



Facultad de Derecho y Gobernabilidad

Tema del trabajo:

Propuesta normativa para disminuir la afectación de delitos que se cometen a través de medios digitales en el sector empresarial en la ciudad de Guayaquil, período 2023

Línea de Investigación:

Gestión de las Relaciones Jurídicas

Modalidad de titulación:

Proyecto de investigación

Carrera:

Derecho con énfasis en Ciencias Penales – Empresariales / Tributarias

Título a obtener:

Abogados de los Juzgados y Tribunales de la República del Ecuador

Elaborado por:

Gustavo Javier Zambrano Ramírez

Esperanza Francesca Vera Barberán

Tutor:

Abg. Fabian Ernesto Orellana Batallas

Guayaquil – Ecuador

2024



ANEXO No. 9

**PROCESO DE TITULACIÓN
CERTIFICADO DE APROBACIÓN DEL TUTOR**

Samborondón, 6 de agosto de 2024

Magíster

Andrés Madero Poveda

Derecho y Gobernabilidad

Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: PROPUESTA NORMATIVA PARA DISMINUIR LA AFECTACIÓN DE DELITOS QUE SE COMETEN A TRAVÉS DE MEDIOS DIGITALES EN EL SECTOR EMPRESARIAL EN LA CIUDAD DE GUAYAQUIL, PERIODO 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 al estudiante: **Esperanza Francesca Vera Barberán y Gustavo Javier Zambrano Ramírez**, para que proceda con la presentación oral del mismo.

ATENTAMENTE,

**FABIAN
ERNESTO
ORELLANA
BATALLAS**

Firmado digitalmente por FABIAN
ERNESTO ORELLANA
BATALLAS
DN: cn=FABIAN ERNESTO
ORELLANA BATALLAS
gn=FABIAN ERNESTO cncC
Motivo: Soy el autor de este
documento
Ubicación:
Fecha: 2024.08.10 09:33+02:00

**Abg. Mgtr. Fabian Ernesto Orellana Batallas.
Tutor**



ANEXO No. 10

PROCESO DE TITULACIÓN CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS DEL TRABAJO DE TITULACIÓN

Habiendo sido revisado el trabajo de titulación TITULADO: PROPUESTA NORMATIVA PARA DISMINUIR LA AFECTACIÓN DE DELITOS QUE SE COMETEN A TRAVÉS DE MEDIOS DIGITALES EN EL SECTOR EMPRESARIAL EN LA CIUDAD DE GUAYAQUIL, PERIODO 2023, elaborado por Esperanza Francesca Vera Barberán y Gustavo Javier Zambrano Ramírez, fue remitido al sistema de coincidencias en todo su contenido el mismo que presentó un porcentaje del 2% 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.

INFORME DE ANÁLISIS
registro

TESIS VERA Y ZAMBRANO

2% Textos sospechosos

- 2% Similitudes
 - + 1% similitudes entre oraciones
 - + 1% entre las fuentes mencionadas
 - + 1% similitudes no reconocidas

Nombre del documento: TESIS VERA Y ZAMBRANO.docx
 ID del documento: 684014605a73e02971990754636c78e7536deaf
 Tamaño del documento original: 195,63 KB

Depositante: FABIAN ERNESTO ORELLANA BATALLAS
 Fecha de depósito: 08/03/24
 Tipo de carga: interface
 Fecha de fin de análisis: 05/03/24

Número de palabras: 11.250
 Número de caracteres: 75.558

Ubicación de las similitudes en el documento:

