaje coloquial para que esta pueda ser entendible a todas las personas y no únicamente sea dirigida a los especialistas o estudiosos de la materia, de esa forma se podrá alertar a la ciudadanía para estar preparada y saber cómo actuar en caso de ser víctima de este tipo de delito, se espera conseguir con el trabajo una explicación sobre este tipo de procesos, en qué consisten

Objetivos

Objetivo general

Identificar en que consiste el delito de estafa informática por medio de tarjetas electrónicas y su alcance al igual que su conjunto de leyes aplicables en la sanción de la misma, junto al proceso legal llevado a cabo para determinar la penalidad además de su objetivo y modus operandi.

Objetivos específicos

Observar el aumento de la figura delictiva en el periodo 2020 – 2022

Determinar el ciclo delictivo de la estafa informática

Establecer el tipo objetivo del delito de estafa informática y las dimensiones

Justificación

Con el paso de los años el índice delictivo de la ciudad ha ido en aumento," el foco de esa violencia se centra en Guayaquil, catalogada como la ciudad costera más importante, que, además, empuja gran parte de la economía por poseer cinco de los ocho puertos del país y que históricamente han captado una notable migración interna que busca oportunidades de mejor vida. No obstante, las políticas públicas de la ciudad no han respondido como se esperaba en relación al crecimiento poblacional, y lo que provocó exclusión a los barrios de las obras públicas, y se convirtió en un búnker para grupos delincuenciales", dice Aquiles Álvarez.

La dinámica de vida de la población ha cambiado significativamente debido a estos sucesos, buscan estar seguros por lo que ahora se adopta la modalidad virtual para la mayoría de trámites, están páginas webs, apps y demás e incluso ahora para actividades diarias como almorzar se usa de internet, por lo que la estafa representa un peligro a la población, este tipo de delito no es nuevo, no obstante, cogió incremento debido a la era de la tecnología, no hay solo una forma en la que el delito se produce, por el contrario son varias las conocidas con links falsos, correos engañosos o llamadas telefónicas.

Si la ciudadanía conoce la forma en que se produce el cometimiento, los mecanismos que estas personas suelen emplear para producir estos actos, el modus operandi y su tipo de victimología estarán más prevenidas y el índice de estos crímenes bajaría, por ejemplo se sabe en la

actualidad de los correos nigerianos como un tipo de estafa, por lo que las personas ya se encuentran atentas sobre esto puesto que se tiene información de correos donde se estipule de la ganancia de la lotería, premios donde no se ha inscrito deben ser ignorados puesto que solicitan información personal como datos bancarios para cometer fraudes

A su vez se conoce sobre revisar bien el remitente de un correo por los casos vistos en que el ”Banco Pichincha” pide información confidencial y privada para “confirmar la seguridad del usuario“ por lo que ahora se revisa bien los datos del correo, se llama a confirmar o inclusive las mismas instituciones bancarias crean anuncios dirigidos a sus usuarios sobre seguridad para que no sucedan este tipo de eventos y evitar que terminen perjudicados.

CAPÍTULO I: Marco teórico

A continuación, se abordarán diversos temas vinculados al objeto de estudio con el único objetivo de entender la vital importancia que tiene la informática en nuestra actualidad y los peligros que trajo consigo su crecimiento y desarrollo tecnológico. A su vez, se procederá a analizar el tema principal de esta tesis, que es la estafa informática y lo que se ha sucedido por esta figura en el Ecuador durante los últimos cinco años, su historia en el país. Finalmente, se ha examinado dentro del Código Orgánico Integral Penal conocido por sus siglas COIP, del Ecuador, así como las penas que son impuestas al cometer este delito, al igual que el derecho comparado.

1. La delincuencia informática

Los nuevos avances tecnológicos junto con la llamada sociedad de la información y comunicación, como en cualquier otra vertiente de la sociedad van a influir en la esfera propia de la criminalidad, la cual es inseparable de los parámetros sobre los que se desarrolla la sociedad, ajustando sus formas de operar a las posibilidades que ésta les ofrece. De esta forma la era de la informática, además de beneficiar la actividad en diversos aspectos de la información y campos de desarrollo ha generado a su vez nuevas formas de cometimientos en actividades delictivas.

Las vertientes vinculadas a la telemática, junto con la irrupción de internet como una red de redes de alcance a nivel global, ha generado no solo una inmediatez en la respuesta, sino posibilitó brindar acción pese a la distancia, que brinda de eficacia tanto a la actividad criminal como al derecho punitivo de los Estados, lo cual crea estragos. Pese a eso la actividad ilícita vinculada con la telemática no siempre supone el nacimiento de nuevos bienes jurídicos a proteger

En la mayoría de casos, el bien jurídico protegido que se encuentra vulnerado a consecuencia del uso de las nuevas tecnologías es un bien jurídico tradicional, el cual ya es conocido para el derecho penal. Son las recientes formas de lesión a estos valores fundamentales para la sociedad los que se ven desfavorecidos por las innovaciones tecnológicas.

1.1 La informática

En el Diccionario de la Real Academia Española, la determina como el conglomerado de conocimientos científicos y técnicos, que hacen posible el tratamiento automático de información mediante los computadores, es catalogado también una ciencia enfocada al estudio de métodos, procesos y técnicas, con el propósito de almacenar, procesar y transmitir

información y datos de forma digital, que se ha desarrollado con rapidez a partir de la mitad del siglo XX con el nacimiento en tecnologías tales como al circuito integrado, internet y el teléfono móvil. (española.)

Konrad Zuse, ingeniero alemán que además fue uno de los principales pioneros de la computación, define a la informática como "la instrucción que examina el tratamiento automático de la información por medio de dispositivos electrónicos y los sistemas computacionales." (Falcón, 2022). A su vez diversos autores expresan como la ciencia que analiza el tratamiento de la información o también como la ciencia de la información automática.

1.1.1 Reseña histórica de la informática

Todo empieza con la búsqueda del hombre por tener dispositivos que le ayuden en la vida cotidiana a ejecutar cálculos más precisos y rápidos, Pibanck dice que ”es cuando los chinos que desde hace aproximadamente más de 3000 años a C. desarrollaron el ABACO, que les brindaba cálculos más rápidos y complejos, catalogada como una herramienta de grabación de cálculo numérico” (2020), en 1614 John Napier anunció su descubrimiento de logaritmos, logrando que los resultados de multiplicaciones se abreviaran a un proceso de suma, tiempo después se logro la invención del objeto llamado la regla de calculo dentro de los años 20, basada en los principios matemáticos que fueron descubiertos por Napier.

En 1642, Pascal crea una máquina mecánica dedicada a sumar que era parecida a los cuenta kilómetros usados en los automóviles, pero presentaba inconvenientes con sumas largas y en 1971 Leibnitz añadió otra función que fue la posibilidad de restar, sumar, multiplicar y dividir, su máquina estaba formada encima de ruedas dentadas y cada una de estas ruedas tenía diez dientes, estos correspondían a los números de 0 al 9. La calculadora de Blaise Pascal exigía intervención del operador, ya que debía escribir cada resultado parcial en una hoja lo que era largo y por lo tanto genera errores en informes.

Charles Babbage desarrollo la primera calculadora, llamó al descubrimiento “Máquina de las diferencias”, considerado el primero en la informática. En el año de 1833 se surgió un segundo invento, la máquina que le llevó 20 años. En 1930, el norteamericano Vannevar Bush diseñó el material electrónico cuyo nombre es el analizador diferencial, siendo así el inicio de nuestra era de computadoras. La primera computadora considerada completamente electrónica fue la ENIAC por sus siglas significaba Electric Numeric Integrator And Calculator, que fue

construida en el año 1943 y 1945 por dos personas que fueron John Manchi y J. Proper Eckut. lograba multiplicar mil veces más rápido que la máquina de AIKEN.

Es una rama del derecho la informática jurídica, la cual está encargada del estudio y análisis de datos e información ubicados y contenidos en documentos de carácter jurídico empleados en la realización de archivos documentales, como ejemplo de esto se encuentra la acerca de un expediente a por medio del sistema judicial de expedientes. La computadora con su infalible y basto amplio banco de información jurídica sea idoneo para brindar los resultados sobre algún caso existente.

Peña nos cuenta que" se compone de un extenso abanico de normas encargadas de regular diferentes materias las cuales van desde los delitos cometidos mediante los medios informáticos hasta los que son en derechos de propiedad intelectual e inclusive encaja también el tratamiento y protección de datos personales" (2021). Por ello la esfera de aplicación del derecho informático es extensa. Además de los delitos que son efectuados a través de medios informáticos, también se buscará proteger la privacidad, el honor e imagen de las personas en uso y mediante el Internet, busca resguardar los datos personales y los también catalogados como sensibles, crear un marco seguro para la publicidad online, brindar un espacio positivo para el uso de redes sociales, operaciones en comercio electrónico junto con trámites telemáticos por medio de firmas y certificados digitales, etc.

Una de las normas que forman parte del bloque que compone el derecho informático es el Código Penal el cual es el encargado de reunir aquellas acciones catalogadas como delitos informáticos entre los cuales se encuentra: el fraude mediante el uso de ordenador, el uso no autorizado de datos y sistemas informáticos, la destrucción de programas y datos, el ciberacoso, mientras que La Ley de Protección de Datos Personales y garantía de los derechos digitales es otro texto indispensable en este ámbito, se dedica a regular el tratamiento de los datos personales y la Ley de Propiedad Intelectual establece los mecanismos para responder a las vulneraciones de estos derechos al igual en el entorno digital.

