UNIVERSIDAD TECNOLÓGICA ECOTEC

FACULTAD DE DERECHO Y GOBERNABILIDAD

Título del trabajo:

Análisis del delito de estafa a través del internet en la modalidad phishing en la ciudad de Guayaquil, en el año 2023.

Línea de trabajo:

Gestión de las relaciones jurídicas

Modalidad de Titulación:

Proyecto de Investigación

Nombre de la Carrera:

Derecho

Título a obtener:

Abogado

AUTORES:

CARANQUI RUMIPAMBA DENISSE EVELYN
LÓPEZ NÚÑEZ JAIME JOSÉ

TUTOR:

Mgtr. Miguel Emilio Félix Romero

Samborondón – Ecuador

2024

ANEXO No. 9

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

Samborondón, 31 de julio de 2024

Magíster Andrés Madero Poveda
Decano de la Facultad
Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **Análisis del delito de estafa a través del internet en la modalidad phishing en la ciudad de Guayaquil, en el año 2023**, fue revisado, siendo su contenido original en su totalidad, así como el cumplimiento de los requerimientos establecidos en la guía para su elaboración, por lo que se autoriza a los estudiantes: Caranqui Rumipamba Denisse Evelyn y López Núñez Jaime José**,** para que procedan con la presentación oral del mismo.

ATENTAMENTE,

Firmado electrónicamente por:
MIGUEL EMILIO FELIX ROMERO

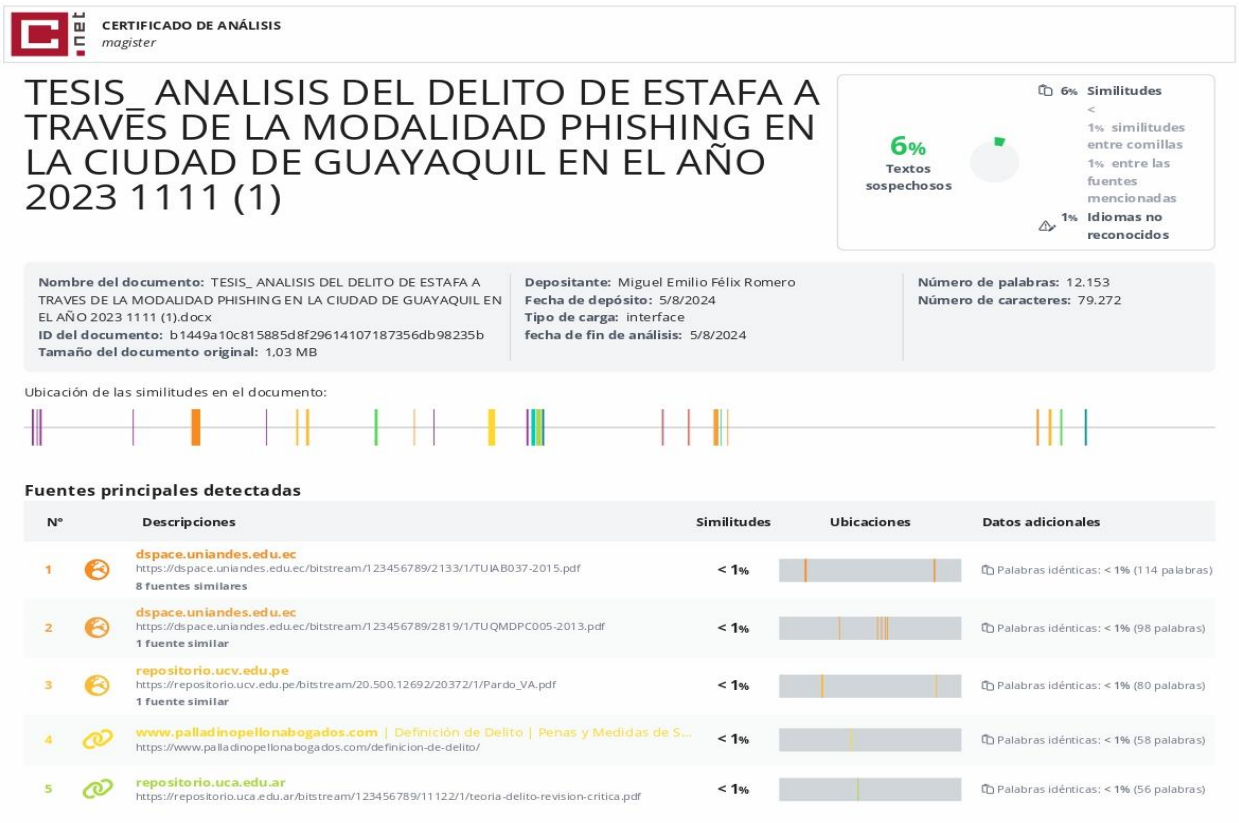
Abg. Mgtr. Miguel Emilio Félix Romero

Tutor

ANEXO No. 10

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido revisado el trabajo de titulación TITULADO: **Análisis del delito de estafa a través del internet en la modalidad phishing en la ciudad de Guayaquil, en el año 2023,** elaborado por **Caranqui Rumipamba Denisse Evelyn y López Núñez Jaime José** fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del 6 % mismo que cumple con el valor aceptado para su presentación que es inferior o igual al 10% sobre el total de hojas del documento. Adicional se adjunta print de pantalla de dicho resultado.



CERTIFICADO DE ANÁLISIS
magister

TESIS_ ANALISIS DEL DELITO DE ESTAFA A TRAVÉS DE LA MODALIDAD PHISHING EN LA CIUDAD DE GUAYAQUIL EN EL AÑO 2023 1111 (1)

6% Textos sospechosos

6% Similitudes
< 1% similitudes entre comillas
1% entre las fuentes mencionadas
1% Idiomas no reconocidos

Nombre del documento: TESIS_ ANALISIS DEL DELITO DE ESTAFA A TRAVES DE LA MODALIDAD PHISHING EN LA CIUDAD DE GUAYAQUIL EN EL AÑO 2023 1111 (1).docx
ID del documento: b1449a10c815885d8f29614107187356db98235b
Tamaño del documento original: 1,03 MB

Depositante: Miguel Emilio Félix Romero
Fecha de depósito: 5/8/2024
Tipo de carga: interface
fecha de fin de análisis: 5/8/2024

Número de palabras: 12.153
Número de caracteres: 79.272

Ubicación de las similitudes en el documento:

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Datos adicionales
1	dspace.uniandes.edu.ec https://dspace.uniandes.edu.ec/bitstream/123456789/2133/1/TUIAB037-2015.pdf 8 fuentes similares	< 1%		Palabras idénticas: < 1% (114 palabras)
2	dspace.uniandes.edu.ec https://dspace.uniandes.edu.ec/bitstream/123456789/2819/1/TUQMDPC005-2013.pdf 1 fuente similar	< 1%		Palabras idénticas: < 1% (98 palabras)
3	repositorio.ucv.edu.pe https://repositorio.ucv.edu.pe/bitstream/20.500.12692/20372/1/Pardo_VA.pdf 1 fuente similar	< 1%		Palabras idénticas: < 1% (80 palabras)
4	www.palladinopellonabogados.com | Definición de Delito | Penas y Medidas de S... https://www.palladinopellonabogados.com/definicion-de-delito/	< 1%		Palabras idénticas: < 1% (58 palabras)
5	repositorio.uca.edu.ar https://repositorio.uca.edu.ar/bitstream/123456789/11122/1/teoria-delito-revision-critica.pdf	< 1%		Palabras idénticas: < 1% (56 palabras)

Firmado electrónicamente por:
MIGUEL EMILIO FELIX ROMERO

Firma del Tutor
Miguel Emilio Félix Romero

DEDICATORIA

Este trabajo de investigación lo dedico con profundo amor y agradecimiento a mi familia, quienes han sido el pilar fundamental en mi vida. Su apoyo incondicional ha sido la fuerza que me ha impulsado a alcanzar mis metas y superar los obstáculos que se han presentado en mi camino. Han estado presentes en los momentos más alegres y en los más difíciles, brindándome su apoyo emocional, sus sabios consejos y su infinito amor.

Reconozco con humildad que sin el apoyo y el esfuerzo de mi familia no habría podido llegar hasta aquí. A ellos les debo mi formación como persona y como profesional. Esta tesis es un reflejo de su dedicación, su amor y su sacrificio.

Gracias por ser mi fuente de fortaleza e inspiración. Los amo profundamente.

AGRADECIMIENTO

Con profunda gratitud, elevo mi voz al cielo para agradecer a Dios por el don de la vida, la salud y la inteligencia que me han permitido alcanzar mis sueños. A mis padres, pilares fundamentales en mi existencia, les expreso mi más sincero reconocimiento por su apoyo incondicional, tanto económico como moral. Su amor y guía han sido la fuerza que me ha impulsado a convertirme en el profesional que soy hoy en día.

RESUMEN

Este presente trabajo de titulación se investigó sobre el delito de estafa en relación al phishing, en base a cómo funciona, sus estructuras, modalidades de operar en el ciberespacio, sujetos procesales y cómo podríamos determinar esta modalidad de “delito informático”. Para así configurarlo como un delito autónomo y proponer una reforma de ley, puesto que en nuestro marco legislativo ecuatoriano no está tipificado, solo encontramos una gran gama de delitos, para ser más específicos en el Código Orgánico Integral Penal, como resultado se sancionan aquellas penas tipificadas.

Se entiende que en esta tesis tuvo como objetivo abordar temas muy importantes y complementarios en la materia de delitos informáticos /electrónicos, para proteger al mismo modo de prevenir futuras vulneraciones de derechos tutelados y ser víctimas de la modalidad de phishing, siendo esta un método para la comisión de delitos a causa del desconocimiento que existe por del agente pasivo, dado a que cae por error, manipulación o fraude, mediante correos falsos, páginas de web falsas, entre otros que describiremos en el contenido teórico.

Para ello, se utilizó información encontrada en libros, documentos de sitio web, informes. Los resultados de este trabajo se verán reflejado en el contenido del marco metodológico, utilizando el método empírico y entrevistas dirigidas a profesionales del derecho penal. Por lo tanto, hemos concluido que es necesario la inclusión de la modalidad de pishing como estafa digital.

Palabras claves: *delitos informáticos, estafa, phishing, delito autónomo.*

ABSTRACT

This present degree work was investigated on the crime of fraud in relation to phishing, based on how the phishing technique works, its structures, modalities of operating in cyberspace, procedural subjects and how we could determine this type of "computer crime". In order to configure it as an autonomous crime, since in our Ecuadorian legislative framework we find a wide range of crimes, to be more specific in the Comprehensive Organic Criminal Code, as a result those typified penalties are sanctioned.

It is understood that this thesis aimed to address very important and complementary topics in the field of computer/electronic crimes, to protect as well as prevent future violations of protected rights and being victims of the form of phishing, this being a method to the commission of crimes due to the ignorance that exists on the part of the passive agent, given that it falls due to error, manipulation or fraud, through false emails, false web pages, among others that we will describe in the theoretical content

To do this, information found in books, website documents, and reports was used. The results of this work will be reflected in the content of the methodological framework, using the empirical method and interviews aimed at criminal law professionals. Therefore, we have concluded that it is necessary to include the phishing modality as a digital scam.