Fuentes de similitudes

Fuentes principales detectadas

Nº	Descripciones	Similitudes	Ubicaciones	Otros atributos
1	www.conallega.gob.ec https://www.conallega.gob.ec/planes-y-proyectos/documentos/CONSEJO-ORDINARIO-INTERRUPCION-PENAL.pdf 31 fuentes similares	2%		Ej: palabras idénticas: 28(110 palabras)
2	repositorio.uq.edu.ec https://repositorio.uq.edu.ec/bitstream/handle/123456789/123456789/1/tesis-vera-y-zambrano.pdf 31 fuentes similares	2%		Ej: palabras idénticas: 28(110 palabras)
3	www.casaplay.com Agregación de alumnos por medios electrónicos - diversión... https://www.casaplay.com/planes-y-proyectos/agregacion-de-alumnos-por-medios-electronicos... 20 fuentes similares	1%		Ej: palabras idénticas: 19(147 palabras)
4	repositorio.uq.edu.ec https://repositorio.uq.edu.ec/bitstream/handle/123456789/123456789/1/tesis-vera-y-zambrano.pdf 20 fuentes similares	1%		Ej: palabras idénticas: 19(147 palabras)

ATENTAMENTE,

FABIAN
ERNESTO
ORELLANA
BATALLAS

Firmado digitalmente por FABIAN
ERNESTO ORELLANA BATALLAS
DN: cn=FABIAN ERNESTO
ORELLANA BATALLAS
gn=FABIAN ERNESTO o=EC
Motivo: Soy el autor de este
documento
Ubicación:
Fecha: 2024-08-10 09:46+02:00

Abg. Mgtr. Fabian Ernesto Orellana Batallas.
Tutor.

DEDICATORIA

A Dios, mi mamá, a mi abuelita, a mis hermanos, por su amor incondicional y su apoyo constante. A mis amigos, por su compañía y ánimo. Este logro es tanto suyo como mío.

Esperanza Francesca Vera Barberán

A Dios, por darme sabiduría en cada paso de mi vida, mi madre, quien ha sido mi pilar inquebrantable. Tu amor incondicional y palabras de aliento me han dado el valor para seguir adelante, incluso en los momentos más difíciles. A mis abuelos, cuyas enseñanzas y ejemplo de vida han sido una luz en mi camino, este logro es tanto de ustedes como mío.

Gustavo Javier Zambrano Ramírez

AGRADECIMIENTO

A Dios, mis padres, a mi abuelita y a mis hermanos, por su apoyo inquebrantable. A toda mi familia y a mis amigos, por ser mi fortaleza en este camino. Gracias por hacer posible este logro.

Esperanza Francesca Vera Barberán

A Dios, por su infinita bondad, por guiarme con su luz en cada etapa de esta aventura. A mi familia, por demostrarme su apoyo incondicional. A mis amigos los cuales hicieron que este trayecto sea más divertido. A mi enamorada, tu amor ha sido esencial para que pueda culminar esta etapa. Cada uno de ustedes ha jugado un papel crucial en este proceso, gracias por creer en mí.

Gustavo Javier Zambrano Ramírez

PROPUESTA NORMATIVA PARA DISMINUIR LA AFECTACIÓN DE DELITOS QUE SE
COMETEN A TRAVÉS DE MEDIOS DIGITALES EN EL SECTOR EMPRESARIAL EN LA
CIUDAD DE GUAYAQUIL, PERÍODO 2023

RESUMEN

La investigación jurídica realizada tuvo como finalidad desarrollar una normativa encaminada a disminuir el cometimiento de los delitos digitales en el sector empresarial en la ciudad de Guayaquil, lo cual constituye una mejora en la confianza de los clientes de empresas locales, reducción en las pérdidas monetarias ocasionadas por los delitos cibernéticos, incremento en la competitividad organizacional por emplear sistemas más fiables y fortalecimiento en la cooperación empresarial. Se efectuó un análisis con respecto a los diversos métodos por los cuales se materializan los ciberdelitos, específicamente los relacionados con el phishing (suplantación de identidad) junto con sus modalidades, fases y tipos. Para el estudio, se tomó en consideración el delito de “Apropiación fraudulenta por medios electrónicos”, en virtud de, su considerada deficiencia sancionatoria y falta de reglamentación en cuanto a las afectaciones generadas en el sector empresarial. El trabajo se efectuó mediante la implementación de un enfoque cualitativo con alcance descriptivo, esto permitió analizar el fenómeno estudiado a profundidad con el propósito de poder comprender sus diferentes modus operandi, para así, obtener mecanismos preventivos y represivos en concordancia con la normativa legal vigente. En base a los resultados que se obtuvieron de este estudio, se elaboró una propuesta la cual se centra en una reforma de la legislación actual.