El primer concepto sobre Derecho Informático fue otorgado por El profesor Dr. Wilhelm Steinmüller de la universidad de Regensburg en Alemania en los 70s. No obstante, no se trató de un concepto con una exclusiva interpretación, se centro en el estudio del derecho telemático y otros términos como, derecho de las nuevas tecnologías y derecho de la sociedad de la Información. Se lo conceptualiza como una perspectiva de inflexión en el derecho, debido a que todas las áreas del mismo se han visto de alguna manera perjudicadas y vulneradas por la

catalogada sociedad de la Información, alterando los procesos sociales y por ello los procesos políticos y jurídicos. Se hace la aparición el derecho informático como un cambio puesto que desde la aparición de la computación como un fenómeno ha sido beneficioso en distintas áreas de la ciencia y cultura.

La tecnología ha sido ayuda para el ser humano, no obstante, ahora los delincuentes utilizan este medio para consumar sus actos delictivos. Por definición general el derecho debe ir a la par en la evolución con las necesidades del ser humano, sus costumbres para así gestionar las nuevas relaciones que surjan. Por ello nació el Derecho Informático, que se comprende como la agrupación de normas objetivas destinadas a mediar los actos que surjan producto del uso de la informática.

El surgimiento de la información ha generado la diversificación de los procesos jurídicos, así como juicios, pruebas, evidencia, medios de delinquir, etc. A causa de la informática el derecho se ha quebrantado es en dos ramas clásicas del derecho, el derecho civil y penal. En derecho penal, se enfrenta un desafío dado la penalización y categorización de los delitos, puesto que el delito se lo a denominado como una conducta y dicha conducta es penalizada por las leyes de defensa social, no puede aplicarse pena alguna que no esté predefinida en la Ley.

1.1.3 La tipificación del delito informático en la ley penal ecuatoriana

El delito informático está tipificado en el COIP, que desmenuzando las siglas es el Código Orgánico Penal Integral del Ecuador, el cual fue aprobado en el año 2014, no obstante," desde el 2009 en el país se empezó a hablar sobre estos delitos y a pesar de que se conoce, el 80% de los delitos informáticos no son eran, en cuanto al índice delictivo en aquel entonces. lo que a juicio de la ONU era consecuente por la falta de una cultura de denuncia" (comercio, 2022)

Dentro del artículo 190 establecido en el Código Orgánico Integral Penal en base a lo establecido como delito expone que es el uso de un sistema informático, al igual que de redes electrónicas y de las telecomunicaciones para beneficiarse mediante la apropiación de un bien ajeno o de igual forma este procure la transferencia no autorizada de bienes, valores o derechos que causen un perjuicio a un tercero, en beneficio propio o de otro mediante la alteración, a su vez también se integra la manipulación junto con la modificación del correcto funcionamiento de redes electrónicas al igual aquí se integran si atacasen programas, los sistemas informáticos, telemáticos junto con equipos terminales de telecomunicaciones y esto será sancionado con una pena privativa de libertad que será de uno a tres años".

En el 2014 el delito de la estafa informática se encontraba ubicado en el COIP en el Art. 553.2 ”Los que usen engañosamente los sistemas de información o redes electrónicas, para posibilitar en la apropiación de un bien, valor o derecho ajeno en afectación de ésta o algún tercero, provocando alguna utilidad para el en el funcionamiento de las redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos” (NACIONAL R. D., Código Orgánico Integral Penal, COIP) Pena específica 6 meses a 5 años, la multa es de $500 a $1000 dólares, los autores podrán ser establecidos bajo la observación especial de las autoridades a cargo dentro de un periodo de 2 años a 5, sin contar con las circunstancias modificatorias no constitutivas.

1.1.4 Causas de crecimiento del delito

Sin duda fueron diversos factores los que influyeron en esto, como principal está la dependencia a los dispositivos electrónicos y los pocos mecanismos de seguridad que se tiene en los mismos, ”cuando esto sucede en una empresa por lo general no reportan el delito, lo cual se debe al temor de pérdida reputacional, que conduzca a la fuga de clientes y afecte a los negocios e inclusive las relaciones con otras empresas” (Zulia, 2020).

En nuestra actualidad la informatización se ha implantado en la mayoría de los países. Yamilka Estrada Cabrera y Everardo Luis Ramos Alvarez nos exponen que esto surgió “tanto en la organización, en la administración de empresas, junto con administraciones públicas de igual forma en la investigación científica, junto con la producción industrial, el estudio e incluso para disfrute y descanso personal, el uso de la informática es en determinadas circunstancias indispensable y hasta considerado conveniente” (S/f). Sin embargo, junto a laos incuestionables avances que supone empiezan a emerger diversos aspectos negativos, como, por ejemplo, lo que ya se conoce como “criminalidad informática”

1.1.5 Nuevas tecnologías y la criminalidad transnacional

Uno de los principales problemas de este tipo de delitos es la inmediatez del resultado y la distancia con la que se puede ejecutar la actividad, una de las características del mismo es la jurisdicción y competencia, la cual trata en que se actuar en cualquier lugar del mundo desde distancias remotas valiéndose de un dispositivo, pudiendo provocando daños en otras partes, lo que obliga a los estados a cooperar para ejecutar su persecución. Al contar con valiosos recursos, la delincuencia organizada se vuelve más compleja de detectar, el uso de tecnología en delitos de tráfico, como realización de fraudes en y mediante Internet, representa ganancias multimillonarias para la industria criminal.

En los últimos años estos delitos se han destacado por la diversificación de sus actividades ilícitas dada a la globalización económica y comercial, el tema de los flujos internacionales de personas, además la desaparición o escases en controles fronterizos, junto con la aparición de nuevos mercados, la producción en comunicaciones y el auge de la Internet ha sido puesto al servicio para los grupos criminales para la expansión de sus actividades y formación de alianzas para delinquir.

El principal instrumento internacional en la lucha contra este fenómeno es la Convención de las Naciones Unidas contra la delincuencia organizada que va a nivel transnacional, la misma que entró en vigor el día 29 de septiembre del año 2003 y que la misma ya ha sido ratificada por más de cien estados que son miembros de la Organización de las Naciones Unidas

1.1.6 Historia evolutiva del delito electrónico en Ecuador

En los últimos años el Ecuador se ha visto inmerso en una serie de profundas transformaciones tanto económicas como políticas y sociales. En la Constitución del 2008 se exigen obligaciones inaplazables y urgentes como los es la revisión del sistema jurídico para así cumplir con el imperativo deber de brin justicia y certidumbre a los ecuatorianos (Asamblea Nacional, 2008).

En Ecuador a partir de su época republicana se han promulgado cinco Códigos Penales que fueron en los años: 1837, 1872, 1889, 1906 y 1938. La legislación penal que se encuentra actualmente vigente es una codificación más y que posee una fuerte influencia del Código italiano de 1930 que fue conocido como "Código Rocco", a su vez el argentino de 1922 y el belga de 1867 el cual a su vez del francés de 1810 "Código Napoleónico". En suma, tenemos un Código desde hace dos siglos con la influencia" trágica del siglo XX, que es la Ley penal del fascismo italiano.

El Código Penal COIP que se encuentra vigente se localiza antiguo, inconcluso y corregido ha sido constantemente modificado. La codificación de 1971 ha soportado aproximadamente cuarenta años desde octubre de 1971 hasta la que fue dada en mayo del 2010, en la que se han presentado cuarenta y seis reformas. A esto se deben agregar las más de doscientas normas no penales que a su vez se encargan de tipificar las infracciones.

En materia de procedimiento penal el Ecuador ha tenido más de cinco leyes. El Código de Procedimiento Penal se encuentra vigente desde el año 2000, lo que generó una variación vital en relación con el procedimiento de 1983 que se basaba en el sistema acusatorio. No obstante, no fue de sencillo de poder aplicar y pasó múltiples modificaciones. Para resumir el Código

penal ha sido reformado catorce veces. Reformas las cuales no tomaron en consideración a las normas penales sustantivas que son las cuales tienen una finalidad propia, subsistente por sí, fijando las reglas de conducta y deberes de cada cual, y por lo que únicamente estos intentaron modificar el sistema penal, cambiando únicamente una parte suelta.

La asamblea nos cuenta que el Código de Ejecución de Penas, fue publicado por primera vez en 1982 y desde allí este a sido reformado en un total de diez veces. Las normas penales de ejecución vigentes en aquel entonces que fueron creadas sin previamente considerar a las normas sustantivas y procesales, por lo que las mismas fueron inaplicables debido a su inconsistencia. Técnicamente no se puede rehabilitar a una persona que nunca ha sido "habilitada", por ende ni reinsertarla en una sociedad que tampoco se encuentra idonea para la reinserción (2023).

Se añade que el sistema unicamente funciona solo si cuenta con la verdadera voluntad de las personas condenadas, cosa que ha originado en definitiva los espacios propicios para el surgimiento de la violencia y la corrupción. Es muy notable que las normas sustantivas, procesales y ejecutivas penales vigentes no responden unicamente a una sola línea de pensamiento. Sus contextos históricos han sido variados. Las finalidades y estructuras son diversas, sin coordinación alguna, inclusive contienen normas contradictorias. Esto se reduce a la obtención de un sistema penal incoherente y poco práctico.