Keywords*: computer crimes, scam, phishing, autonomous crimes*

INDICE DE CONTENIDO

Introducción

A lo largo de la historia y la evolución de nuestra sociedad, nos encontramos en una nueva era, es decir en la era digital, que ha desencadenado grandes cambios, más aún a partir de la creación del internet, ya que se ha impregnado en nuestra vida cotidiana, junto al aumento del crecimiento acelerado del internet en lo que ha ido el tiempo, creando así una red de comunicación global y permitiendo la interconexión en los sistemas informáticos a nivel mundial, trayendo como resultados beneficios y perjuicios por el mal uso del sistema.

En esta presente investigación nos centraremos en cómo se han desarrollado nuevas formas de delinquir dentro de la ciudad de Guayaquil, asimismo el estudio de la evolución de la modalidad del phishing, puesto que se basa principalmente en engañar a la víctima, ya sea a través de correo electrónico, mensajes de texto o suplantando páginas web, entre otros que se le irán explicando más adelante, y de esta manera causar un perjuicio al patrimonio de la víctima, dado que este tipo de modalidad ha desencadenado una serie de delitos informáticos y económicos.

Es importante abordar de qué manera actúan los ciberdelincuentes y qué herramientas utilizan para obtener ilícitamente datos personales, información personal o confidencial y ser utilizados para la apertura de cierta gama de delitos como el delito de estafa, considerando que esta se encuentra tipificada en nuestra legislación Ecuatoriana en el código integral penal COIP art 186; en consecuencia, esta técnica desleal trae perjuicios para las personas naturales o jurídicas.

Además, en este trabajo se busca demostrar significativamente incluir nuevas formas de fraude informático, como el phishing, dentro de la legislación ecuatoriana. A pesar de que el Código Orgánico Integral Penal (COIP) ya sanciona ciertos delitos informáticos, es necesario actualizar y ampliar estas normativas para abordar de manera efectiva el phishing. Esto no proporcionaría un marco legal más robusto para combatir estos delitos, sino que

fortalecería la capacidad del sistema judicial para enfrentar la ciberdelincuencia de manera más efectiva.

Es trascendental que los administradores de justicia de Ecuador estén debidamente capacitados para su tratamiento debido a la complejidad y naturaleza de estos actos ilícitos. Esto incluye la necesidad de especializaciones que les permitan distinguir las diversas modalidades mediante las cuales se cometen estos delitos, superando así las limitaciones de las directrices tradicionales aplicadas a los delitos convencionales.

Las experiencias de otros países que han adoptado normativas especializadas también influyen de manera positiva, ya que no se limita a su propio marco normativo, como el convenio de Budapest, de modo que nos ofrecen valiosas lecciones sobre cómo estructurar nuestras leyes para enfrentar mejor estos desafíos. Por ejemplo, en nuestro país vecino Perú. La adopción de este convenio ha implicado mejoras significativas en la definición y tratamiento de los delitos informáticos.

Finalmente, a través de este trabajo, se examinará este tipo de estafa y el existente nexo del fraude informático por el resultado del aumento considerable en Ecuador, especialmente en la ciudad de Guayaquil en el año 2023, y cómo la falta de peritos en tecnología ha dificultado la identificación y sanción de los delincuentes. Esta situación ha generado una deficiencia en la seguridad jurídica, lo cual subraya la necesidad urgente de reformas.

Antecedentes

Según la autora, Chaucha Acero nos menciona en su investigación que el delito informático, o crimen electrónico, o bien ilícito digital es el término genérico para aquellas operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Sin embargo, las categorías que definen un delito informático son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje o pornografía infantil, en los cuales ordenadores y redes han sido utilizados. Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados. (Cristina, 2014, pág. 1)

Una de las principales causas del éxito del phishing es la falta de conocimiento y conciencia entre los usuarios de Internet sobre este tipo de fraude. Muchos usuarios no saben cómo identificar correos electrónicos o sitios web falsos, ni toman las medidas de precaución necesarias para proteger su información personal.

Las entidades públicas y privadas también suelen ser víctimas de phishing debido a la falta de seguridad en su sistema; como consecuencia de este instrumento delictivo se puede conseguir información confidencial de los clientes o empleados.

Planteamiento del problema

En la ciudad de Guayaquil, al igual que el resto del mundo, el uso del internet ha experimentado un crecimiento considerable en los últimos años. Esta creciente conectividad ha traído consigo grandes beneficios, pero también ha creado un terreno fértil para el desarrollo de actividades delictivas. Debido a las transacciones y actividades que se realizan en línea. Una de las modalidades delictuosas que ha experimentado un auge significativo en los últimos años es el phishing.

El phishing representa una grave amenaza para la seguridad de los usuarios en Internet, ya que puede ocasionar importantes daños financieros, perjuicios a la reputación y

el robo de información personal. Las víctimas de este tipo de fraude pueden sufrir pérdidas económicas considerables, ser víctimas de suplantación de identidad o incluso ver comprometida su seguridad personal.

A pesar de los esfuerzos realizados por las autoridades y organizaciones especializadas en ciberseguridad, el phishing sigue siendo un delito prevalente y de constante evolución. La facilidad con la que los delincuentes pueden crear sitios web falsos, enviar correos electrónicos engañosos y aprovechar las vulnerabilidades de los usuarios convierte al phishing en un desafío complejo de abordar.

Formulación del problema:

¿La no tipificación del delito en la modalidad phishing está afectando a la seguridad, la economía y la sociedad en general, y qué estrategias se pueden implementar para prevenirlo y combatirlo de manera efectiva?

Objetivo general

Analizar la estructura delictiva de la técnica del phishing, para así identificarlo como delito que se desencadena a través de la red de Internet.

Objetivo específico

- Analizar las causas de estafa común por medio del phishing en la ciudad de Guayaquil, durante el periodo 2023.
- Identificar los derechos vulnerados de las personas víctimas de estafa mediante el phishing en la ciudad de Guayaquil durante el periodo 2023.
- Establecer una propuesta de reforma al COIP para que tenga sustento legal y que esta conducta de estafa sea reprimida para su correspondiente sanción.

Justificación

La tecnología está avanzando muy rápido y la recopilación de información cada vez es más fácil, debido a esto ha traído consigo un aumento considerable de la delincuencia, ya

que al recopilar datos de forma fraudulenta esto puede ser usado de forma negativa en el individuo con la finalidad de afectar su patrimonio. Cabe recalcar, que el phishing afecta tanto a personas como a empresas, ya sean estas públicas o privadas. Ya que los delincuentes pueden eliminar con facilidad cualquier rastro para no ser identificados o crear páginas webs falsas para no ser localizados. es un delito global que ha experimentado un crecimiento exponencial en los últimos años.

La falta de tipificación de este tipo de delito, como es el phishing, en el código orgánico integral penal ecuatoriano, sumado a la deficiencia del sistema penal, perjudica el derecho a la seguridad jurídica de las víctimas. Las estadísticas de la fiscalía general del Estado muestran que desde el 2020 hasta el 2023 ha existido un aumento considerable de denuncias a través de este tipo de delito, especialmente en la ciudad de Guayaquil, por lo que a falta de una figura penal específica para este delito dificulta la investigación. “Un estudio de la firma Kaspersky reveló que el 20% de las víctimas de phishing experimentan estrés, ansiedad o miedo, y el 10% incluso desarrolla problemas de salud mental a largo plazo”. (daily, 2018)

El derecho a la privacidad, la seguridad de la información y la libertad de expresión en Internet se ven amenazados por el phishing. Los ciberdelincuentes que perpetran ataques de phishing pueden obtener acceso a información personal confidencial, como contraseñas, datos bancarios o números de tarjetas de crédito. Esta información puede ser utilizada para cometer fraudes, robar identidades o incluso silenciar a personas que expresan sus opiniones en línea.

La investigación puede contribuir a la protección de estos derechos y libertades fundamentales en el entorno digital. Por ejemplo, se podrían desarrollar nuevas tecnologías para proteger la privacidad de los datos en línea, fortalecer los marcos legales para castigar a los ciberdelincuentes y promover la educación sobre el uso responsable de Internet.

MARCO TEÓRICO

Desafíos tecnológicos

El autor Joaquim Serrahima nos enseña que

En su libro detalla que el peligro es inminente: que los ciberdelincuentes explotan la tecnología para robar datos con la ayuda de recursos que se encuentran en el Internet. Además, menciona que conforme la tecnología va avanzando, los delitos también. Es muy penoso que las leyes no sigan el mismo desafío de avanzar con el mismo auge en que la tecnología avanza; como consecuencia de esto lo único que se obtiene es impunidad frente al cometimiento de dicho delito, es de suma importancia que en nuestra actual legislación tome los correctivos necesarios. (Serrahima, 2009)

En estos tiempos, constantemente vemos el aumento de los delitos o fraude informático alrededor del mundo y más aún en países altamente desarrollados a nivel tecnológico, pero también debemos tomar en cuenta que este modo de delinquir es transfronterizo, es decir que cualquier persona puede cometer esta fechoría desde otra parte, ya sea un país o continente ajeno, por consecuencia de que el internet tiene un sistema global que nos mantiene enlazados a todos los que tenemos acceso.

Delitos por medio digitales

Los delitos por medio digitales son aquellos que se realizan con la ayuda de medios electrónicos y sistemas informáticos. “Los delitos informáticos se presentan en varias modalidades, como usurpación de la identidad, distribución de imágenes de agresiones sexuales contra menores, estafas a través de Internet, phishing (adquisición fraudulenta de información personal confidencial), entre otros”. (González, 2013, pág. 2).

En relación con la anterior cita, debemos entender que no todo delito que se realice por medio digital es un delito informático. Por ejemplo, si una persona envía amenazas de

muerte a otra persona por medio de un correo electrónico o alguna red social, esto no quiere decir que ya se esté cometiendo dicho delito.

El autor Jesús Alberto Loredo González nos enlista ciertos delitos o conductas punibles a continuación:

- Ataques contra sistemas y datos informáticos
- Usurpación de la identidad
- Distribución de imágenes de agresiones sexuales contra menores
- Estafas a través de Internet
- Intrusión en servicios financieros en línea
- Botnets
- Phishing

Ciberdelincuente

El ciberdelincuente es aquel sujeto activo que respecto a su conducta dolosa utiliza el espacio digital para su propio beneficio y causando daños a su víctima. En el contexto de la estafa por medios digitales, utiliza sitios web falsos que imitan a la perfección páginas legítimas para engañar a los usuarios y robarles información confidencial.

Lo hacen a través de correos electrónicos fraudulentos; convencen a las víctimas de que visiten estos sitios web falsos, que aparentan ser páginas de bancos, tiendas online o empresas de servicios públicos. Los usuarios incautos son inducidos a ingresar sus datos personales, como contraseñas, números de tarjetas de crédito e información personal. Esta información es utilizada por los delincuentes para realizar estafas, robar dinero o incluso suplantar la identidad de las víctimas.