Palabras claves: Sector empresarial, ciberseguridad, phishing, apropiación fraudulenta por medios electrónicos y modus operandi.

SUMMARY

The purpose of the legal research carried out was to develop regulations aimed at reducing the commission of digital crimes in the business sector in the city of Guayaquil, which constitutes an improvement in the confidence of clients of local companies, a reduction in the monetary losses caused. due to cybercrimes, an increase in organizational competitiveness by using more reliable systems and the strengthening of business cooperation and authorities in charge of handling cybersecurity cases. An analysis was carried out regarding the various methods by which cybercrimes materialize, specifically those related to phishing (identity theft) along with its modalities, phases and types. For the study, the crime of "Fraudulent appropriation by electronic means" was taken into consideration, due to its considered sanctioning deficiency and lack of regulation regarding the effects generated in the business sector. The work was carried out through the implementation of a qualitative approach with a descriptive scope, this allowed us to analyze the phenomenon studied in depth with the purpose of being able to understand its different modus operandi, in order to obtain preventive and repressive mechanisms in accordance with current legal regulations. Based on the results obtained from this study, was prepared which focuses on a reform of the current legislation.

Keywords: Business sector, cybersecurity, phishing, fraudulent appropriation by electronic means and modus operandi.

CONTENIDO	
RESUMEN	7
SUMMARY	8
INTRODUCCIÓN	12
CAPÍTULO 1	14
PROBLEMA	14
1.1 PLANTEAMIENTO DEL PROBLEMA	15
1.1.1 PREGUNTA PROBLEMA	15
1.1.2 OBJETIVO GENERAL	15
1.1.3 OBJETIVOS ESPECÍFICOS	15
1.1.4 JUSTIFICACIÓN	15
CAPÍTULO 2	17
MARCO TEÓRICO	17
2.1 MARCO TEÓRICO	18
2.1.1 GENERALIDADES	18
2.1.2 EL DELITO	18
2.1.3 DELITO INFORMÁTICO	20
2.1.4 SUJETOS QUE INTERVIENEN EN EL COMETIMIENTO DE ESTOS	
DELITOS	21
2.1.4.1 SUJETO ACTIVO	21
2.1.4.2 SUJETO PASIVO	22
2.1.4.3 MEDIOS	22
2.1.4.4 OBJETO	22
2.1.5 DEFINICIÓN DE PHISHING.....	22

	10
SMISHING.....	23
VISHING.....	23
2.1.6 FASES DEL PHISHING	24
2.1.6.1 PLANIFICACIÓN Y CONFIGURACIÓN	24
2.1.6.2 ATAQUE DE PHISHING	25
2.1.6.2 INFILTRACIÓN	25
2.1.6.2 RECOPIACIÓN DE DATOS	25
2.1.6.3 EXTRACCIÓN.....	25
2.1.7 BIENES JURÍDICOS VULNERADOS	26
2.1.8 TIPOS DE PHISHING	27
2.1.9 AFECTACIÓN DEL PHISHING A LA ESFERA EMPRESARIAL	28
2.1.10 CASO PICHINCHA POR "PHISHING"	29
CAPÍTULO 3	31
METODOLOGÍA DE LA INVESTIGACIÓN	31
3.1 MARCO METODOLÓGICO	32
3.1.2 LA METODOLOGÍA	32
3.1.3 LOS MÉTODOS	32
3.1.4 ENFOQUE DE LA INVESTIGACIÓN	32
3.1.5 ALCANCE DE INVESTIGACIÓN.....	33
3.1.6 DELIMITACIÓN DE LA INVESTIGACIÓN	34
3.1.7 POBLACIÓN Y MUESTRA	34
3.1.7.1 MÉTODOS A NIVEL EMPÍRICO Y TEÓRICO	35
3.1.7.2 MÉTODO DE OBSERVACIÓN.....	35