Páez Rivadeneira expuso que “dentro el Código Penal Ecuatoriano en materia de Delitos Informáticos siempre han existido deficiencias graves y pese a que el uso de tecnología dentro del país es nuevo (lo que se entendía como pretextos), y sumado a la prevención del tema, la cual no ha sido la más propicia” (2010).

No obstante, hubo un gran avance el cual fue La Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, esta fue promulgada en 1999, “dicha ley representó un gran avance en cuanto a la búsqueda de un sistema jurídico que genere confianza a los usuarios de la tecnología. A su vez en el año del 2002 se agregó a la ley cambios que fueron considerados como interesantes en el incompleto paisaje de los delitos informáticos” (Rivadeneira & Pino, Derecho y nuevas tecnologías , 2010).

Según el artículo 190 del código orgánico integral penal “El uso de un sistema informático o redes electrónicas y de telecomunicaciones para ayudar en la apropiación de un bien ajeno o que la misma procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o un tercero, en beneficio suyo o de otro alterando, manipulando o modificando el

funcionamiento normal de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será castigado con una pena privativa de libertad de uno a tres años" Código orgánico integral penal de Ecuador [COIP]. pag. 52 (Ecuador).

La tipificación del delito informático en la ley penal ecuatoriana en Ecuador surgió en el 2009, donde se comienza a dialogar de delitos informáticos, pudiendo registrarse hasta en el año 2013 un total de 3,143 casos, esto a pesar de que solamente se conoce que el 80% de los delitos informáticos dado a que estos no suelen ser son reportados, en cuanto al índice delictivo, estos delitos están tipificados en el COIP del Ecuador aprobado en el año 2014.

El desarrollo de la investigación argumenta que la tipificación de los delitos es lo que ha permitido sancionar con mayor rigurosidad a delitos vinculados que se encuentran vinculados con la estafa informática, de igual forma existen otros pensamientos los cuales mencionan que las sanciones establecidas por los delitos informáticos se deben endurecer, dada la gravedad de las características con las que se produce el cometimiento de estos tipos de delitos.

Actualmente se ha demostrado que la difusión entre la población sobre que tratan este tipo de delitos, los informáticos, es escasa, lo que acarrea que el delito no sea denunciado (ecuatoriano, 2015). La mayoría de los expertos del tema, explican que, por las características del mismo, el delito informático es difícil de comprobar, por ello surge la necesidad de que el personal que garantiza esta actividad posea el basto conocimiento y la experticia para poder detectar en cualquiera que fuera el caso planteado la existencia a una violación en la seguridad informática o en sus sistemas, lo que incurriría en el delito informático.

Por ende se considera imprescindible la creación de juzgados especiales para la atención de estos delitos. Es necesario señalar que el derecho informático en el campo penal es importante, porque de esta manera se sanciona a las personas que conculcan garantías que le asiste a las personas y de los cuales precautelan del derecho informático (María, 2014).

Es de vital importancia que junto al avance del delito vaya a la par la tipificación del mismo, de esta forma se garantiza que al cometimiento de la conducta típica antijurídica y culpable no se deje en indefensión a la víctima del delito. Uno de los principales problemas existentes en la ciudad de Guayaquil, es que no se dispone con personal especializado, y que este mismo se encuentre correctamente acreditado por el Consejo de la Judicatura, para realizar pericias pertinentes en delitos informáticos.

El 29 de marzo del presente año 2023 se incorpora una serie de importantes agregados para el contenido digital en base al realce que tiene la cooperación internacional entre países para luchar contra la ciber delincuencia .

1.17 Peritos

El Perito es una fuente confiable en determinado campo de estudia, una persona con formación, capacitación, conocimientos y experiencia en una ciencia o ámbito técnico, el testimonio del mismo puede ayudar en la resolución de conflictos ya sea en la vía prejudicial o judicial. Brindará su conocimiento a la hora de resolver dudas en determinado tema, se encuentran registrados en el consejo de la judicatura.

Entre las cualidades del perito está el actuar de forma limpia y transparente, este actúa fuera de los intereses personales, no se pondrá de una parte ni brindará juicios de valor, dando una respuesta objetiva sobre el examen efectuado en la materia que se especialice y respondiendo las dudas en el mismo, debe respaldar lo vertido por el por medio de pruebas y respaldar lo escrito en el mismo a la hora de la audiencia, tendrá mínimo dos años de haberse graduado y dos de estar ejerciendo la actividad. Se dividen por especialidades.

1.1.8 Peritos informáticos

son quienes están encargados de otorgar el soporte tanto a particulares como empresas u organizaciones al momento de la hora de presentación de pruebas tecnológicas ante un tribunal, estos son los ñunicos encargados de analizar la veracidad y fiabilidad de dichas pruebas recopiladas y por ende son quienes deben de exponerlas de forma clara y sencilla para que estas puedan ser comprendidas ante el juez, se encargan de extraer la información de los dispositivos y sistemas electrónicos con la misión de realizar análisis forenses, analizar las pruebas, extraer conclusiones y elaborar los informes pertinentes en base a dicha investigación, para su posterior presentación ante un tribunal.

Cuenta Tablado que esto se usa en dichos casos en los que se sospecha o se tiene la certeza de que se ha ejecutado el uso inadecuado de la tecnología, se ha generado una brecha de seguridad en un sistema informático, o de que los mismos soportes informáticos han sido el medio para el cometimiento de un delito, como por ejemplo en casos de revelación de secretos o violación de la propiedad industrial, en intruciones ilegítimas en la intimidad de las personas, en los accesos ilegales a documentos o a su vez ficheros de la empresa, también se lo aplica en la competencia desleal realizada por parte de un empleado o ex empleado, interceptación de

comunicaciones, acceso o manipulación ilegítima de software, estafas y fraudes a través de soportes digitales, etc" (2020).

En Ecuador el consejo de la judicatura posee peritos en informática forense e Informática y Telecomunicaciones quienes son los encargados de los análisis de sitios y páginas web, en cuentas de correos electrónicos, el análisis físico y lógico de equipos de cómputo además en sistemas informáticos y dispositivos de almacenamiento identifica los procesos y los delitos informáticos los autores del fraude, no obstante, pese a sus atribuciones y alcances requeridos no se logra cumplir con ellos, los peritos que deberían cumplir con lo establecido no puede por su falta de conocimientos en el área.

El tema de procesos informáticos es amplio y los peritos quienes cuentan con título de ingeniería en sistemas no cuentan con la experticia necesaria para cumplir con su deber, el Comercio señala que "en el proceso de selección en el cual se halló una carencia en esta clase de profesionales. Como por ejemplo en las ciudades de Bolívar, Cañar o Carchi, son territorios en donde no se cuenta con peritos informáticos registrados puesto que los postulantes no han logrado superar las pruebas técnicas o los cursos de formación inicial" (2018).

El Ecuador al igual que otros países de Latinoamérica tiene una brecha en la adquisición de la tecnología en comparación a los países desarrollados lo que se amplía debido a que no genera su propia tecnología, sino que la adquiere lo que genera una situación de dependencia lo que da por resultado que no se cuente con las herramientas propicias al momento de indagar.

1.1.9 Sujetos activos del delito informático de estafa

Los sujetos activos en delitos informáticos son quienes comenten el delito, algunos delincuentes de cuello blanco, no ejercen fuerza, es por conocimiento o estatus social que lo cometen, en el perfil de las personas que cometen estos crímenes, en especial el fraude financiero se cree que poseen habilidades destacables para el control óptimo de sistemas informáticos y generalmente su lugar de trabajo brinda una posición estratégica para acceder a información sensible, al igual se considera la posibilidad que no necesariamente posean una posición laboral favorable para el cometimiento del delito.

Según un estudio publicado en el Manual de las Naciones Unidas para la prevención y control de delitos informáticos, el 90% de delitos en que se utilizó como medio una computadora, fueron ejecutados por trabajadores de la misma empresa que fue afectada, estos son catalogados como" Insiders". De la misma forma de acuerdo con una investigación que fue realizada en

América del Norte y Europa las actividades ilícitas informáticas eran causadas más por trabajadores del interior de dicha institución afectada y solo de 23% provinieron de actividades externas estos son catalogados como" outsiders". (Humanitarios., 1994)

El uso descuidado del Internet refleja las vulnerabilidades de los sistemas informáticos, sobre todo aquellos utilizados por las instituciones financieras, es una realidad que cada día se va demostrando, es más frecuente que el delito del fraude financiero informático tenga una fuente a larga distancia que fuente interna, de esa forma el sujeto activo del delito tiene diferentes caras, se ha evidenciado que los autores de los delitos informáticos son extensos y lo que marca una desigualdad entre ellos es la naturaleza del delito cometido, de tal forma que quien daña un sistema informático es opuesta a la que tiene el trabajador de una institución financiera que desvía los fondos de las cuentas de los usuarios de dicha institución.

El nivel de habilidad que posee el delincuente informático es catalogado un tema que genera discusión ya que para algunos esto no es precisamente un indicador del índice delincuencial informático pese que para otros individuos los posibles delincuentes informáticos son exclusivamente personas con un vasto y extenso conocimiento en la materia con cualidades de ser decididos, motivados y dispuestos a aceptar un desafío tecnológico, características que pueden estar en un trabajador del sector financiero o procesamiento de datos.