Las características más frecuentes que poseen los correos electrónicos para engañar a los internautas son:

Los ciberdelincuentes buscan nuevas formas de engañar a las personas. Una de sus tácticas más comunes es el phishing, que consiste en enviar correos electrónicos fraudulentos que imitan la apariencia de mensajes legítimos de empresas reales; es decir, clonan la apariencia y funcionalidad de sitios web de empresas ya existentes. Esto les permite engañar aún más a las víctimas, ya que el sitio web falso parece ser idéntico al real.

Constantemente perfeccionando sus técnicas para engañar a las personas. Una de sus tácticas más recientes consiste en utilizar nombres de empleados reales de empresas en los correos electrónicos de phishing.

De esta manera, si la víctima intenta verificar la veracidad del correo electrónico llamando a la empresa, es posible que un empleado real confirme que la persona que figura como remitente del correo sí trabaja en la empresa; esto genera una falsa sensación de seguridad en la víctima, quien podría estar más propensa a revelar información confidencial o seguir las instrucciones del correo electrónico fraudulento.

Estafa

En nuestro marco legal encontramos el Código Orgánico Integral Penal art. 186, el delito de estafa. Nos menciona e interpretamos que este delito tiene por objetivo causar el error por medio del engaño hacia el sujeto pasivo a causa de que este tenga pérdidas patrimoniales, así afectando sus activos, para que el sujeto activo se vea beneficiado económicamente.

Elementos de la estafa

Estos son los elementos que hemos podido constatar en el anterior artículo del coip:

Engaño: se usa como estrategia la confianza o el desconocimiento de la víctima con la intención de hacerle creer algo verdadero pero que realmente es falso.

Error: sucede cuando el victimario induce al error, es decir que logra que la víctima se perjudique a sí misma.

Disposición Patrimonio: en el contexto de la estafa, es necesario que la víctima tenga algún tipo de patrimonio para que el actor del delito quiera actuar fraudulentamente.

Ánimo de lucro: Esto quiero decir que el actor lo hace con la intención de beneficiarse económicamente de manera ilícita.

Perjuicio patrimonial: La víctima pierde parte o la totalidad de su patrimonio, porque está cedé o transfiere su patrimonio al estafador, viéndose afectado por la estafa.

Así podemos deducir que la estafa se configura por los elementos anteriores. Es necesario que cumplan con todos esos componentes, ya que, si llegase a faltar uno o varios, cambiaría el tipo penal o no traería consecuencia penal. Por ejemplo: si (A) le dice a (B) mediante una red social que tiene en venta dos boletos en primera fila con el valor de 390.00 dólares americanos c/u, para el concierto de un cantante muy reconocido del país, pero esto es falso ya que boletos están adulterados y A solo quiere engañar a B para obtener su dinero, B accede y dice que sí quiere los boletos, pero B nunca le paga a (A) y así no pudo obtener sus “boletos”, salvándose indirectamente de ser estafado. Con este ejemplo podemos ver que faltaron los siguientes elementos: error y perjuicio patrimonial. Ahora bien, notamos cómo a falta de los elementos no se configura el hecho punible.

La estafa convencional por medios electrónicos o sistema informáticos

La estafa convencional de manera subjetiva es la que no necesariamente tiene que ser presencial la operación, sino que esta es realizada por un medio electrónico o sistema informático. “El elemento determinante de la nueva modalidad defraudatoria y que además permite filtrar los supuestos correspondientes a la estafa convencional, es la existencia de una manipulación informática”. (Martín, 2008, pág. 5) con esta cita informativa podemos decir que el fraude es un hecho típico con apariencia de delito, pero bajo la figura del delito de estafa, el fraude es un componente principal para la práctica del acto ilícito.

Fraude digital

En este tipo de conductas, los delincuentes manipulan datos o programas para obtener beneficios ilícitos. Una práctica común es la "sustracción de datos", donde el atacante accede a información confidencial sin necesidad de grandes conocimientos informáticos. En cambio, la manipulación de programas requiere de habilidades técnicas para modificar o insertar código en los sistemas.

Falsificaciones: Las falsificaciones digitales pueden ser de dos tipos:

- **Falsificación de objetos:** se altera información en documentos almacenados en computadoras o servidores.
- **Falsificación de instrumentos:** Se utilizan las computadoras para crear documentos comerciales falsos. La tecnología de fotocopiadoras a color ha facilitado este tipo de fraude, ya que permite modificar o crear documentos falsos con gran calidad, dificultando su distinción de los originales.

En ambos casos, los delitos informáticos representan un desafío para las autoridades debido a su complejidad y facilidad para pasar desapercibidos.

Bien jurídico protegido

Los bienes jurídicos protegidos que vulnera el delito informático, se podrían individualizar en indirectos y directos. Esto quiere decir que al vulnerar de manera directa a una persona se verá infringida en su entorno social; ahora, en la otra forma indirecta repercute a la sociedad en general, por lo cual se debe garantizar la seguridad y el desarrollo de la sociedad, en este contexto, siendo estos los siguientes bienes jurídicos que se pueden transgredir: seguridad jurídica y libertad informática. (Carcelén, y otros, 2017, pág. 13)

Pishing

El método de phishing quebranta la seguridad y protección de datos que se encuentran en el ciberespacio, en conjunto del ransomware, que esto es un tipo de malware, por consiguiente, creando y encontrando modelos para perpetuar los ciberdelitos. Los delincuentes

informáticos se capacitan de manera ágil y eficaz, gracias a la coordinación que mantiene la estructura de esta infracción ilícita, a causa de lo cual aprovecha el avance tecnológico, adaptándose sus batallas y colaborando de distintas maneras. (Interpol, s.f.).

En octubre de 2007, el Instituto Nacional de Tecnologías de la Comunicación (INTECO) de España publicó un estudio sobre el phishing, una práctica fraudulenta que afecta a usuarios y entidades tanto públicas como privadas. El estudio analiza los diferentes tipos de phishing y sus fases de evolución, destacando la complejidad de este tipo de delito debido a la rápida aparición de nuevas variantes y la combinación de diferentes técnicas. (Comunicación, 2017).

Actualmente, esta técnica se ha sofisticado y es utilizada para robar información confidencial como contraseñas, números de tarjetas de crédito e información personal.

¿Cómo funciona el phishing?

- *Recibes un correo electrónico falso*: Un ciberdelincuente te envía un correo electrónico que parece provenir de una empresa o institución legítima, como tu banco, una tienda online o un servicio público. El mensaje suele ser urgente o alarmante y te pide que realices una acción, como actualizar tus datos, verificar tu cuenta o descargar un archivo.
- *Haces clic en un enlace*: El correo electrónico contiene un enlace que te redirige a un sitio web falso. Este sitio web tiene la apariencia del sitio web real de la empresa o institución que supuestamente te ha enviado el correo electrónico.
- *Ingresas tu información confidencial*: En el sitio web falso, te piden que ingreses información confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios.
- *¡Tus datos están en manos de los ciberdelincuentes!* Una vez que ingresas tu información confidencial, los ciberdelincuentes la utilizan para realizar estafas, robar dinero o incluso suplantar tu identidad.

Modalidades de la técnica del phishing

Vishing: Se realiza mediante llamadas telefónicas. Los ciberdelincuentes utilizan software para marcar números automáticamente y, cuando la víctima responde, se activa una grabación que la intenta convencer de que visite un sitio web falso o revele sus datos personales.

Smishing: se realiza mediante mensajes de texto. Los ciberdelincuentes envían mensajes SMS a las víctimas, informándoles de un problema falso o una oferta atractiva. Si la víctima hace clic en el enlace o responde al mensaje, puede ser dirigida a un sitio web falso o proporcionar sus datos personales.

-Existen dos formas principales en que los ciberdelincuentes propagan este tipo de phishing:

1. Ingeniería social: Te engañan para que ejecutes el software malicioso. Por ejemplo, pueden enviarte un correo electrónico con un archivo adjunto que parece legítimo, pero que en realidad contiene malware. También pueden crear un sitio web falso que se parece a un sitio web legítimo y que te engañe para que descargues e instales software malicioso.

2. Explotación de vulnerabilidades: Aprovechan las fallas de seguridad en tu computadora o en un sitio web legítimo para instalar software malicioso sin tu conocimiento o consentimiento.

Fases del phishing

1. *Reconocimiento:* Los ciberdelincuentes buscan víctimas potenciales, recopilando información sobre ellas a través de redes sociales, sitios web no seguros o incluso métodos de ingeniería social.

2. *Planificación*: Una vez identificadas las víctimas, los ciberdelincuentes planifican el ataque, creando correos electrónicos o mensajes de texto personalizados que imitan a instituciones legítimas.

3. *Diseño:* Se diseña el sitio web falso o la página de aterrizaje que la víctima visitará, imitando con detalle el diseño y la funcionalidad del sitio web legítimo.

4. *Envío:* Los correos electrónicos o mensajes de texto se envían a las víctimas, utilizando técnicas de ingeniería social para generar confianza y persuadirlas de que hagan clic en los enlaces maliciosos.

5. *Recolección de datos:* Una vez que la víctima hace clic en el enlace, se la dirige al sitio web falso, donde se le solicita que ingrese información confidencial como contraseñas, datos bancarios o información personal.

6. *Explotación:* Los ciberdelincuentes utilizan la información robada para realizar fraudes, acceder a cuentas bancarias o vender los datos en la web oscura.

Es importante destacar que, si bien estas seis fases representan la estructura general de un ataque de phishing, la complejidad y el alcance de cada etapa pueden variar significativamente.

¿La técnica del phishing puedes ser un delito?

En este sentido, bien sabemos que en nuestro marco legal ecuatoriano no está tipificado el phishing y por ende no es un delito, pero cabe destacar que en cierto sentido el phishing podría encajar en la configuración de un delito. Para esto recurrimos en el estudio de fondo del delito en general hasta sus elementos esenciales.

¿Qué es el delito?

Es aquella conducta que tiene como resultado el perjuicio hacia una persona o un grupo de personas naturales / jurídicas, siendo esta conducta realizada por la acción u omisión del sujeto, en la cual implica una sanción penal a raíz de la prohibición de delitos existentes dentro de las normas de cada país.

El siguiente autor hace mención en su investigación al siguiente.

Profundizando sobre la definición de delito, es importante saber que, para poder determinar la responsabilidad penal de un sujeto a raíz de unos hechos determinados, ese delito debe reunir una serie de elementos que deben estar presentes. El concepto de delito está confirmado entonces por la concurrencia de 5 elementos: conducta, tipicidad, Antijuridicidad, culpabilidad y punibilidad, relacionados entre sí de manera lógica y secuencial. (Pellón, 2021).

Elementos del tipo procesal penal

Sujetos procesales: participan en proceso judicial.

- Sujeto activo; es aquella persona que realiza el delito prohibido por la ley.
- Sujeto pasivo; es la persona natural o jurídica que sufre daños o perjuicios.

Objeto: Está protegida por la ley acerca de la persona, bien o cosa.

- Material: es aquel que recibe el impacto como consecuencia de la acción delictiva.
- Jurídico: el bien jurídico tutelado, por ejemplo: el patrimonio.

Acción típica: se define como el acto que origina un delito y acarrea la sanción penal; se puede dividir en dos partes para mejor comprensión.