3.1.7.3 ENTREVISTA.....	35
3.1.8 OPERACIONALIZACIÓN DE LAS VARIABLES.....	35
3.1.9 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN	37
ANÁLISIS DE DATOS.....	38
3.2 ENTREVISTAS.....	38
3.3 DISCUSIÓN DE RESULTADOS.....	54
CAPÍTULO 4.....	59
4.1 CONCLUSIONES.....	60
4.2 RECOMENDACIÓN / PROPUESTA.....	62
4.3 BIBLIOGRAFÍA	64
4.4 ANEXOS	69

INTRODUCCIÓN

El presente trabajo de investigación tiene como finalidad efectuar un estudio del delito de phishing y su afectación en el ámbito empresarial, a través de la revisión del tipo penal de “Apropiación fraudulenta por medios electrónicos”, debido a la ineficacia de la normativa legal en cuanto a la regulación de los ciberdelitos. El análisis se centra en los delitos cometidos por medios digitales, desde su entorno, sistema, bienes jurídicos que vulnera, y esencialmente su forma de operar a través de los sistemas de información y comunicación, para la consumación de este ilícito informático.

Los avances tecnológicos representan un mecanismo de mejora en las comunicaciones a nivel mundial, lo cual constituye un beneficio a la vida cotidiana de las personas. No obstante, el desarrollo de los sistemas de la información, también ocasiona que se efectúen nuevos desafíos, como los ilícitos que se suscitan por medios telemáticos.

El término “phishing” cuya traducción al español es “pesca”. Tiene su origen a mediados de los años 90. El mismo se refiere a la técnica implementada con la finalidad de duplicar una página digital o manipular el diseño de un correo electrónico, para que este enlace generado por los phishers, tenga la apariencia de uno oficial, de manera que, los usuarios puedan creer que aquella dirección proviene de una identidad confiable. (Alcívar Trejo, Calderón Cisneros, Blanc Pihuave, & Duchi Ortega, 2016)

En consecuencia, desde que se originó el primer malware se disparó la actividad delincriminal a través de medios telemáticos. Los ciberdelitos representan un agravio al desarrollo de los entornos digitales, debido a que buscan revestir sus actividades, para poder asegurar el cometimiento del delito. Tomando como punto de referencia este precepto, se considera fundamental que se establezca un análisis crítico jurisprudencial con respecto a los elementos que configuran al delito de suplantación de identidad. (Nascimento Fernández, 2021)

Se considera esencial abordar la modalidad del phishing, debido a que generó gran cantidad de víctimas en el año 2015, en países latinoamericanos como Ecuador y Brasil, de acuerdo a un estudio mundial sobre seguridad en internet, en el cual se demostró la vulnerabilidad de estas locaciones en relación a los ataques cibernéticos. (Alcívar Trejo, Calderón Cisneros, Blanc Pihuave, & Duchi Ortega, 2016)

En los últimos años se ha evidenciado un cambio indiscutible derivado de la era tecnológica. Esto representa un nuevo entorno, el telemático, el cual se adapta a las actividades cotidianas, como en el caso de las prestaciones de servicios profesiones o la adquisición de productos de primera necesidad, lo cual ha materializado que la utilización de la virtualidad sea más usual.

Es pertinente referir que, la indagación del tema objeto de interés se origina por la falta de disposiciones legales útiles para afrontar los delitos cibernéticos que afectan el sector empresarial en el Ecuador. Una de las formas más efectivas para frenar este ilícito es través de la implementación de una sanción normativa rigurosa en contra de los delincuentes en línea.