1.1.10 Sujetos pasivos del delito informático

El sujeto pasivo en el fraude financiero informático, es la víctima, quien se ve perjudicada por la conducta cometida por el sujeto activo, es decir por la apropiación ilícita del dinero depositado en la entidad financiera. En delitos informáticos los sujetos pasivos pueden ser individuos, los mismos podrían estar como a la vez no en instituciones financieras, dentro de los gobiernos, etc., las personas que utilizan sistemas automatizados, que por lo general mayormente se encuentran enlazados mediante Internet.

Por lo que es improbable el determinar el impacto que poseen este tipo de cometimientos, puesto que la mayoría de estos actos no suelen ser descubiertos y peor aún ser denunciados, las víctimas al enterarse que fueron agraviados, no sacan a la luz pública, debido a la desconfianza en el sistema de justicia actual, o la vergüenza que provocaría para unos que se enteren sus conocidos que fue víctima de estos actos, ocasionando que se conviertan en pérdidas económicas, de tal forma que los números nunca reflejaran la realidad oculta.

El sujeto pasivo es el titular del bien jurídico protegido y sobre este recae la actividad típica del sujeto activo, dentro del tema principal de este proyecto de investigación el bien jurídico que se debe resguardar es el dinero delegado al cuidado de las instituciones financieras, el sujeto pasivo ayuda a identificar el modus operandi de los sujetos activos quienes cometen los fraudes financieros.

1.1.11 Bien jurídico protegido de la estafa

El objeto jurídico es el bien que fue violentado o también puesto en peligro por la conducta que tuvo el sujeto activo, Jamás debe dejar de existir ya que constituye la razón de ser del delito y no suele estar expresamente señalado en los tipos penales. (PINO, 2016) Dentro de los delitos informáticos, la tendencia es que el resguardo a los bienes jurídicos, se le realice desde el mismo enfoque que presentan los delitos tradicionales ya conocidos esto sí, con una re-interpretación teleológica de los tipos penales ya conocidos y previamente existentes.

para intentar subsanar las lagunas originadas por los novedosos comportamientos delictivos. Esto sin duda da como norma global que los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su segimiento y sanción por parte del órgano jurisdiccional competente

1.1.13 El delito de Estafa informática

El nuevo Código Penal a introducido el concepto de fraude informático, el cual consistente en la manipulación informática o artificio similar que, concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. El Código Penal anterior exigía la concurrencia de engaño en una persona, lo cual excluía cualquier forma de comisión basada en el engaño a una máquina. Los delitos de estafa, pueden llegar a agravarse si el perjuicio causado es contra la propiedad del estado.

Es considerado durante estos últimos años como el delito informático más común. Se configura cuando la persona utiliza ilícitamente un sistema informático o las redes electrónicas para adueñarse del bien o patrimonio ajeno, de transferencias de dinero o bienes no consentidos en perjuicio de una persona. Se sanciona con cárcel de uno a tres años, según el artículo 190 del Código Integral Penal (COIP).

Para contrarrestar estos actos delictivos, y bajar la tasa delincuencial la Policía ejecutó 38 operativos en dos años y medio, como resultado se detuvieron a diversas personas que

probablemente cometieron ciberdelitos. En el año 2021, otra banda que se dedicaba a estafar por Internet fue desarticulada.

En base a las denuncias presentadas por las mismas víctimas en contra de esta organización, los afectados indicaron que habrían perdido alrededor de $100 000. Las investigaciones mostraron que tres personas eran quienes se dedicaban a recaudar el dinero de las estafas y posteriormente a esto lo depositaban en las cuentas de quien encabezaba el grupo. Un informe de Inteligencia estipula que las bandas que roban dinero por medios electrónicos obtienen cada mes entre $6 000 y 9 000. (comercio, 2022)

1.1.14 Concepto de estafa

El código nos dice que "Mandato, P., & Nacional, L. A. (2022) Art. 186 se establece como estafa que la persona que genere un beneficio patrimonial mediante la simulación de hechos falsos, deformación u ocultamiento de hechos, que induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de otro, esto será sancionadao con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.

2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares".

Se debe diferenciar entre estafa y la estafa electrónica puesto que genera confusión y se tiende a unificar creyendo que aborda lo mismo y no existe diferenciación, pero por el contrario es preciso definir que mientras en la primera el sujeto activo es quien causa un engaño ya sea producto de simulación, ocultamiento o defraudación de hechos para generar error en la víctima, error que implica la disposición del patrimonial para el sujeto activo o para un tercero, mientras que la estafa informática no utiliza simulación ni medios engañosos para lograr su cometido, se basa en alterar, clonar, duplicar, hurtar, robar, obtener del propietario la información de su dispositivo sin su respectivo consentimiento.

El fraude brevemente se lo puede definir como un engaño o simulación, acción contraria a la verdad, mientras el delito puede ser definido de forma compleja dado a sus elementos

integrantes que son: “El delito es un acto humano, por lo cual es una acción (acción u omisión) dado acto ha de ser antijurídico, este mismo debe lesionar o poner en riesgo a un interés que se encuentre jurídicamente protegido por lo que este debe corresponder a un tipo legal (figura de delito), que previamente a esto se encuentre establecido por La Ley y el mismo ha de ser un acto típico. Tal acto previamente mencionado debe de ser culpable, por lo que este es imputable al dolo que es la (intención) o a culpa (negligencia), y una acción es imputable cuando esta puede ponerse a cargo de una determinada persona La ejecución u omisión del acto debe estar sancionada por una pena” (Calón, 2020)

En este sentido un delito es una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena, siendo así el fraude informático es la apropiación ilícita de fondos ajenos, también es un delito realizado mediante un dispositivo electrónico y quien lo realiza no es catalogado un delincuente común, sino una persona con un alto grado de conocimiento, el delito informático se considera a toda acción u omisión culpable, la cual es ejecutada por un ser humano y que la misma cause un perjuicio a personas sin que necesariamente se beneficie el autor o que al contrario, genere un beneficio ilícito a su autor aunque este no perjudique a la víctima, no tipificado por la Ley y que se realiza en el entorno informático sin que sea sancionado con una pena.

En la actualidad las computadoras únicamente no son utilizadas como herramientas de trabajo a diferentes actividades, sino como medio para obtener y conseguir información, por lo que a su vez son un medio de comunicación, cuyo trasfondo básicamente se acorta en la invensión, el procesamiento, almacenamiento y transmisión de datos, que en ocasiones son usados para cometer fraude financiero, dado a que la informática no tiene límites previsibles e incrementa la forma que aún puede impresionar a muchos actores del proceso.

En la actualidad se ve en medios de comunicación que la nueva modalidad de robo es dirigida a las cuentas bancarias, dado que es más sencillo para un cyber delincuente crear un sitio falso, programa infeccioso, robar ahorros mediante llamadas telefónicas o correos falsos y desparecer con el dinero.

1.1.15 El ciclo delictivo

Es un término bastante utilizado dentro de la esfera del derecho penal para con esto referirse al proceso que tiene el desarrollo del delito que se produce, de forma más sencilla a las etapas del mismo, comienza desde el momento en que se desarrolla la idea y finaliza en el momento que esta se llega a consumar, a menudo se llega a confundir con el termino de comportamiento

delictivo el cual trata, es la violencia producida en un determinado entorno cultural, económico, político o social, que se materializa dentro de la dinámica de los grupos para de esta forma poderse diversificar en cuanto a sus indicadores. De este modo el estado del conocimiento ha edificado modelos explicativos de la violencia con el objetivo de poder diferenciar las causas y los efectos.

1.1.16 Clases de estafa informática

Se han clasificado de diferentes formas los tipos de delitos informáticos según diversos criterios, para efectos de la presente investigación mencionaremos los principales que son los siguientes:

Fraudes informáticos mediante la manipulación de computadoras

(programas, repetición automática de procesos) este caso se refiere al fraude que es cometido mediante el uso de una computadora por medio de Internet. La piratería informática conocida comúnmente como hacking es una forma común de fraude en el cual el delincuente utiliza instrumentos tecnológicos sofisticadas para de esta forma poder acceder sin restricciones de distancia a una computadora con información catalogada como confidencial o sensible.

En la sustracción de datos, que es catalogado como el delito informático más cometido ya que es sencillo de cometer y difícil de descubrir, puesto que no requiere de los conocimientos técnicos de informática, de tal forma que lo puede realizar cualquier persona que cuente con el acceso a funciones normales o básicas del tratamiento de los datos en la etapa de apropiamiento de los mismos.

Falsificaciones informáticas

(alteración o falsificación de documentos Daños o modificaciones de programas o datos computarizados (sabotaje, virus, bombas lógicas). La falsedad documental es un problema jurídico, el cual a sido objeto de análisis desde la antigüedad, encontrándose varias posiciones, no obstante, la más destacada es por la alteración de la verdad en sí, aludía a la intención subjetiva de causar engaño y la realidad objetiva del trastorno ocasionado de la realidad.

Por ende, surge recalcar cuál es el bien jurídico que protege la legislación penal ecuatoriana con la amenaza de una pena que la castigue, produciendo el surgimiento sin fin de posturas sobre este fenómeno, en donde varios juristas han defendido el derecho existente a la verdad

por medio de la protección de la fe pública y otros expertos establecen que no se encuentra existente tal derecho a la verdad, por lo que se expone al objeto protegido, aseverando que se trata del tráfico de documentos en donde esto crea una vulneración a la fiabilidad que es obtenida exclusivamente de la prueba documental.