Acción objetiva: Es esencial para el tipo penal, ya que, a través de la conducta delictiva en materia penal, la cual acarea una amonestación por la vulneración de bien jurídico tutelado, a consecuencia de la relación entre la acción y el resultado.

Constituye el tipo objetivo, el sujeto, la acción (como la aparición externa del hecho producido por la conducta desarrollada por medio de verbos rectores como, sustraer, entrar en morada ajena, simular, entre otros), el bien jurídico. pueden integrar la relación de causalidad y la imputación objetiva. (Girón, 2021).

Acción subjetiva: Está claro que esta acción afecta al derecho subjetivo se analiza si la persona actúa con la intención de dañar físicamente, económicamente, etc., o de manera culposa.

Se refiere a la finalidad, el ánimo, la tendencia que impulsó actuar al sujeto activo a realizar la acción y la omisión, a título de dolo o de culpa. De este elemento se deriva el tipo doloso y el tipo culposo, y la doctrina dominante los incluye dentro de la tipicidad. (Girón, 2021).

¿Cómo se configura el delito?

Es importante que todos los elementos que configuren el delito cumplan con todos sus requisitos.

Tipicidad / Atipicidad: Conducta dolosa o culposa descrita en las normas que ocasiona la penalización; muy por lo contrario, la atipicidad es aquel comportamiento que no se encuentra escrito y por ende no cabe sanción.

Según el Dr. José Girón menciona en su artículo sobre lo que es la tipicidad, “Es la característica o cualidad que tiene una conducta (acción u omisión) de encuadrar, subsumir o adecuarse a un tipo penal”. Ahora bien, tipificar es la acción de encuadrar la conducta en un tipo penal. (Girón, 2021).

Antijurídica: Conducta que es opuesta a nuestras leyes que lesiona derechos.

La antijuricidad es lo contrario al Derecho; por lo tanto, no basta que la conducta encuadre en el tipo penal; se necesita que esta conducta sea antijurídica, considerando como tal, a toda aquella definida por la ley no protegida por causas de justificación, establecidas de manera expresa en la misma. (Michoacan, 2019)

Aunque se integre la antijuridicidad, ya que con la acción u omisión se afecta un bien jurídico protegido por el Derecho Penal, aunque se vaya contra la norma penal, se ponga en peligro o lesione un derecho; sucede que, en ocasiones, pueda el actor estar legitimado, autorizado o justificado, para llevar a cabo esta conducta antijurídica. (Soria, 2020).

Punibilidad:

En este sentido, el autor señala que “la punibilidad es la formulación de la prescripción, en la que se expresa mediante un sistema de símbolos para que sus destinatarios puedan conocerla”. (Ramírez, 2021). Bajo este podemos explicar que a partir de la tipificación de la norma y en conjunto de la antijurídica, se encasilla la punibilidad, es decir que la ley prevé y castiga a razón de las conductas o práctica del delito; en pocas palabras, impone la pena.

Conducta: es el comportamiento humano voluntario que debido a ello tiene como resultado una conducta positiva o negativa.

Culpabilidad:

La culpabilidad se puede dividir en dolo y culpa, pero también depende de la acción o la omisión que realice la persona. La diferencia es que el infractor realice el acto con intención de vulnerar o dañar, lo hace de forma dolosa, pero si lo hace de manera culposa no tiene intención de dañar o afectar, sin embargo, no se puede eximir su totalidad de la culpa, según los casos que se lleguen a presentar.

Según la concepción dominante, la imputabilidad es un presupuesto o el primer elemento del juicio de culpabilidad (se la define como capacidad de culpabilidad), y consiste en un determinado grado de normalidad en las facultades psíquicas del sujeto, que le permite conocer que el comportamiento que lleva a cabo es ilícito y actuar de acuerdo con dicha comprensión (Martínez Garay, 2007).

Límites de jurisdicción y competencia en los delitos digitales

A lo largo de la carrera de derecho nos encontramos con este término, jurisdicción y competencia, suele existir una confusión con sus conceptos. Entonces partimos mencionando que la competencia es el poder racionalizado o distribuido sobre la jurisdicción, siendo limitada sobre determinados asuntos, a diferencia de la jurisdicción es el poder general del

estado que es impartida mediante los tribunales como órganos imparciales para resolver dentro del territorio nacional.

Ahora bien, en los delitos informáticos se conoce que los agentes procesales pueden encontrarse en la misma localidad o en el exterior, es decir que aquellos delitos informáticos pueden ser cometidos de manera transnacional. A continuación, en la siguiente cita textual que recopilamos en la tesis de la autora Sofía Arrocha nos habla sobre la competencia para tener mayor compresión.

En el proceso penal la competencia es improrrogable, por lo que las normas que regulan los criterios para establecer qué órgano es el competente territorialmente para conocer de un asunto son imperativas y gracias a ellas podremos saber qué órgano va a poder conocer de un hecho concreto. (Arrocha, 2017, pág. 11).

Por lo tanto, para encontrar la forma de resolver y partir justicia buscando condenar a la persona responsable de la comisión de delitos transfronterizos e informáticos, llega a ser difícil o hasta casi imposible su búsqueda y su captura, dado que el victimario puede encontrarse en otro país o continente diferente al de su víctima. En tal caso se buscaría el apoyo de los órganos jurisdiccionales internacionales pertinentes e involucrados, por ej. El convenio de Budapest.

Podemos llegar a pensar que se abandona de alguna forma dicha característica imperativa del proceso penal, puesto que, al no existir reglas o criterios exactos y claros para poder determinar, por ejemplo, en este caso, la competencia de los órganos jurisdiccionales para conocer de delitos cometidos a través de Internet, se van a tener que buscar soluciones que hayan podido ser aportadas a nivel nacional o internacional. (Arrocha, 2017, pág. 11).

Sin embargo, a través del lugar donde se cometen los delitos es probable ubicar al sujeto y así aplicar justicia en la debida jurisdicción.

Se tendrá que analizar e investigar cuántos países, territorios e individuos se encuentran implicados con motivo de la comisión de la conducta penal y si alguno de ellos ha

decidido emprender un proceso penal en sus tribunales. Posteriormente, el juez o tribunal tendrá que resolver si se trata de un delito federal o estatal. (Velasco San Martin, 2012)

Configuración del delito		
Elementos esenciales del delito	**Phishing**	**Resultado**
Conducta	El agente activo tiene la intención (dolo) de engañar y dañar al sujeto pasivo, lucrándose de la información privada, confidencial e inclusive del patrimonio de la víctima.	Utiliza y envía a sus víctimas correos, llamadas, sitios web, todos fraudulentos con la intención de engañar y obtener beneficio propio.
Tipicidad / Atipicidad	No hay sanción, por ende, la conducta no está tipificada en la ley. Sin embargo, el phishing también es utilizado para delitos como: estafa; o apropiación fraudulenta por medios electrónicos.	No hay responsabilidad penal
Antijuricidad	La conducta vulnera o afecta el bien jurídico protegido de los siguientes; patrimonio, seguridad jurídica, privacidad personal o confidencial.	La conducta opuesta a la ley vulnera el bien jurídico tutelado.

Culpabilidad	El responsable tiene que realizar la acción de manera dolosa y consciente.	Consecuencias legales para el agente activo, responsabilidad civil y penal
Punibilidad	Imponer una pena	Cumplir la pena

Elaboración propia

Convenio de Ciberdelincuencia del Consejo de Europa

La definición del Convenio de Budapest es importante porque proporciona un marco legal común para combatir los delitos informáticos a nivel internacional. Esto ayuda a los países a cooperar en la investigación y enjuiciamiento de los delincuentes cibernéticos, así como a desarrollar leyes y políticas nacionales para prevenir y combatir este tipo de crimen. (Europeos, 2001)

Legislación comparada

El proyecto se basa en sólidos principios jurídicos para garantizar su viabilidad y legalidad. En el marco del siglo XXI, es fundamental establecer normas obligatorias que definan los derechos y deberes de los ciudadanos en relación con las Tecnologías de la Información y Comunicación (TIC).

Legislación sobre delitos informáticos en chile

Chile fue pionero en Latinoamérica en la lucha contra los delitos informáticos con la Ley 19.223, publicada el 7 de junio de 1993. Esta ley tipifica como delito la destrucción o inutilización de un sistema informático, con penas de prisión de un año y medio a cinco años. La ley no exige que el acceso al sistema sea ilegal, por lo que puede aplicarse a los creadores de virus. Si la acción afecta a los datos del sistema, la pena aumenta a entre tres y cinco años de prisión.

La ley en cuestión abarca 4 artículos, como son el sabotaje y el espionaje informáticos, aunque no los menciona explícitamente. El primer artículo se refiere claramente al sabotaje

de sistemas informáticos, mientras que los artículos 2 al 4 abordan el espionaje informático. Sin embargo, la ley no cubre otros delitos informáticos como la estafa digital o el hackeo.

Numeral 1: - Quien, con malicia, destruya o inutilice un sistema informático, sus componentes o partes, o impida, obstaculice o modifique su funcionamiento, será penado con prisión menor en su grado medio a máximo.

Numeral 2: - Quien, con la intención de robar, usar o acceder sin autorización a la información contenida en un sistema informático, la intercepte, interfiera o acceda a él, será penado con prisión menor en su grado mínimo medio.

Numeral 3: - Quien, con malicia, altere, dañe o destruya los datos almacenados en un sistema informático, será penado con prisión menor en su grado medio.

Numeral 4: - Quien, con malicia, revele o difunda información confidencial almacenada en un sistema informático, será penado con prisión menor en su grado medio. Si quien comete este delito es el responsable del sistema informático, la pena se agravará en un grado.

Similitudes y diferencias con la ley inglesa:

La ley chilena es similar a la inglesa, pero agrega la protección de la información privada.

Legislación sobre delitos informáticos en España

España cuenta con una amplia experiencia en la lucha contra los delitos informáticos, siendo uno de los países europeos con mayor desarrollo en este ámbito. La actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP), aprobada en 1999, consolida la protección de la información y contempla un amplio abanico de acciones tipificadas como delitos informáticos.

Delitos contemplados en la LOPDCP:

- **Obtención o violación de secretos:** Se sanciona la obtención o divulgación de información confidencial sin autorización.
- **Espionaje:** Se prohíbe la utilización de medios técnicos para obtener información privada sin consentimiento.
- **Divulgación de datos privados:** Se castiga la revelación de datos personales protegidos por la ley.
- **Estafas electrónicas:** Se tipifica como delito el uso de medios electrónicos para obtener un beneficio económico ilícito.
- **Hacking malicioso o militar:** Se sanciona el acceso no autorizado a sistemas informáticos con fines delictivos o para causar daños.
- **Phreaking:** Se prohíbe la manipulación de las telecomunicaciones con fines fraudulentos.
- **Introducción de virus:** Se castiga la creación o distribución de virus informáticos con la intención de causar daños.

Penas:

La LOPDCP establece penas de prisión y multas para los delitos informáticos. Las penas se agravan cuando el delito se comete con dolo o por parte de funcionarios públicos.

Código Penal:

El Código Penal español también contempla delitos informáticos, incluyendo la destrucción, alteración o inutilización de datos, programas o documentos electrónicos ajenos.