En definitiva, para el análisis se aplicará un método descriptivo, lo cual permitirá estudiar las características de la temática escogida por medio de la revisión de la figura de phishing y su incidencia con el delito de "Apropiación fraudulenta por medios electrónicos", para determinar su incidencia en las organizaciones corporativas. De esta forma, se podrá identificar las causas que originan el cometimiento del mismo.

CAPÍTULO 1

PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La investigación busca abordar la problemática que representa la falta de precisión y rigurosidad en la normativa legal ecuatoriana con relación al cometimiento de los delitos electrónicos, y como este afecta al ámbito empresarial. Es pertinente reconocer que los avances tecnológicos son categorizados como un beneficio para la sociedad. Sin embargo, han traído consigo diversas formas de materialización de los delitos.

1.1.1 PREGUNTA PROBLEMA

¿Cómo disminuir los delitos que se cometen a través de medios digitales en el sector empresarial en la ciudad de Guayaquil, período 2023?

1.1.2 OBJETIVO GENERAL

Determinar el alcance de la reforma normativa para disminuir el cometimiento de los delitos que se cometen a través de medios digitales en el sector empresarial en la ciudad de Guayaquil, período 2023.

1.1.3 OBJETIVOS ESPECÍFICOS

1. Analizar el momento en el cual se considera que los delitos cometidos a través de medios digitales afectan a las organizaciones corporativas.
2. Identificar la afectación de los delitos de suplantación de identidad en el sector empresarial en la ciudad de Guayaquil.
3. Establecer las diversas tipologías que guardan relación con los delitos electrónicos y mecanismos para prevenir su configuración.

1.1.4 JUSTIFICACIÓN

El phishing es considerado como un delito electrónico, se caracteriza por ser una amenaza con repercusiones severas. El sector empresarial ecuatoriano, se encuentra en un riesgo latente a sufrir prejuicios financieros, daños a su imagen e inclusive vulneración a los datos de carácter confidencial como consecuencia del ataque. Esta problemática se ve agravada por la creciente era tecnológica de los procesos empresariales y su dependencia

en cuanto a los medios digitales, lo cual constituye una mayor probabilidad de vulneración ante los ciberdelitos.

El Código Orgánico Integral Penal tipifica al delito de “Apropiación fraudulenta por medios electrónicos”. No obstante, su contenido es disperso, con falta de rigurosidad normativa, lo cual ocasiona que se continúen cometiendo delitos, como el phishing aplicado en sus diversas modalidades. Las reglamentaciones poco específicas traen consigo la impunidad de los actos.

La ausencia de políticas sancionatorias claras incrementa la susceptibilidad de las empresas a ser víctimas de ciberdelitos. Es importante mencionar que las afectaciones no solo se evidencian a nivel de patrimonio, sino que también, se vulnera la información personal de la persona natural o jurídica.

Las organizaciones empresariales deben aplicar protocolos de seguridad informática y dictar charlas de educación continua a sus colaboradores con relación a las diversas modalidades del phishing y la manera en la cual se podrá reconocerlas. Estas prácticas junto con la legislación adecuada, representan mecanismos de prevención y concientización para la esfera empresarial.

CAPÍTULO 2

MARCO TEÓRICO

2.1 MARCO TEÓRICO

2.1.1 GENERALIDADES

El presente trabajo de investigación es de gran relevancia, debido a que permite comprender los aspectos que generan la propagación de los delitos informáticos, considerados como penalmente relevante. Para el efecto, se analizará al delito de phishing aterrizado en el tipo penal de "Apropiación fraudulenta por medios electrónicos", para comprender su incidencia en la esfera empresarial.