La verdadera problemática existente surge sobre la indeterminación del bien jurídico protegido por el delito de la falsedad de documentos, el cual nació en Europa precisamente en el país de Italia y Alemania fue el sitio en donde se congregaron quienes defendían el derecho a la verdad y de la violación al tráfico documental, "no obstante, en la actualidad esta situación conflictiva todavía genera conflictos inherentes al Derecho Penal, también en naciones latinoamericanas que se han visto perjudicada por la legalización de las firmas electrónicas". (Andrade, 2019)

En el Ecuador el COIP se refiere a tres tipos de delitos vinculados a la falsedad, que son la falsificación o adulteración de bienes del patrimonio cultural que se encuentra establecido en el artículo 239 que se expone que ocasiona lesión en el derecho a la veracidad cultural, el segundo es la falsificación de la moneda y demás documentos tanto físicos como digitales al igual forma como lo son los cheques, títulos valores, entre otros (artículo 306) vulnera al régimen monetario y el tercero es la falsificación de firmas físicas o electrónicas y la utilización de documentos falsos (artículos 327 al 329) refiere a los delitos contra la fe pública, (Asamblea Nacional, 2014).

El sabotaje informático es conocido como el acto de eliminar, suprimir, dañar o modificar sin ninguna autorización previa a las funciones o datos de computadora con el único propósito de intervenir dentro del funcionamiento normal del sistema dejándolo inoperativo. Las técnicas que permiten cometer sabotajes informáticos son los virus, como el gusano el cuales un programa dañino que infecta al computador, no tiene una reproducción autónoma, este ataca a un determinado archivo como a programas o páginas

Por otro lado, también dentro del sabotaje se encuentran las bombas lógicas que son programas dañinos encargados de ejecutarse al momento de que se cumpla una determinada condición, estas pueden ser una fecha exacta, cumplida la condición borrará los datos pertenecientes al disco duro, por lo que en conclusión estos virus informáticos son programas maliciosos que atacan e infectan a los ordenadores y de reproducción propia. Esta serie de claves programadas que pueden añadirse a los programas originales, legítimos para así propagarse e infectar a otros programas informáticos.

Accesos no autorizados a servicios y sistemas informáticos

"(piratas, reproducción no autorizada, se da desde una mera curiosidad como es en los casos de diveroso piratas informáticos pudiendo llegar hasta el sabotaje o espionaje informático." (Naciones, 2010). El acceso se produce a frecuentemente desde un lugar en el exterior, ubicado en la red de telecomunicaciones, requiriendo a uno de los varios medios que se señalan a continuación.

El delincuente suele beneficiarse debido a la falta de fuerza en las medidas de seguridad para así lograr crear el acceso e incluso podría desenmascarar deficiencias en las medidas vigentes de seguridad al igual que en los procedimientos del sistema a las catalogadas puertas falsas, las cuales tratan de lo previamente mencionado, el encontrar un error en el código fuente, una abertura en el programa por el cual estos piratas se valen para poder acceder.

A menudo, los piratas informáticos se disfrazan de los mismos usuarios legítimos del sistema, esto suele suceder con regularidad dentro de los sistemas en los que los usuarios pueden hacer uso de contraseñas genéricas o de mantenimiento que están en el mismo sistema. A su vez también entra el tema de llaves maestras, trata de softwares para con ello acceder a los sistemas informáticos.

Derecho comparado

Con el fin de establecer analogías jurídicas y diferencias es necesario conocer algunas leyes que rigen en otros países

Colombia

Se promulgó la Ley 1273 el 5 de enero de 2009 por el Congreso de la República de Colombia con esto se transformó el Código Penal y crearon un nuevo bien jurídico protegido llamado "De la Protección de la información y de los datos" se busca conservar integralmente los sistemas que utilicen la tecnología de la información y comunicación, entre otras disposiciones". Esta ley tipificó como delitos un conglomerado de conductas relacionadas al manejo de datos personales, por lo que es de suma importancia que las empresas se blinden jurídicamente para prevenir caer en alguno de estos tipos penales.

De ahí radica la vital importancia de esta ley, que se suma al Código Penal colombiano con el Título VII BIS llamado «De la Protección de la información y de los datos» el cual se divide en únicamente dos capítulos, a saber:el primero es de los atentados que van en contra de la

confidencialidad e integridad de la disponibilidad de los datos en conjunto a los sistemas informáticos y el segundo de los atentados informáticos y otras infracciones.

En el capítulo segundo que trata de los atentados informáticos y otras infracciones se encuentra en el Artículo 269j donde se habla de la transferencia no consentida de activos, aquí se estipula que quien con ánimo de lucro y por medio de algún tipo de manipulación informática o artificio parecido este obtenga la transferencia no autorizada de cualquier activo ocasionando daño a un tercero," y siempre que la conducta no establezca algún delito sancionado con una pena más grave se incurrirá a una pena de prisión de cuarenta y ocho a ciento veinte meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes". (T., 2018)

La misma sanción se le otorgará a quien fabrique, introduzca, posea o permita algún programa de computador que sea destinado para el cometimiento del delito estipulado en el inciso anterior, o de una estafa. Si la conducta estipulada previamente tuviese una cuantía que ascienda a los 200 salarios mínimos legales y mensuales, la pena allí estipulada ascenderá en la mitad.

Perú

Dado que existe la criminalidad informática y está con el avance del tiempo aumenta más su complejidad, en la legislación vigente penal peruana se avanzó en identificar y tipificar a los delitos informáticos mayor mente ejecutados por lo que existe la Ley Nº 30096 que se publicó en octubre del 2013, la cual trata sobre los delitos vinculados al uso incorrecto de los sofwares y hardwares, como lo son las bases de datos generando daño a los titulares de datos o terceros

Fraude informático se sanciona a quien, por medio de tecnología de información o comunicación obtenga un beneficio o provecho de carácter ilícito para sí u otro en perjuicio de tercero por medio de diseño, introducción, alteración, anulado, supresión, clonación de datos informáticos o que a su vez este genere una interferencia o empleo en el correcto funcionamiento del sistema informático, "será sancionado con una pena privativa de libertad entre tres a ocho años y con sesenta a ciento veinte días multa y si atenta contra el patrimonio del estado que fuere destinado a fines humanitarios como los programas asistenciales o de apoyo social, esta sanción será entre cinco ni a diez años y de ochenta a ciento cuarenta días de multa". (REPÚBLICA, 2013)

Brasil

Se encuentra la ley 12.737 que entró en vigor en el 2013 y tipifica en el Código Penal los delitos cometidos por internet que posee penas de tres meses hasta un año de prisión además de multas,

se incorporan penas por robo de información personal, reproducción de programas informáticos y accesos no autorizados a dispositivos.

En la ley general de protección de datos personales de Brasil conocida como Ley N° 13.709/2018, "LGPD"que fue emitida el día 14 de agosto del año 2018, gracias a la cual fue el transporte que dio el surgimiento para la creación de la Autoridad Nacional de Protección de Datos (ANPD). Los términos relativos a la creación de la ANPD y del Comité Consultivo Brasileño de Privacidad y Protección de Datos entraron en vigor el 28 de diciembre de 2018. Sin embargo, la medida cautelar retrasa la aplicación de las restantes disposiciones de la LGPD hasta el 15 de agosto de 2020. El propósito de esta regla es proteger los datos personales, que se definen como información sobre una persona física identificada o identificable.

La Oficina para la Represión de la Delincuencia Cibernética de la Policía Federal es la principal entidad encargada de investigar los delitos cibernéticos, si bien el sector privado no está obligado a divulgar incidentes cibernéticos, la Oficina de Cumplimiento de Delitos Cibernéticos tiene relaciones de trabajo con las empresas.

Sus facultades van desde la investigación de delitos contra organismos públicos federales hasta infracciones con implicaciones interestatales e internacionales. Está involucrado en la investigación de fraude electrónico (fraude de tarjetas de crédito y banca electrónica) y redes criminales que facilitan el abuso infantil en línea, la Policía Federal será responsable de abordar los casos no autorizados acceso a sistemas y redes

Chile

En junio de 1993 entró en vigencia la Ley N°19.223 que trata sobre los delitos informáticos, no obstante, no se contemplan las figuras del hacking, ni fraude informático, por lo que la ley chilena presenta falencias, vacios y huecos respecto a la regulación de la misma, aun así, es pionera en la región al tratar expresamente el tema de los delitos informáticos.

Marco legal

Convenio de Cibercriminalidad de la Unión Europea

Este convenio fue firmado el día 21 de noviembre del año 2001 en Budapest, este mismo fue promovido por el Consejo de Europa y otros países como Estados Unidos y Japón. Aquel se recopila principalmente de varios puntos entre los cuales se destacan definiciones de términos

que son necesarios para comprender el espíritu del convenio, incluyendo los pensamientos existentes sobre los sistemas, el tráfico de datos o los proveedores de los servicios.

El segundo capítulo se encuentra destinado a las disposiciones que deben ser adheridas a nivel nacional, con la infracción de los derechos de propiedad intelectual y derechos afines, y también las referidas a los aspectos de procedimiento, como las condiciones y garantías, o también jurisdiccionales.