Legislación sobre información y tecnología en el Ecuador.

En Ecuador, la información es considerada un bien jurídico a proteger. La legislación ecuatoriana cuenta con diversas leyes y decretos que establecen marcos legales para el uso y protección de la información en el contexto de las tecnologías de la información y la comunicación (TIC). Entre las leyes más relevantes se encuentran:

1. **Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP):** Publicada en 2004, esta ley tiene como objetivo garantizar el derecho de acceso a la información pública, estableciendo la obligación de las instituciones del sector público de poner a disposición de la ciudadanía información sobre su estructura, funcionamiento, presupuesto, resultados, etc., a través de sus sitios web.

2. **Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos:** Esta ley regula el comercio electrónico, las firmas electrónicas y los mensajes de datos, brindando un marco legal para las transacciones electrónicas y la protección de la información en el ámbito digital.

3. **Ley de Propiedad Intelectual:** Esta ley protege los derechos de propiedad intelectual sobre obras literarias, artísticas, invenciones y otros productos creativos, incluyendo aquellos creados en el entorno digital.

4. **Ley Especial de Telecomunicaciones:** Esta ley regula el sector de las telecomunicaciones en Ecuador, estableciendo las normas para la prestación de servicios de telecomunicaciones, la gestión del espectro radioeléctrico y la protección de los usuarios.

5. **Ley de Control Constitucional (Reglamento Habeas Data):** Esta ley establece el derecho de Habeas Data, que permite a las personas acceder a la información personal que sobre ellas conste en bases de datos públicas o privadas y solicitar su rectificación, cancelación o actualización.

Consideraciones adicionales:

- La Constitución Política de Ecuador de 2008, en su artículo 81, reconoce el derecho de acceso a la información pública como un derecho fundamental de las personas.
- Las disposiciones contenidas en la Constitución Política del Ecuador vigente, en su capítulo tercero de las Garantías Jurisdiccionales de sus secciones cuarta y quinta de los Art. 91 y 92 sobre la acción de acceso a la información pública y acción de Habeas Data, también establecen dichas garantías.

Un estudio realizado por el Grupo Faro 17 en marzo de 2007 reveló que los Ministerios ecuatorianos, en promedio, solo cumplen con el 49% de las obligaciones establecidas en la Ley Orgánica de Transparencia y Acceso a la Información. Esto significa que casi la mitad de la información que debería estar disponible al público no lo está, lo que representa un obstáculo significativo para el ejercicio del derecho a la información y la transparencia en el sector público ecuatoriano. (Faro, 2007)

La Defensoría del Pueblo, como organismo encargado de vigilar y garantizar el cumplimiento de la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), realizó un estudio en el que se analizaron 380 instituciones públicas. El estudio reveló que 291 instituciones cumplen con la publicación de su información según lo establecido en la ley, mientras que a 89 se les notificó para que cumplan con sus obligaciones.

De las instituciones que no cumplían inicialmente, 72 solicitaron una prórroga para completar los requisitos, 70 cumplieron tras recibir la notificación y 17 no respondieron. 12 instituciones indicaron que sus páginas web estaban en construcción y 7 no cumplieron con las disposiciones de la ley en ningún momento.

En la provincia del Guayas, la Defensoría del Pueblo firmó un convenio con Participación ciudadana en junio de 2008 para promover el cumplimiento de la LOTAIP en la región.

MARCO METODOLÓGICO

1. Enfoque de la investigación:

En la presente investigación, se optó por un enfoque metodológico cualitativo. Este enfoque se centra en analizar el objeto de estudio y su impacto en un grupo específico de ciudadanos. El objetivo es comprender la relación entre el objeto de estudio y el colectivo, y cómo esta relación puede ser mejorada o modificada. Para ello, se recurrirá al análisis y estudio de las opiniones de expertos en la materia.

El enfoque cualitativo en la investigación se utiliza para analizar información no numérica, como conceptos, opiniones y experiencias, con el objetivo de comprender a fondo la problemática en estudio. A diferencia del enfoque cuantitativo que se basa en datos numéricos y estadísticos, el enfoque cualitativo profundiza en las perspectivas y vivencias de las personas, permitiendo obtener resultados comprensibles que describen y explican la situación de manera detallada. (Malagón, Morales, Malagón, Santos, & E., 2014)

2. Tipo de investigación:

En esta investigación se utilizó un enfoque explicativo. Esto significa que se analizaron los elementos que componen el problema y cómo estos impactan al individuo. El objetivo fue comprender las relaciones causales entre estos elementos y el problema en sí.

La investigación explicativa tiene como objetivo principal descubrir las causas de los fenómenos, eventos o procesos que conforman una problemática. Esto permite comprender mejor la naturaleza del problema y sentar las bases para futuras investigaciones. Al identificar las causas, se puede analizar el problema en profundidad y desarrollar soluciones más efectivas. (Castro-Maldonado., Gómez-Macho., & Camargo-Casallas, 2023)

Junto con la investigación explicativa, se utilizó un enfoque descriptivo. Esto permitió describir en detalle la problemática de la estafa digital a través de internet en la modalidad

phishing durante el periodo 2023. El objetivo fue comprender las características, dimensiones y manifestaciones del problema, proporcionando una base sólida para el análisis explicativo. La investigación descriptiva recopila y organiza datos sobre la problemática, permitiendo obtener una imagen clara y precisa de la situación.

La investigación descriptiva, también llamada investigación de diagnóstico, se centra en estudiar a fondo una problemática social. Para ello, describe con precisión las actividades, objetos, procesos y personas que la componen. El objetivo es identificar las relaciones que existen entre las diferentes variables involucradas y obtener conclusiones significativas que aporten al conocimiento sobre el tema. (Morales, 2012)

Periodo y lugar de investigación

El periodo que se eligió para realizar el trabajo de investigación fue del año 2023, lugar seleccionado, ciudad de Guayaquil.

Universo y muestra de la investigación

Universo

El universo es el conjunto de elementos que serán estudiados y analizados para obtener los datos necesarios y así poder llegar a una conclusión. Este conjunto puede incluir personas, fenómenos, objetos o cualquier otra cosa relevante para la investigación. La selección del universo adecuado es crucial para asegurar la validez y confiabilidad de los resultados. (Condori-Ojeda, 2020).

En esta investigación, el universo está compuesto por los elementos jurídicos que definen el delito de estafa que es realizado a través del internet bajo la modalidad phishing. Actualmente no está tipificado en el Código Orgánico Integral Penal (COIP), por lo que la investigación busca identificar y analizar los elementos que lo caracterizan para contribuir a su tipificación legal.

La muestra es un subconjunto del universo de la investigación, cuidadosamente seleccionado por el investigador. Se espera que esta muestra sea representativa del universo, permitiendo obtener resultados generalizables a toda la población. La selección de una muestra adecuada es crucial para la validez y confiabilidad de la investigación. (López, 2004).

Métodos empíricos

La entrevista

En esta investigación se utilizará la metodología de entrevistas para recopilar información valiosa sobre el delito de estafa a través del internet bajo la modalidad phishing. Se elaborarán preguntas específicas para obtener las opiniones, experiencias y conocimientos de abogados expertos en derecho penal y derecho informático.

Las entrevistas permitirán comprender el problema desde diferentes perspectivas profesionales y obtener información crucial para formular conclusiones relevantes.

En la técnica de la entrevista, un entrevistador formula preguntas personalizadas a un entrevistado. El objetivo es obtener información valiosa sobre las experiencias, opiniones, conocimientos y valoraciones del entrevistado en relación al tema de estudio.

La entrevista permite establecer un diálogo con el entrevistado, lo que facilita la recopilación de información detallada y profunda. Esta técnica es útil para comprender diferentes perspectivas y obtener información que no se puede obtener a través de otros métodos. (Murillo Torrecilla, 2007).

Interpretación de resultados.

En relación al delito de estafa a través de la modalidad phishing, los expertos que fueron consultados supieron explicar que la estafa realizada bajo esta modalidad como es el phishing es un delito que cada día afecta a más personas, en las que aprovechan la facilidad con la que pueden ocultar su identidad y ubicación mediante uso de softwares; el abogado Ricardo Sierra destacó que la sociedad es poco atenta y crédula y con poco conocimiento

acerca del alcance que tiene el internet, por eso que es muy común que exista este tipo de fraudes, por lo que enfatizó que debe existir resoluciones que amplíen más el tema con la finalidad de detener, prevenir y erradicar de acuerdo a la gravedad causada, con la finalidad de que esto no quede impune, el abogado Guaman Sagñay hace referencia a que con la llegada de la tecnología ha fomentado los ciberdelitos, ya que los ciberdelincuentes se aprovechan de que al estar detrás de un computador pasan desapercibidos y no van a poder ser identificados. El delito de estafa está tipificado en el art 186 del coip sin embargo no está debidamente señalado por eso considera que se debe reformar el coip para tipificarlo como tal. También hace referencia a que las personas deben tener mucha precaución al momento de compartir información en la web.

Al realizar la consulta a los expertos sobre las causas que conllevan a que las personas cometan este tipo de delito de estafa utilizando la técnica phishing, los expertos establecen varios motivos, como por ejemplo que las víctimas no cuentan con una correcta protección digital, aparte que al delincuente no es fácil poder rastrearlo y que el usuario se puede dejar llevar por un entorno digital falso pensando que es el original; la abogada Judy Tutiven Galvez recalcó que es viable la reforma al coip para incluir este delito, debido que cada día aumenta de manera considerable las estafas bajo esta modalidad, ya que el internet es una herramienta de fácil acceso. Debido a esto, los delincuentes hacen de la suya.

Cuando se consultó a los expertos si consideraban que dentro de nuestra legislación ecuatoriana existan normas que permitan combatir este tipo de delito, gran parte de los entrevistados tuvieron similares respuestas, debido a que nuestro país tiene mínimas regulaciones que permitan combatir este ilícito. El Abogado Alex López Ávila mencionó que el art 186 del coip en el que se hace referencia a la estafa puede ser utilizado para este mismo tipo de estafa digital. Podemos evidenciar que puede ser confundido por el tipo penal de apropiación a través de medios electrónicos.

El abogado Carlos Caranqui Morocho menciona que debido a su difícil identificación y el alcance que pueden tener sus efectos, es decir, puede estar en cualquier parte del mundo

y puede estafar a miles de personas, considera necesario una reforma al coip para que este tipificado como tal y de esta manera sancionar sin dilaciones; el abogado Bryan López Robles menciona que en nuestra legislación si existen disposiciones, pero que no son del todo efectivas como en otros sistemas, por lo tanto el coip debe ser reformado para que así de esta manera examinar en todos los ámbitos la conducta como delito, agravantes, pena.

En la actualidad, las plataformas digitales se han convertido en espacios donde individuos sin escrúpulos aprovechan la confianza de otros para obtener beneficios económicos a costa de sus víctimas. Sin embargo, en Ecuador, la seguridad jurídica contra este tipo de delitos informáticos es limitada.

Si bien el artículo 186 del Código Orgánico Integral Penal (COIP) puede ser utilizado para sancionar las estafas digitales, este resulta insuficiente para abordar la problemática en su totalidad. Incluso, existe la posibilidad de confusión con el tipo penal de apropiación fraudulenta por medios electrónicos.