2.1.2 EL DELITO

El delito es una conducta típica y antijurídica y culpable. En ese sentido, para que se constituya se deberán cumplir diversos objetivos del tipo penal; la manifestación de la conducta, relación o nexos causal, y consecuentemente, se origina el elemento subjetivo (dolo o culpa). La conducta típica guarda relación con la condición de antijuricidad, debido a que lesiona el bien jurídico protegido sin encontrarse en un estado de necesidad. Finalmente, la culpabilidad señala que debe haber intención o negligencia en el cometimiento del acto. (Montiel Rojas, 1999)

Con relación a la teoría del delito, Raúl Zaffaroni en su manual de Derecho penal, establece que es un sistema de filtros que generan interrogantes con relación a la función de las agencias jurídicas en cuanto a la aplicación del poder punitivo. Asimismo, refiere que es esencial la imposición de sanciones penales rigurosas, con la finalidad de reducir el cometimiento de los delitos. (Zaffaroni, 2006)

Con el propósito de mejorar la comprensión del lector, se procede a esquematizar cada uno de los elementos que conforman la teoría del caso. Tomando en consideración el hecho de que el compendio de información produce una mejora en la retentiva del contenido. El análisis se efectúa de acuerdo a la recolección de datos obtenidos de fuentes primarias y secundarias.

Tabla 1

Elementos del delito

Conducta	Tipicidad	Antijuricidad	Culpabilidad
La conducta es conocida como el primer paso para identificar si un acto es un delito. Recordemos que se encuentra representada por un comportamiento voluntario ejercido por una persona. Puede suscitarse por acción u omisión.	La tipicidad se centra en la relación entre el comportamiento de una persona y la tipificación de un delito establecido en la ley. Es importante mencionar que, si una conducta reúne todos los elementos del delito, podrá ser considerada como típica.	La antijuricidad genera una controversia entre un acto y el ordenamiento jurídico, ya que una conducta puede ser típica, pero se debe analizar si existe una justificación que la legitime, como es el caso de la legítima defensa o cumplimiento de una obligación legal.	La culpa hace alusión a la libertad y capacidad que posee una persona al momento de elegir no cometer un delito, lo que significa que un individuo solamente podrá ser declarado como culpable, cuando haya tenido la capacidad de comprender el significado y consecuencias de sus actos al momento de cometer el delito.

(Iñahuazo López, 2024)

En definitiva, para un acto ser considerado como delictivo, debe contar con cuatro elementos esenciales que son; la conducta (comportamiento voluntario), la tipicidad (acción que encaja en la categoría de delito), la antijuricidad (acto contrario a la normativa legal que no se encuentra justificado), y la culpabilidad (capacidad humana de comprender y controlar sus acciones). Estos elementos permiten que netamente sean penalizados actos ilícitos.