Convenio sobre la Ciberdelincuencia de Budapest

Aquí se establece la cooperación existente entre los estados para luchar contra la ciberdelincuencia y defender los intereses legítimos en el campo de las tecnologías de la información. se focaliza en tres principales elementos básicos: el primero radica en la importancia que tienen las medidas legislativas sustantivas, mientras el segundo elemento es la arraiga en la importancia que tiene una legislación procesal adecuada a la naturaleza del delito y por último el tercero es la importancia de la cooperación internacional y regional en el campo de los ciberdelitos.

A su vez se describen diversos métodos para cosechar la evidencia digital, ya que los residuos digitales que dejan los criminales son difíciles de identificar en el curso de una investigación criminal. Estos métodos también son aplicables a la investigación del delito en general, lo que quiere decir que estos no están reservados únicamente a los ciberdelitos. Estos métodos cumplen condiciones de compatibilidad con los derechos fundamentales de las personas, por lo que consecuentemente, al autorizar la aplicación legal de los métodos los estados mejoran su marco legal.

CAPÍTULO II: METODOLOGíA DE INVESTIGACIÓN

2.1 Enfoque de la investigación

2.1.1 Cualitativo

El enfoque de la investigación es preciso determinar puesto que da la forma en la que se va a aproximar al objeto de estudio, los fenómenos en profundidad son explorados por medio de este enfoque.

La universidad de Jaén define a este tipo de investigación como el "estudio de los individuos a partir de lo que estos mismos expresan y reaccionan, en otras palabras el comportamiento de las personas en el escenario social y cultural, con el principal objetivo de proporcionar una metodología que les posibilite el comprender al laberintico mundo que es el de la experiencia vivida desde el enfoque de aquellas personas que la viven" (Jaén, (S/F)). La distingible característica primordial de este tipo de estudios se lo puede abreviar como centradas o enfocada en los sujetos que acogen la perspectiva emic o también llamada de interior del fenómeno que se va a analizar de forma parcial o completa.

Los investigadores ofrecen respuestas en base a sus experiencias vividas, a su vez está la utilización de revistas, estudios de caso o los análisis documentales. En los temas de ciencias sociales se suele utilizar el enfoque cualitativo, las preguntas abiertas y la exploración para a partir de ese medio realizar la recolección de datos.

El proceso de indagación es inductivo y se pueden clasificar en dos categorías que son los estudios descriptivos en donde se ven los diseños conocidos como etnográficos, a su vez los fenomenológicos, los biográficos o narrativos, de igual manera los de investigación de acción, documentales y los estudios interpretativos que contienen teoría Fundamentada, Inducción analítica.

2.2 Tipos de investigación empleados

2.2.1 Investigación descriptiva

Este tipo de investigación pone su interés en la descripción de los datos, sin la conceptualización ni interpretación de la misma, pretenden describir de forma apegada la vida, lo que acontece, lo que la gente cuenta, cómo lo expresa y de qué manera reacciona, se suelen presentar como una narración.

Muguira dice que "es la encargada de puntualizar las características de la población a la que se está estudiando. Esta metodología se enfoca más en el "qué", en vez del "por qué" del sujeto

de investigación, como su principal objetivo es explicar a la naturaleza de un preciso segmento demográfico, sin centrarse en las razones que ocurrieron para que se produzca un determinado fenómeno en cuestión" (2018). Es decir, "define" el tema de investigación, sin llegar a tapar el "por qué" ocurre.

Este tipo de diseño de investigación conduce a la construcción de dudas, interrogantes que derivan al nacimiento del análisis de datos que se llevarán a cabo sobre el tema, también se lo cataloga como el método de investigación observacional en virtud a que ninguna de las variables que conforman al estudio se encuentra de alguna manera siendo influenciada.

2.3 Periodo y lugar

El periodo es durante los años 2019-2023, con enfoque en la pandemia producida a raíz del Covid- 2019 que abarca el año 2020-2021, en el sur de Guayaquil

2.4 Universo

El universo son los casos de delitos informáticos, el de fraude por medios informáticos en la era de la tecnología y en el periodo de la pandemia 2020-2021.

2.5 Muestra

El referente trabajo de investigación tomo como muestra las leyes existentes en temas de delitos electrónicos del Ecuador y a su vez las de países vecinos para poder comparar los objetivos existentes entre estos a la hora de sancionar estas actividades, a su vez la comparación busca el que es lo que desean sancionar, que tipo de actividades, que es lo que estas deben contener

Se tomó datos de la policía publicados en una noticia del periódico local el comercio

2.6 Metodos empleados

2.6.2 Observación

En base a la investigación presente se registró de fuentes de denuncias presentadas en el periodo 2020-2021, además se revisaron noticias expuestas por la policía nacional en donde se habla del incremento de estos crímenes con su respectivo porcentaje, haciendo hincapié en que pocas personas se atreven a denunciar debido a la dificultad de identificar al autor del crimen.

2.6.2 Entrevistas

Por medio de las entrevistas realizadas a profesionales y expertos del campo de estudio que se trató en la zona sur de la ciudad de Guayaquil en el presente proyecto de investigación se realiza con el objetivo de determinar si esta figura va en aumento y si las medidas sancionadoras impuestas en el Ecuador son suficientes a la hora de juzgar estos delitos son suficientes

Se realizará a los defensores públicos, puesto que son personas encargadas de la defensa o acompañamiento a las víctimas de este tipo de delitos, por lo que son apropiados al momento de verter una opinión o tener una postura en base al tema, conocen el procedimiento, la manera de actuar de los sujetos, ya sean el activo como el pasivo y el campo en que se desarrolla. La información recopilada en estas entrevistas es vital para la investigación, puesto que nos llevará a fundamentarla para dar una solución a la duda planteada

2.7 Procesamiento y análisis de información

El presente proyecto se encuentra planteado con un enfoque cualitativo y su tipo de investigación es descriptiva, debido a que se estudia el avance de la norma se desarrolla en un periodo de cinco años, desde el 2019 hasta la actualidad 2023, no obstante, se realiza una vital aportación en el periodo de la pandemia que comprende desde el 2020 hasta el 2021 dado a que se desarrolló una rutina virtual en diversos aspectos.

Nos encontramos en la era digital, sociedad de la información por lo que se genera un fuerte impacto en el tema de estudio, el análisis se desarrolla tomando noticias, mediante entrevistas a profesionales y comparando la situación actual normativa con la de otros países vecinos para ver como se ha ido desenvolviendo este delito.

CAPITULO 3: Análisis e interpretación de resultados de la investigación

Entrevistas

Entrevista 1

Nombre: Hector Vanegas

Perfil Profesional: Penalista y criminólogo

¿Cómo definiría a la estafa o fraude informático?

Actualmente esto constituye una modalidad que a cogido mucha fuerza y a permitido a travez del sistema electrónico engañar a la gente, que terminan cayendo en ofertas que a todas luces son fantasiosas, pero ellos llegan a convencerse que son posibles, este es una de las características de la estafa, las quimeras, los hechos imposibles y falsos que los adorna a través del sistema informático, donde usted lo que hace es ser invitado, usted termina cayendo en eso, Como por ejemplo el sistema piramidal que es una forma muy común que a través del sistema informático se engañe a la gente.

Esto de ganar dinero fácilmente, de entregar una cuota pequeña con la idea de que luego va a acrecentar su dinero es una forma de engaño, la forma en que le llega al correo y le dicen: usted acaba heredar un millón de dólares, soy el último sobreviviente de una familia, pero necesito que usted llene la siguiente información y a lo que usted va a llenar la información termina usted teniendo que pagar $200 o $300 para mandar la petición, ahí lo están timando.

¿Cree usted que es un tema que vaya en ascenso?

Si, es que hoy en día todo es a través de la parte electrónica, hoy en día se ha desarrollado con tanta rapidez que hoy las audiencias ya son telemáticas, hoy la relación amorosa ya no es cogiéndose a la mano sino viéndose por pantallas o chateándose, usted ya perdió la parte emocional. Entonces Si eso ya invadió al ser humano que evidentemente también estafa, se hace más fácil hacer de forma informática, porque además asegura la impunidad ¿cómo persigue a la persona que le levanta un correo falso o red falsa?

¿Considera usted que la legislación vigente en materia de delitos informáticos en nuestro país es suficiente al momento de sancionar este tipo de delitos?

Actualmente el código orgánico ha introducido algunos tipos penales a copiado de algunas otras legislaciones, creo que para nuestro desarrollo en nuestro medio alcanza momentáneamente al tipo penal

La parte informática está en una evolución tan rápida que evidentemente esos tipos en el futuro se van a tener que modificar

¿Ecuador cuenta con las suficientes herramientas para averiguar quién o como se cometió el delito?

Yo no lo creo, creo que recién están desarrollándose, no solo las herramientas sino también los peritos, las mecánicas para también poder dar con los responsables, aquí en el tema informático tenemos que saber de qué computadora o que teléfono, de que celda, quien es el verdadero dueño y en tema informático es bastante fácil falsear información usted va y levante una computadora o un correo falso ¿Cómo logra detectar quien es el verdadero autor de ese hecho? Podrá ubicar talvez la celda y esa a su vez un ciber, pero ¿cómo persigue al responsable? Otra cosa es que sea en una casa, en el domicilio, la oficina, entonces estamos a años luz todavía.

Tanto es así que el zoom llegó a nuestro país hace unos años cuando en Japón ya tenía 20 años funcionando, la tecnología nuestra galopa, trata de correr al mismo rito que los países desarrollados, pero nunca va a tener el mismo nivel.