Ante esta situación, se hace evidente la necesidad de realizar reformas en el ordenamiento jurídico penal ecuatoriano. La mejor solución sería establecer la estafa bajo la técnica phishing como un nuevo delito dentro del COIP, con una tipificación clara y precisa, agravantes específicas y penas proporcionales al daño causado.

Esta medida permitiría combatir de manera más efectiva este tipo de delitos, proteger a los ciudadanos y enviar un mensaje claro de que este tipo de actividades ilícitas no serán toleradas.

Justificación

De acuerdo al análisis realizado de toda la información que concierne al marco teórico, y al criterio de los expertos en derecho penal obtenido a través de las entrevistas realizadas, hemos llegado a deducir que es necesaria de una reforma al código orgánico integral penal

para tipificar este tipo de delitos de estafa a través de la web bajo la modalidad phishing como un delito autónomo de estafa

Con el único fin de sancionar de manera correcta y eficaz a quienes cometen este tipo de delito. Este trabajo de investigación es relevante y esencial para profundizar un poco más sobre este problema de estafa bajo la técnica phishing, y cómo los ciberdelincuentes atacan de manera constante a sus víctimas con más frecuencia.

Cabe mencionar, que la propuesta de adherir un nuevo articulado al coip donde se establezca el delito de estafa bajo la modalidad phishing, es esencial, debido que en nuestro país actualmente hay falencias tanto de garantías como de seguridad informática. adicionalmente, podemos concluir que intentar sancionar este tipo de estafa digital como si fuese ordinaria, solo llevaría a procesos demorados e ineficientes al momento de sancionar al ciberdelincuente.

El estafador tiene como finalidad de apropiarse del patrimonio de su posible víctima, aprovechándose de su ingenuidad y haciendo uso de su argucia. En pocas palabras, cuando se intente sancionar este tipo de delito como una estafa común, ordinaria, se omitiría el factor principal e importante, el uso de plataformas digitales, lo que llevaría a que estos procesos no se resuelvan con la celeridad ni la decisión adecuada.

Este tipo de estafa digital, puede tener similares características a otros delitos, el uso de plataformas digitales lo hace un delito diferente, el uso de sistemas informáticos permite que el delincuente cometa el delito sin utilizar su identidad, es más sin siquiera dejar algún rastro que lo identifique, ya eso depende del conocimiento que tenga el delincuente en ingeniería.

Con lo expuesto anteriormente, se demuestra la importante necesidad de implementar la propuesta mencionada, con el único objetivo de minimizar los procesos y sancionar adecuadamente sin dejar impune.

Propuesta

De acuerdo al estudio realizado y a la evidente problemática que existe, proponemos que el código orgánico integral penal sea reformado, con la finalidad que en el artículo 186 se agregue el siguiente artículo.

Art 186.1: - Estafa digital. La persona que realice cualquiera de las actividades fraudulentas mencionadas en el artículo anterior, utilizando dispositivos electrónicos o plataformas digitales con el objetivo de causar un daño al patrimonio, ya sea de otra persona o un tercero, se sancionará con una pena que prive de su libertad de cinco a siete años, de acuerdo con las reglas establecidas en el artículo 186. Se aplicará la pena máxima en los siguientes casos:

1. La persona u organización que con ayuda de alguna plataforma digital suplante la identidad de una persona, ya sea natural o jurídica, con la intensión de causarle perjuicio.
2. La persona u organización que a través de artimañas y con ayuda de sistemas informáticos cree una identidad falsa con la finalidad de cometer delitos.
3. La persona u organización, que, a través de engaños, instale programas maliciosos en el dispositivo electrónico de la víctima, en la que permita tener acceso a datos de carácter personal o que le cauce daño al equipo electrónico.

Si se llega a comprobar la responsabilidad penal del individuo por el cometimiento de alguna conducta que va en contra del ordenamiento jurídico, debe ser sancionado con una multa que puede ir de cien a doscientos salarios básicos unificados.

Conclusiones

Finalmente, se analizó y demostró que no existen las medidas de seguridad adecuadas ni las garantías necesarias para proteger de manera eficaz la información personal o confidencial de los usuarios o empresas, en donde se cometen las “estafas digitales”, así es como lo denominamos en este trabajo. dicho de otro modo, es la realidad

existente la falta de tipificación de este tipo de conductas delictivas que operan dentro de territorios nacionales o transnacionales.

Sin embargo, también hay que resaltar que existe poco conocimiento sobre su prevención, puesto que, a pesar de que las víctimas en ciertas ocasiones pueden ser responsables de las estafas digitales, a consecuencia, que los usuarios no tienen el conocimiento necesario en informática y no cuentan con la seguridad necesaria para evitar las estafas digitales.

Segundo, la identificación del derecho vulnerado es la seguridad jurídica, que a la misma vez mencionamos la seguridad informática. en este ámbito, encontramos que es una garantía constitucional, ya que la información privada o particular de la persona natural o jurídica es propia de sí mismo, y al momento que se acceda sin autorización o bajo una conducta ilegal para consentir el ingreso de dicha información, se verán vulneradas estas garantías.

En el artículo 186 del COIP, se ha demostrado que es necesario establecer al delito de estafa bajo la modalidad phishing como un delito autónomo, no como únicamente otra forma en la cual se comete el delito de estafa sin ser mencionado en el código. Esto tiene como único fin evitar dilaciones y ser ágil y eficiente al momento de sancionar.

Podemos constatar que en la legislación penal ecuatoriana carece de las regulaciones necesarias para sancionar los delitos que se cometen en plataformas digitales. Hay un cierto vacío. Por lo tanto, es necesario establecer una ley específica para sancionar estos delitos. Reformar el COIP para incluir un nuevo capítulo que categorice los delitos informáticos, así es como dentro de nuestro trabajo de titulación se estableció una propuesta de reforma al COIP, que tal vez se incluya más adelante en nuestras normas penales.

El phishing, más allá de ser una conducta ilegal para la obtención de información personal o reservada bajo engaños, representa una grave amenaza para la seguridad de los

individuos. Al obtener datos importantes, los ciberdelincuentes no solo pueden causar pérdidas económicas, sino también vulnerar la identidad y la privacidad de las víctimas.

Del párrafo anterior, también señalamos que, a través de la modalidad del phishing, se puede aperturar una serie de delitos o conductas delictivas, como el robo de información, suplantación de identidad o apropiación fraudulenta por medios electrónicos, ya tipificado en el coip.

El internet ha sido de gran ayuda en nuestras vidas; gracias a esto podemos estar comunicados, tener acceso a información, realizar trabajos de manera remota, es decir, desde cualquier parte del mundo. Incluso ha sido de gran ayuda tanto para el comercio como para la educación. En nuestro país se han esforzado para mejorar las infraestructuras de la tecnología, para así fomentar un desarrollo en la creación de industrias tecnológicas.

Sin duda, la tecnología ha avanzado de manera asombrosa y se estima que en unos cuantos años más esta tecnología avanzará en conjunto con la inteligencia artificial. Será un gran desafío en el que se debe mejorar a medida que evoluciona nuestra era, para así de esta manera tener un mejor control con los delitos tales como el phishing. Es necesario que el Ecuador invierta en investigaciones, desarrollos y seguridad para prevenir este tipo de delitos. Los ciberdelincuentes estarán siempre en busca de una posible víctima sin importar de que país sea.

Recomendaciones

Es fundamental que el gobierno central lidere una campaña de concienciación para educar a la población ecuatoriana sobre los riesgos del entorno digital. Esta iniciativa debe llegar a todos los sectores de la sociedad, utilizando diversos canales de comunicación y enfatizando las graves consecuencias de no tomar las precauciones necesarias al navegar por internet.

Se recomienda a la Asamblea Nacional del Ecuador realizar un estudio de los casos de estafas digitales bajo la modalidad phishing en nuestro país. Este análisis permitirá comprender las tendencias, las modalidades más comunes y el impacto real de este problema en la sociedad ecuatoriana, y que la reforma al coip es necesaria.

La recomendación a la sociedad es que tienen que estar atentos, ya que hay muchas modalidades de delitos utilizando la tecnología, ya que cualquiera puede ser víctima de este tipo de conductas, como es el phishing.

Las instituciones financieras o entidades públicas jamás solicitan información de carácter personal a través de correos electrónicos o por cualquier medio digital; este tipo de información es requerida de manera presencial con la única finalidad de garantizar la seguridad del usuario.

Actualmente no contamos con una adecuada legislación penal con respecto al phishing, pero se debería hacer un esfuerzo por controlar y frenar este tipo de delito. Cabe recalcar que el phishing al no estar tipificado como delito hay un vacío, el principio de legalidad (Nullum crimen, Nulla Poena Sine Lege) nos indica que debe estar tipificado para que sea considerado como tal y así de esta manera no quede impune y evitar que este tipo de delito aumente.

Referencias

Arrocha, S. (marzo de 2017). *Universidad de La Laguna.* Obtenido de Universidad de La Laguna: https://riull.ull.es/xmlui/bitstream/handle/915/4335/CIBERDELINCUENCIA%20PROBLEMAS%20EN%20LA%20DETERMINACION%20DE%20LA%20JURISDICCION%20Y%20COMPETENCIA%20DE%20LOS%20TRIBUNALES%20EN%20EL%20ORDEN%20PENAL.pdf?sequence=1&isAllowed=y

Carcelén, J. M., Mier, E. F., Falconí, J. G., Cabezas, R. V., Carcelén, M. R., Dayán, A. P., . . . Márquez, Á. R. (Diciembre de 3 de 2017). *CORTE NACIONAL DE JUSTICIA* . Obtenido de CORTE NACIONAL DE JUSTICIA : https://www.cortenacional.gob.ec/cnj/images/pdf/publicaciones_cnj/Temas%20Penales%203.pdf

Castro-Maldonado., J., Gómez-Macho., L., & Camargo-Casallas. (1 de Enero de 2023). *Universidad Distrital Francisco Jóse de Caldaz.* Obtenido de Universidad Distrital Francisco Jóse de Caldaz: https://doi.org/10.14483/22487638.19171

Comunicación, I. N. (octubre de 2017). Estudio sobre usuarios y entidades publica y privadas afectada por la práctica fraudulenta conocida como el phising. *Estudio phishing observatorio_inteco*. España.

Condori-Ojeda, P. (2020). *Acta Académica.* Obtenido de Acta Académica: https://www.aacademica.org/cporfirio/18

Cristina, C. A. (26 de AGOSTO de 2014). EL PRINCIPIO DE PROPORCIONALIDAD EN LA PREVENCION DE LOS DELITOS INFORMATICOS. *EL PRINCIPIO DE PROPORCIONALIDAD EN LA PREVENCION DE LOS DELITOS INFORMATICOS*. Ibarra, Imbabura, Ecuador: UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES.

daily, k. (06 de 07 de 2018). Obtenido de https://latam.kaspersky.com/blog/data-breach-stress/13124/

Europeos, S. d. (23 de junio de 2001). *Convenio sobre la cyberdelincuencia .* Obtenido de Convenio sobre la cyberdelincuencia : https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Faro, G. (2007). *Grupo Faro*. Obtenido de Grupo Faro: Grupo Faro, Acción Colectiva para el Bienestar Público

Girón, J. (2021). Teoria del delito. En J. Girón, *Teoria del delito* (págs. 64-65). Guatemala .

González, J. A. (enero; junio de 2013). Delitos informáticos: su clasificación y vision general de las medidas de acción para combatirlo. *Delitos informáticos: u clasificación y vision general de las medidas de acción para combatirlo*. San Nicolas de los Garza, Nuevo León, México. Obtenido de Portal de Recursos Educativos y Digitales.

Interpol. (s.f.). *Interpol*. Obtenido de Interpol: https://www.interpol.int/es/Delitos/Ciberdelincuencia

López, P. (2004). *Población, muestra y muestro.* Cochabamba: Punto cero.

Malagón, G. V., Morales, J. Á., Malagón, A. V., Santos, N. C., & E., G. L.-A. (mayo de 2014). *PARADIGMAS EN LA INVESTIGACIÓN, ENFOQUE CUANTITATIVO Y CUALITATIVO.* Mexico: Facultad de Medicina de la Universidad Autónoma de Querétaro. Obtenido de PARADIGMAS EN LA INVESTIGACIÓN.

Martín, A. M. (2008). "Estafa convencional, estafa informática y robo en el ámbito de los medios electrónicos de pago. El uso fraudulento de tarjetas y otros instrumentos de pago". *Revista Electrónica de Ciencia Penal y Criminología*, 5.

Martínez Garay, L. (2007). Imputabilidad y elementos del delito. *Estudios de Derecho Judicial*, 93-136.

Michoacan, P. j. (2019). *Poder judicial Michoacan.* Obtenido de Poder judicial Michoacan: https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap2.htm#:~:text=2.2%20ELEMENTOS%20DEL%20DELITO.%2D&text=Positivos%20Negativos.&text=b)%20Tipicidad%20b)%20Ausencia%20de,d)%20Imputabilidad

Morales, F. (2012). *Investigación Descriptiva.* Obtenido de Investigación Descriptiva: http://www. creadess. org/index. php/informate/de-interes/temas-deinteres/17300-conozca-3-tiposde-investigacion-descriptiva-exploratoria-yexplicativa

Murillo Torrecilla, F. J. (2007). *Universidad de la Rioja.* Obtenido de Universidad de la Rioja: https://avances.adide.org/index.php/ase/article/view/267/220

Pellón, P. (27 de diciembre de 2021). *Palladino Pellón*. Obtenido de Palladino Pellón: https://www.palladinopellonabogados.com/definicion-de-delito/

Ramírez, E. I. (2021). *Dialnet.* Obtenido de Dialnet: file:///C:/Users/DENIS/Downloads/Dialnet-LaPunibilidadEnLaTeoriaDelDelito-8359989%20(2).pdf

Serrahima, J. (2009). *La amenza digital.* Barcelona: Profit.

Soria, Y. L. (2020). *repositorio institucional uca*. Obtenido de repositorio institucional uca: https://repositorio.uca.edu.ar/bitstream/123456789/11122/1/teoria-delito-revision-critica.pdf

Unidas, O. d. (12 de junio de 1998). *ONU*. Obtenido de ONU: https://uncitral.un.org/es/texts/ecommerce

Velasco San Martin, C. (2012). *La jurisdicción y competencia sobre delitos cometidos a través de Sistemas de Cómputo e Internet.* Valencia: Tirant lo Blanch.

Anexos

Entrevistas a profesionales del derecho en materia penal.

Experto 1:

Abg. Ricardo sierra BOLAGAY

Graduado en la Universidad Tecnológica Ecotec

Abogado del consultorio jurídico de la Universidad Ecotec

1. **¿Qué opina usted sobre la estafa digital realizada mediante la técnica del phishing?**

   R. Mi opinión respecto al tema es que la sociedad es poco atenta, crédula y con desconocimiento del alcance del internet y sus malos usos. Por lo que caer en esto es muy común para la población que ignora estos temas.

2. **Desde su punto de vista, ¿Cuáles son las motivaciones más comunes que llevan a una persona a comer este tipo de delito de estafas digitales?**

   R. Obtener dinero o información que sea valiosa o de utilidad para el delincuente.

3. **¿Considera usted que en nuestra legislación ecuatoriana existen disposiciones que permitan combatir la estafa digital mediante la técnica del phishing?**

   R. La normativa penal habla acerca de la estafa, y en uno de sus incisos detalla a los medios electrónicos para su cometido. Pero no ahonda en las técnicas y demás mecanismos que se emplean en esto. Por lo cual si debería existir resoluciones que amplíen más el tema para su identificación, detección, prevención, erradicación, sanción de acuerdo a la gravedad; esto en un sentido más amplio al prescrito en el tipo penal de estafa tipificado en el COIP.

4. **¿Cree usted que el Código Orgánico integral penal debería ser reformado para incluir el phishing como un delito autónomo?**

R. No. El Phishing es técnicamente la estafa por medios digitales o electrónicos, y esto ya está tipificado, pero poco conceptualizado como para dar respaldo a fiscales, jueces o abogados que estén frente a esta conducta antijurídica.

Experto 2:

***Abg**. JUAN BOLIVAR GUAMAN SAGÑAY*

1. **¿Qué opina usted sobre la estafa digital realizada mediante la técnica del phishing?**

   R. Con la llegada de la tecnología también han llegado los ciberdelitos en este caso las estafas en línea, misma que en primera instancia la víctima debe tener mucha precaución al momento de compartir información personal u otros datos, por otro lado, este delito debe ser combatida con todo el rigor de la ley a persona que se dedica este tipo de infracciones

2. **Desde su punto de vista, ¿Cuáles son las motivaciones más comunes que llevan a una persona a comer este tipo de delito de estafas digitales?**

   R. Considero que la persona o personas que se dedican a este tipo de delitos lo hacen en primer lugar pensando que al estar atrás de un computador pasan desapercibidos o que no van a poder dar con su responsabilidad, pero sin embargo este no es tan cierto toda vez que con la misma tecnología y las técnicas investigativas avanzadas también se pueden llegar a determinar desde donde proviene este tipo de delitos inclusive desde que país.

3. **¿Considera usted que en nuestra legislación ecuatoriana existen disposiciones que permitan combatir la estafa digital mediante la técnica del phishing?**

   R. En nuestra normativa legar la estafa en línea mediante la modalidad de phishing no está tipificado tal cual, está tipificada de manera general en el Art. 186 más sin embargo esta modalidad no está debidamente señalada.

4. **¿Cree usted que el Código Orgánico integral penal debería ser reformado para incluir el phishing como un delito autónomo?**

R. Considerando el alcance tecnológico y las nuevas modalidades de estafa a través de esta vía es pertinente la reforma al COIP, ya que cada día aumenta este tipo de infracciones y perjudica a muchas personas en su patrimonio.

Experto 3:

Abg. Judy Vanessa Tutiven Galvez

1. **¿Qué opina usted sobre la estafa digital realizada mediante la técnica del phishing?**

   R. Es un tipo de estafa que está subiendo por cuanto las personas no somos cuidadosas con los mensajes que recibimos y tendemos a aceptar todo.

2. **Desde su punto de vista, ¿Cuáles son las motivaciones más comunes que llevan a una persona a comer este tipo de delito de estafas digitales?**

   R. Es una herramienta de fácil acceso para el delincuente

3. **¿Considera usted que en nuestra legislación ecuatoriana existen disposiciones que permitan combatir la estafa digital mediante la técnica del phishing?**

   R. Existe la apropiación fraudulenta pro medios electrónicos que es el medio por el cual se podría juzgar este tipo de delitos.

4. **¿Cree usted que el Código Orgánico integral penal debería ser reformado para incluir el phishing como un delito autónomo?**

   R. Como una reforma de necesidad eminente no sin embargo si sería viable su inclusión en la ley.

Experto 4:

Abg. Carlos Armando Caranqui Morocho

1. **¿Qué opina usted sobre la estafa digital realizada mediante la técnica del phishing?**

R. Considero que es uno de los métodos nuevos para cometer infracción y que sus víctimas podrían ser en multitud.

2. **Desde su punto de vista, ¿Cuáles son las motivaciones más comunes que llevan a una persona a comer este tipo de delito de estafas digitales?**

   R. Considero que a través de la plataforma digital la identificación del estafador es más difícil identificarlo y ubicarlo.

3. **¿Considera usted que en nuestra legislación ecuatoriana existen disposiciones que permitan combatir la estafa digital mediante la técnica del phishing?**

   R. Claro que sí, establece sanciones a aquellos que cometen infracciones por medios digitales.

4. **¿Cree usted que el Código Orgánico integral penal debería ser reformado para incluir el phishing como un delito autónomo?**

   R. Considero que debe existir una reforma al COIP en la parte que corresponda a la identificación del que comete infracción utilizando el phishing.

Experto 5:

Abg. Alex López Ávila

Docente de la universidad Ecotec

Fiscal

4. **¿Qué opina usted sobre la estafa digital realizada mediante la técnica del phishing?**

   R. Que es una modalidad muy vista hoy.

5. **Desde su punto de vista, ¿Cuáles son las motivaciones más comunes que llevan a una persona a comer este tipo de delito de estafas digitales?**

   R. La ingenuidad de la gente.

6. **¿Considera usted que en nuestra legislación ecuatoriana existen disposiciones que permitan combatir la estafa digital mediante la técnica del phishing?**

   R. Si, las mismas que todos los delitos.

7. **¿Cree usted que el Código Orgánico integral penal debería ser reformado para incluir el phishing como un delito autónomo?**

   R. No, ya que está tipificado en el 186.

Experto 6:

Abg. Bryan López Robles

Abogado en libre ejercicio

1. **¿Qué opina usted sobre la estafa digital realizada mediante la técnica del phishing?**

   R. Evidentemente es una modalidad de estafa que funciona de distintas formas, lo más perjudicial son los efectos negativos que este deja ya que al efectuarse deja vulnerable a la víctima con sus datos y otras informaciones personales, se debería tomar medidas más eficientes para contrarrestarlo.

2. **Desde su punto de vista, ¿Cuáles son las motivaciones más comunes que llevan a una persona a comer este tipo de delito de estafas digitales?**

   R. Entre las motivaciones se podrían encontrar factores económicos, socio-culturales, y evidentemente a la fecha los grupos de delincuencia organizada.

3. **¿Considera usted que en nuestra legislación ecuatoriana existen disposiciones que permitan combatir la estafa digital mediante la técnica del phishing?**

   R. En efecto las hay, aun así, cabe señalar que no pueden ser tan eficiente como en otros sistemas.

4. **¿Cree usted que el Código Orgánico integral penal debería ser reformado para incluir el phishing como un delito autónomo?**

   R. En efecto, así la figura podría ser mejor examinado en todos los ámbitos, en cuestión de delito, agravantes, pena, etc.

Anexo 2

Formato de preguntas

Título: Análisis del delito de estafa a través del internet en la modalidad phishing en la ciudad de Guayaquil, en el año 2023.