¿Con la nueva reforma en el COIP del artículo 477.1-477.10 realizada en marzo del presente año cree usted que bajaran los índices delincuenciales?

Ninguna norma tiene el poder de bajar el índice delincuencial, si fuese asa con la reforma que se introdujeron para el femicidio no habría más mujeres muertes y sin embargo todos los días matan gente y con eso no habría más sicariato que es un tipo penal nuevo al código y usted ve que todos los días hay sicariato en cualquier parte del país.

¿A su parecer que considera más relevante o peligroso en este tipo de delitos?

Para mí lo más peligroso es el anonimato, no saber identificar quien es el responsable y otro problema es la ingenuidad de la gente, ya están advertida de no caer en trampas y pese a eso se deja engañar.

¿ha escuchado o llevado casos en materia de delitos informáticos?

Aquí he llevado casos de sistema piramidal que se hace por medio de la computación, hay mucha gente engañada y siempre surge el problema en que es difícil identificar la identidad del autor o la identidad cierta del autor, a través de la computadora, tu como sabes la otra persona de verdad se llama como te dijo, únicamente supones que es así y te estafaron.

¿Considera que ha existido un avance significativo en cuanto a legislación en estos casos?

No se puede frenar ningún delito, ¿cómo evitas que el mundo moderno que ya tiene una herramienta que antes no existía que es casualmente la red social se detenga? Es imposible, lo que hace el sistema penal es incluir en los tipos penales las nuevas modalidades.

No se puede detener porque mientras más avanza el desarrollo más avanza la técnica para estafar, hace unos años el ecuador no tenía computación o computadoras, ni pensarlo, ahora las hay y seguramente en unos años esto va a ser superado ya que la tecnología avanza muy rápido.

Entrevista 2

Nombre: Carlos Galarza

Perfil Profesional: Ing. En sistemas con diplomado en peritaje criminal

¿Cómo definiría a la estafa o fraude informático?

La apropiación fraudulenta sería el tipo y es buscar por medio de redes o sistemas informáticos dañar a terceros, muchas personas con esto buscan apropiarse de medios electrónicos como cuentas webs que son utilizadas para llegar a un tercero, por ejemplo, un posible consumidor al que intentaran vender un producto y posteriormente lo estafan al no brindarle el servicio o producto por el cual pagó.

¿Cree usted que es un tema que vaya en ascenso?

Si, sobre todo para las empresas va a ser beneficioso porque con esto van a poder seguir el hilo del delito que se está realizando

¿Considera usted que la legislación vigente en materia de delitos informáticos en nuestro país es suficiente al momento de sancionar este tipo de delitos?

Es sumamente nueva en realidad, se ha implementado reciente en la reforma de este año puesto que los delitos electrónicos no estaban implementados el año pasado, por lo que hubo siempre ese vacío legal

¿Ecuador cuenta con las suficientes herramientas para averiguar quién o como se cometió el delito?

No, puesto que los peritos no están calificados para eso, no saben que buscar o como perseguir la prueba por lo que el caso se va a caer

¿Con la nueva reforma en el COIP del artículo 477.1-477.10 realizada en marzo del presente año cree usted que bajaran los índices delincuenciales?

Esto ayudaría a los fiscales para con esto poder buscar las pruebas necesarias y así llevar el caso a juicio, se puede seguir el crimen internacional con esta nueva reforma, como ejemplo esto ya se da en la empresa Apple

¿A su parecer que considera más relevante o peligroso en este tipo de delitos?

Llegar a juicio, actualmente no creo que puedan llegar tan fácil porque no hay la suficiente cantidad de herramientas para poder reunir los suficientes elementos de convicción exactos que puedan ayudar a formar el jucio

¿ha escuchado o llevado casos en materia de delitos informáticos?

No

¿Considera que ha existido un avance significativo en cuanto a legislación en estos casos?

Considero que sí, pese a que todavía no lo veo aplicable debido a que las faltas de herramientas generan una traba entre la ciudadanía que ha sido víctima de esto

Entrevista 3

Nombre: Josué Macías

Perfil Profesional: Abogado

¿Cómo definiría a la estafa o fraude informático?

Como la utilización de medios para violar a la ciber seguridad de alguna institución pública o privada para apropiarse de información relevante que le permita cometer otros delitos ligados al primero o en sí mismo al cometimiento de ese delito que sería vulnerar sistemas informáticos

¿Cree usted que es un tema que vaya en ascenso?

Si, creo que a partir de la expedición y publicación de la ley de protección de datos personales, de la entrada en vigencia del régimen sancionatorio, lo que es algo que seguramente va a aumentar por una parte lo que es el cuidado una vez que entre el funcionamiento de la superintendencia va haber mucha reglamentación que aplique estrictamente a la protección de datos de información y a medida que este tipo de información tenga resguardo van a existir diversos mecanismos para vulnerarla y hace que este tipo de delitos en un par de años tenga seguramente un auge más significativo que el que ha tenido con anterioridad

¿Considera usted que la legislación vigente en materia de delitos informáticos en nuestro país es suficiente al momento de sancionar este tipo de delitos?

No, considero que aún falta mucho que avanzar en Ecuador, si bien es cierto se están haciendo ciertas mejoras en nuestro sistema actual, es algo que debe hacerse a manera global en general no solamente puede reformarse el COIP y a partir de eso considerar que podemos tener ya una regulación un poco más estricta sino que también tiene que modificarse normativa complementaria como ya se ha hecho la implicación de la ley de protección de datos personales que es un mecanismo que está tomando este sentido

Entonces hace falta mucha normativa complementaria para que se pueda obligar a las personas naturales y jurídicas a proteger información, a tener mecanismos de seguridad y de resguardo de la información para luego poder pedirles a ellos en un proceso penal información o que demuestren sus herramientas de protección o cuidado de amenazas, como lo son los delitos informáticos.

¿Ecuador cuenta con las suficientes herramientas para averiguar quién o como se cometió el delito?

No, porque todavía se está iniciando en esto, un avance fue la ley de protección de datos, el reglamento, la superintendencia pondrá ciertos parámetros que servirá y ayudará a proteger la información de las personas, actuará en temas de suplantación de identidad y demás.

¿Con la nueva reforma en el COIP del artículo 477.1-477.10 realizada en marzo del presente año cree usted que bajaran los índices delincuenciales?

No creo que baje porque actualmente es una dificultad para los fiscales poder identificar a las personas que cometen estos delitos, más que todo por un tema de competencia en cuanto a la territorialidad y averiguar en qué lugar y desde que momento se cometió el delito

Desde mi percepción es difícil el poder demostrar desde cuándo y quien lo cometió, para a partir de eso iniciar con su investigación, entonces al momento de ellos poder asumir la competencia se presenta un desafío, en ese punto y luego el poder marcar los tiempos de investigación dado a que no saben con quien se enfrentan y es algo que no tiene mecanismos para fiscales, ni policía judicial, Ecuador no cuenta con los peritos acreditados en este tema que puedan facilitar una investigación penal, lo que hace difícil de aquí en corto tiempo tener un proceso penal en este sentido con las herramientas necesarias para poder condenar a una persona

¿A su parecer que considera más relevante o peligroso en este tipo de delitos?

Es la facilitación para el cometimiento de varios delitos, la apropiación de información mediante el uso de temas informáticos puede a una persona darles acceso a los datos personales de una persona jurídica para cometer cualquier tipo de acto, por ejemplo suplantar su información puede hacer que el delito se cometa de manera continua en el tiempo como vender su base de datos a la Deep web, etc. Lo que va hacer que si su información aparece en la Deep web cualquier persona que tenga la intención de cometer un delito en cualquier parte del mundo utilice esa información para tratar de contactarlo y a través de engaños llevarle a cometer actos o que le facilite dinero o información que lo comprometa.

El hecho que se tenga una vulneración a través de un medio electrónico, por cualquier medio informático hace que la información de aquí en adelante se encuentre a disposición de cualquier persona no es un delito que al momento que se comete se sufra los daños sino que los daños se pueden ver a largo tiempo y eso afecta nuevamente al tema del proceso penal, en temas de competencia del fiscal y los tiempos para el cometimiento de la infracción, porque puede que la infracción se cometa hoy pero surta efectos en cinco o seis años.

Los daños se ven a largo tiempo por una persona que encontró la información en internet e hizo contacto, engañas, la victima otorga dinero y la persona está en costa de marfil o en la india operando con información obtenida por medio de un hackeo o una brecha de seguridad en algún sistema de una empresa, por lo que para mí el principal problema es no saber cuándo se va a ver afectada la persona por los efectos de la vulneración a la seguridad.

¿ha escuchado o llevado casos en materia de delitos informáticos?

No

¿Considera que ha existido un avance significativo en cuanto a legislación en estos casos?

Creo que no lo ha habido, últimamente se ha tratado con las reformas al COIP, con la implementación de la ley de protección de datos se ha tratado de darle un mayor enfoque a estos temas que son la filtración de información por medio de ataques cibernéticos pero no ha sido suficiente, dado a que no sirve que la legislación penal tipifique un delito si es que no hay legislación complementaria que obligue a personas que son quienes tienen la información o que tienen esos portales o aplicaciones a tener un mecanismo de protección.