Preguntas:

1. **¿Qué opina usted sobre la estafa digital realizada mediante la técnica del phishing?**

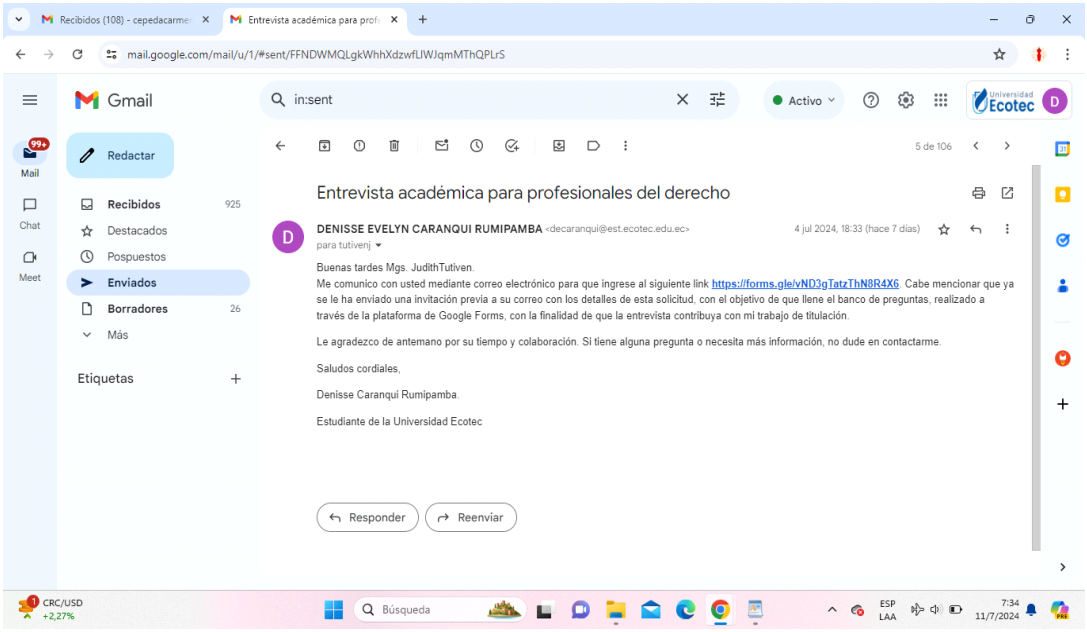
2. **Desde su punto de vista, ¿Cuáles son las motivaciones más comunes que llevan a una persona a comer este tipo de delito de estafas digitales?**

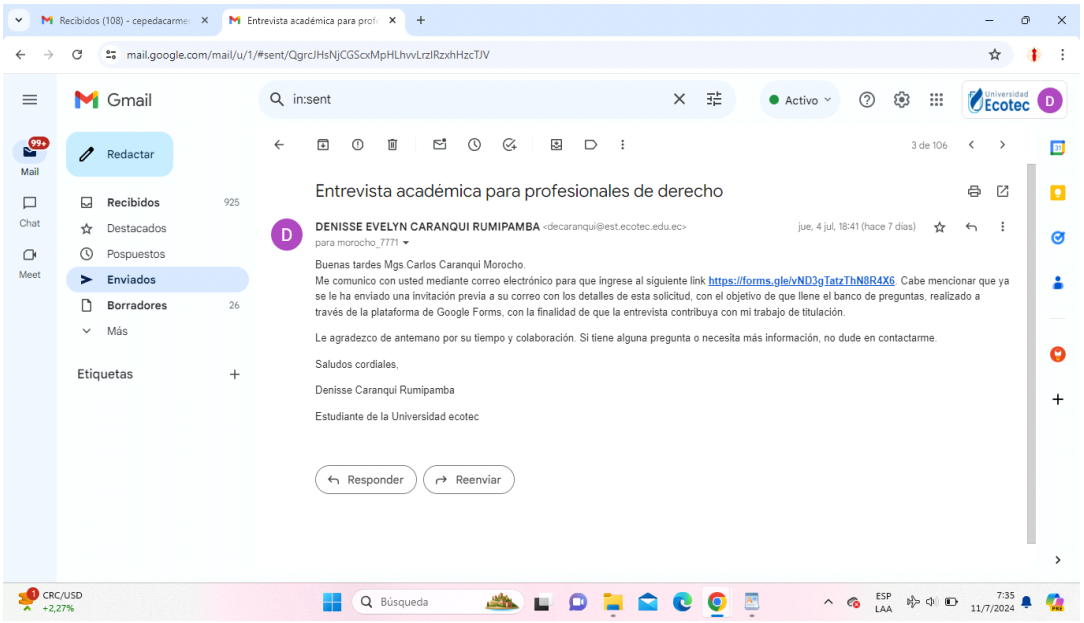
3. **¿Considera usted que en nuestra legislación ecuatoriana existen disposiciones que permitan combatir la estafa digital mediante la técnica del phishing?**

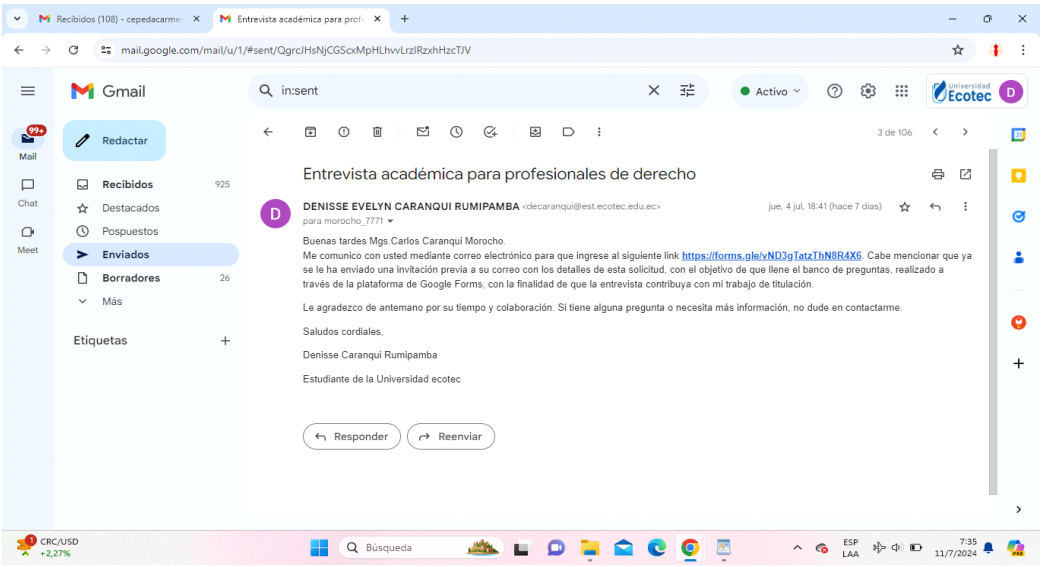
4. **¿Cree usted que el Código Orgánico integral penal debería ser reformado para incluir el phishing como un delito autónomo?**

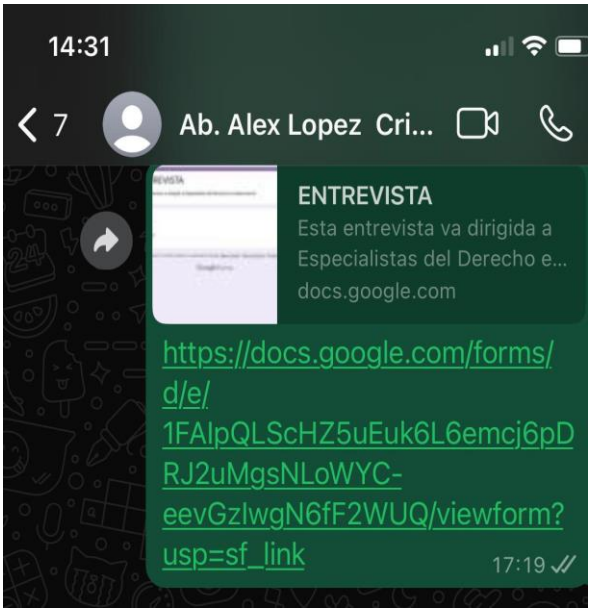
Anexo 3

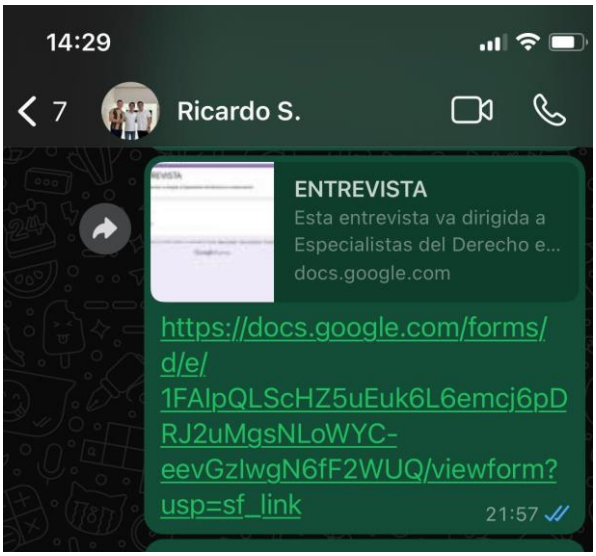
Capture del correo enviado a los diferentes profesionales del derecho, donde se les comparte el link para la entrevista:






Gmail
in:sent
Redactar
Recibidos 925
Destacados
Pospuestos
Enviados
Borradores 26
Más
Etiquetas
Entrevista académica para profesionales de derecho
DENISSE EVELYN CARANQUI RUMIPAMBA <decaranqui@est.ecotec.edu.ec>
para morocho_7771
jue, 4 jul, 18:41 (hace 7 días)
Buenas tardes Mgs.Carlos Caranqui Morocho.
Me comunico con usted mediante correo electrónico para que ingrese al siguiente link https://forms.gle/vND3gTatzThN8R4X6. Cabe mencionar que ya se le ha enviado una invitación previa a su correo con los detalles de esta solicitud, con el objetivo de que llene el banco de preguntas, realizado a través de la plataforma de Google Forms, con la finalidad de que la entrevista contribuya con mi trabajo de titulación.
Le agradezco de antemano por su tiempo y colaboración. Si tiene alguna pregunta o necesita más información, no dude en contactarme.
Saludos cordiales,
Denisse Caranqui Rumipamba
Estudiante de la Universidad ecotec
Responder
Reenviar


14:31
Ab. Alex Lopez Cri...
ENTREVISTA
Esta entrevista va dirigida a Especialistas del Derecho e...
docs.google.com
https://docs.google.com/forms/d/e/1FAIpQLScHZ5uEuk6L6emcj6pDRJ2uMgsNLoWYC-eevGzlwgN6fF2WUQ/viewform?usp=sf_link
17:19


14:29
Ricardo S.
ENTREVISTA
Esta entrevista va dirigida a Especialistas del Derecho e...
docs.google.com
https://docs.google.com/forms/d/e/1FAIpQLScHZ5uEuk6L6emcj6pDRJ2uMgsNLoWYC-eevGzlwgN6fF2WUQ/viewform?usp=sf_link
21:57