CAPITULO 4: PROPUESTA

4.1 Propuesta

Capacitar a Fiscales en materia de delitos electrónicos

Existe una necesidad urgente de profesionales especializados en el tema de la informática para recaudar las pruebas suficientes, junto con los elementos de convicción necesarios para que estos casos puedan llegar a juicio debido a que de ellos depende el buen funcionamiento del sistema de justicia penal.

Tener peritos en el área de delitos electrónicos

Brindar capacitaciones en temas de sistemas informáticos, vulneración en la web, cuentas de correo, registro, contenido digital en servidores, para así cubrir las deficiencias cuando se presentan vulneraciones en estos por medio de virus, hackeos o brechas digitales.

Instaurar un método de rastreos de huellas digitales

Ya existe una ley sobre el tratamiento de datos personales para saber cómo, dónde y por cuánto tiempo se usa nuestra información, sin embargo, debería existir una ley que obligue a las empresas a guardar los datos de forma segura, mediante un sistema de seguridad fiable que evite los robos y hackeos del contenido, para evitar que sus usuarios se conviertan en víctimas de fraudes adelante por robo de información o de los correos.

Conclusiones

La tecnología avanza con la humanidad, es inminente que cada vez serán mayores los avances tecnológicos que surjan y a su vez con estos también las formas y mecanismos para delinquir por lo que es preciso contar con las herramientas necesarias para contrarrestar este mal.

Los delitos electrónicos como la apropiación ilegal por medios electrónicos no se van a poder frenar nunca, no obstante, se va a sancionar a la o las personas que por esta figura delictiva perjudiquen a terceros, para lo cual es preciso y se necesita contar con las herramientas junto con el personal capacitado en esta área, cada vez son más los fraudes, el más común de este tipo es la estafa piramidal, por lo que el Ecuador necesita contar con peritos capacitados a la hora de realizar exámenes de este tipo, necesita fiscales que puedan llevar a juicio el caso, que sepan que es lo que se debe buscar y solicitar al perito que realice, se necesita jueces que comprendan y lo puedan juzgar por lo que es imperativo estudiar el tema.

No solo basta con el personal capacitado, se deben crear leyes que obliguen a las empresas que guardan datos privados, personales con los que se puede identificar a la ciudadanía a tener medidas de seguridad que eviten los robos de información, que estas cuenten con sistema de protección a prueba de hackeo para que posteriormente que sus usuarios no sean víctimas de fraudes.

Recomendaciones

A los usuarios de las entidades bancarias informar sobre medidas de seguridad a tomar en consideración para evitar ser víctimas de fraudes informáticos y así estar prevenido contra estas actividades, además de indicar cuales son los medios oficiales que ellos disponen para informar a sus usuarios o para realizar trámites bancarios.

En las aulas de clases informar de igual forma sobre seguridad informática, claves seguras, virus informáticos y demás mecanismos para no ser víctimas de delitos informáticos, hablar sobre la importancia de los antivirus junto con los peligros de la red y revisar los remitentes en los correos electrónicos, el estar alerta ante cualquier señal.

A las personas en general leer sobre formas de prevención de la información digital, de modo de evitar que esta caiga en terceros o se use para motivos contrarios a los que se busca.

Bibliografía

Andrade, N. D. (10 de Julio de 2019). *portal Aamelica.* Obtenido de portal Amelica: http://portal.amelica.org/ameli/jatsRepo/383/3831589001/html/index.html

Asamblea Nacional, E. (20 de octubre de 2008). Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Cabrera, Y. E., & Alvarez, E. L. (noviembre de S/f). *eumed.* Obtenido de eumed: https://www.eumed.net/rev/cccss/14/ecra.html

Calón, E. C. (2020). *Enciclopedia Jurídica*. Obtenido de Enciclopedia Jurídica: http://www.enciclopedia-juridica.com/d/delito/delito.htm

Chejín, S. R. (16 de septiembre de 2021). *GK city.* Obtenido de GK city: https://gk.city/2021/09/16/estafas-en-los-bancos-datos/

comercio, E. (25 de Julio de 2022). *El comercio*. Obtenido de El comercio: https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

ecuatoriano, F. g. (13 de junio de 2015). *fiscalia.* Obtenido de fiscalia: https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

española, L. r. (s.f.). *La real academia española*. Obtenido de La real academia española: https://dle.rae.es/inform%C3%A1tico

Falcón, P. P. (8 de Enero de 2022). *linkedin*. Obtenido de linkedin: https://www.linkedin.com/pulse/qu%C3%A9-es-la-inform%C3%A1tica-y-cu%C3%A1les-son-sus-ramas-pablo-perdomo-falc%C3%B3n/?originalSubdomain=es

Guerrero-Saade, J. A. (14 de julio de 2014). *kaspersky.* Obtenido de kaspersky: https://latam.kaspersky.com/blog/cuidado-con-los-fraudes-de-las-tarjetas-de-credito-en-brasil/3492/

Humanitarios., N. U. (1994). Manual de las Naciones Unidas sobre prevención y control de los delitos informáticos. *Revista internacional de política criminal*, n.43-44.

J, F., & Centeno, U. (16 de enero de 2015). *Instituto Español de Estudios Estratégicos.* Obtenido de Instituto Español de Estudios Estratégicos: https://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf

Jaén, U. d. ((S/F)). *ujaen*. Obtenido de ujaen: http://www.ujaen.es/investiga/tics_tfg/enfo_cuali.html

María, B. G. (septiembre de 2014). Obtenido de http://www.dspace.uce.edu.ec/bitstream/25000/5318/1/T-UCE-0013-Ab-367.pdf

Muguira, A. (23 de octubre de 2018). *Questionpro*. Obtenido de Questionpro: https://www.questionpro.com/blog/es/investigacion-descriptiva/

NACIONAL, R. D. (8 de marzo de 2023). *LEXIS.* Obtenido de LEXIS: https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf

NACIONAL, R. D. (s.f.). *Lexis S.A.* Obtenido de Lexis S.A: https://www.lexis.com.ec/biblioteca/coip

NACIONAL, R. D.-G. (2009). *Delitos informaticos LEY 1273 DE 2009.* Bogotá, D.C., Colombia. Obtenido de https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Naciones, D. d. (17 de Abril de 2010). Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, Viena (Austria) 10 al 17 de abril de 2000. Obtenido de https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml

Ortiz, S. (14 de abril de 2018). *elcomercio*, SEGURIDAD. Obtenido de elcomercio: https://www.elcomercio.com/actualidad/seguridad/peritosinformaticos-cibermafias-delitos-ecuador.html

Palacios, J. (31 de mayo de 2022). *la barra espaciadora.* Obtenido de la barra espaciadora: https://www.labarraespaciadora.com/ddhh/el-calvario-de-la-clonacion-de-tarjetas-de-credito/

Peña, C. A. (2021). Obtenido de https://www.studocu.com/es-ar/document/universidad-nacional-del-noroeste-de-la-provincia-de-buenos-aires/informatica-y-derecho-informatico/informatica-juridica-y-derecho-informatico/14433022

Pibank. (3 de febrero de 2020). *Pibank.* Obtenido de Pibank.

PINO, D. S. (2016). Delitos Informáticos: Generalidades. *Revista de derecho informático*, 67. Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

REPÚBLICA, E. C. (2013). *LEY DE DELITOS INFORMÁTICOS LEY Nº 30096.* Lima, Perú. Obtenido de https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

Rivadeneira, J. J. (2010). *Derecho y nuevas tecnologías.* Quito, Ecuador: Corporación de Estudios y Publicaciones. Obtenido de https://biblioteca.casadelacultura.gob.ec/cgi-bin/koha/opac-detail.pl?biblionumber=29699

Rivadeneira, J. J., & Pino, S. A. (2010). Obtenido de file:///C:/Users/Dell/Downloads/Dialnet-DelitoInformaticoProcedimientoPenalEnEcuador-5761561%20(2).pdf

T., J. C. (2018). *DELTA Asesores*. Obtenido de DELTA Asesores: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

Tablado, & Fernando. (26 de mayo de 2020). *Grupo Atico34*. Obtenido de Grupo Atico34: https://protecciondatos-lopd.com/empresas/perito-informatico-peritaje/

Zulia, U. d. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89). Obtenido de redalyc: https://www.redalyc.org/journal/290/29062641023/html/

Anexos

Formato de entrevista

Entrevistador: Carrillo Vera María Fernanda

Tema: Delitos electrónicos

Título de tesis: El avance normativo del delito electrónico de estafa por medio de las tarjetas electrónicas desde la normativa jurídica en el 2020 y la dificultad para determinar su autoría.

Preguntas para la entrevista.

¿Cómo definiría a la estafa o fraude informático?

¿Cree usted que es un tema que vaya en ascenso?

¿Considera usted que la legislación vigente en materia de delitos informáticos en nuestro país es suficiente al momento de sancionar este tipo de delitos?

¿Ecuador cuenta con las suficientes herramientas para averiguar quién o como se cometió el delito?

¿Con la nueva reforma en el COIP del artículo 477.1-477.10 realizada en marzo del presente año cree usted que bajaran los índices delincuenciales?

¿A su parecer que considera más relevante o peligroso en este tipo de delitos?

¿ha escuchado o llevado casos en materia de delitos informáticos?

¿Considera que ha existido un avance significativo en cuanto a legislación en estos casos?

Fotos con los entrevistados

Entrevista No. 1

Entrevista No. 2

Entrevista No. 3