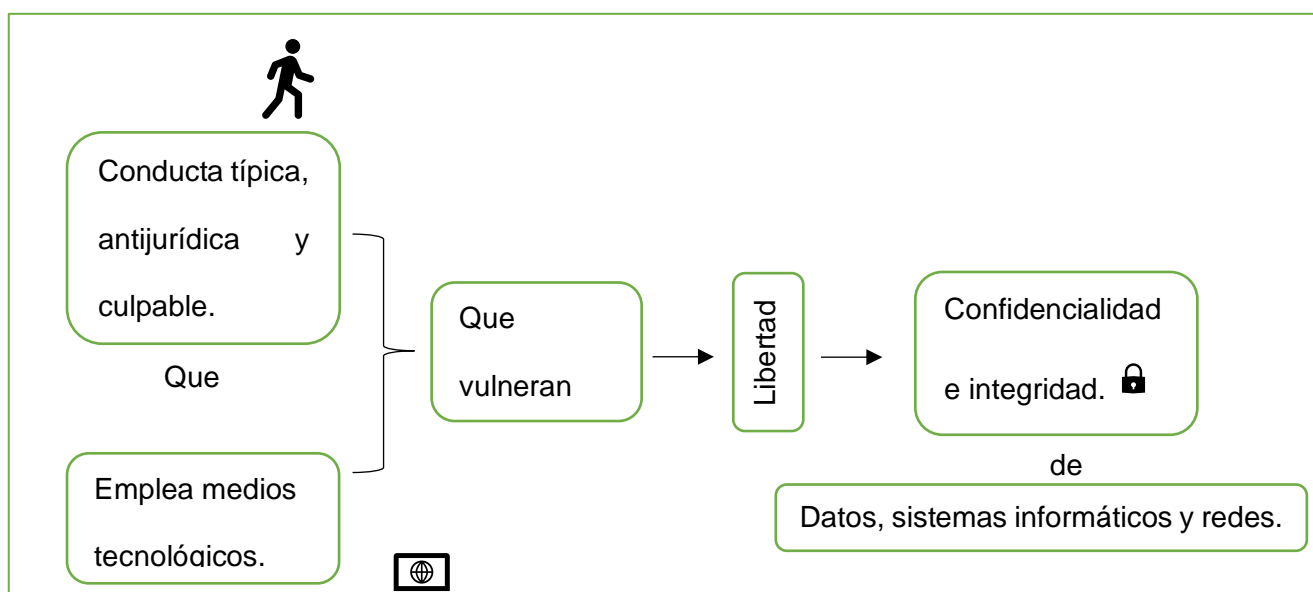
2.1.3 DELITO INFORMÁTICO

El delito informático, posee su apogeo en la década de los setenta, por medio de la utilización de ordenadores en la esfera empresarial, y consecuentemente, se complementó con la delincuencia económica. De esta manera, comenzaron a surgir una serie de métodos contrarios a la ley, como es el caso de la piratería del software, y a su vez, las infracciones contra la propiedad intelectual, en películas y músicas, específicamente, en los años noventa. Es relevante mencionar que, la aparición del internet fue considerada como una herramienta de difusión de contenidos audiovisuales, como el racismo, la xenofobia o la pornografía infantil, e inclusive delitos de terrorismo contra el Estado. (SciELO, 2021)

Las conductas ilícitas efectuadas por cualquier medio informático son susceptibles de ser sancionadas de acuerdo a lo que establece el derecho penal. Los delitos cibernéticos requieren de la existencia de actividades criminales dentro de las cuales se encuentran: Las falsificaciones, los fraudes, las estafas, entre otros. No obstante, el uso de un dispositivo electrónico facilita el cometimiento de estas fechorías. (Blossiers Mazzini, 2018)

Tabla 2

Elementos de los delitos informáticos






Fuente: Elaboración propia

En definitiva, el esquema elaborado permite comprender la definición conceptual de los delitos informáticos, tomando como punto de referencia el análisis de los elementos esenciales que serán considerados como conductas ilícitas. Estos se caracterizan por ocasionar una lesión a la libertad informática, generando un impacto en la seguridad e integridad de los datos, redes y sistemas telemáticos, lo cual crea una necesidad latente en la implementación de medidas preventivas y represivas legales.

Tabla 3

Componentes del delito informático

Sujeto	Medio	Objeto
<p>La persona que comete la conducta delictiva o ilícita.</p> 	<p>El sistema informático.</p> 	<p>El bien que produce un beneficio ilícito o económico.</p> 

(Saltos Salgado, Robalino Villafuerte, & Pazmiño Salazar, 2021)

2.1.4 SUJETOS QUE INTERVIENEN EN EL COMETIMIENTO DE ESTOS DELITOS

2.1.4.1 SUJETO ACTIVO

El sujeto activo se encuentra representado por personas que participan en la comisión de conductas contrarias a la ley, podrán ser naturales o jurídicas, que evidentemente, cuentan con conocimientos en la rama informática, con un nivel de instrucción elevado, mismo que les permite ejecutar una serie de actos, orientados a manipular los sistemas de computación, procurando eliminar rastros, para no ser sancionados según lo que establece la normativa.

2.1.4.2 SUJETO PASIVO

El sujeto pasivo de los ciberdelitos podrá estar ostentado por: individuos, gobiernos, instituciones de crédito o cualquier entidad que desarrolle sus actividades mediante la utilización de los sistemas automáticos de información. Estos se caracterizan por tener la custodia de un medio informático, que posteriormente, podrá ser vulnerado por el sujeto activo. (Ruiz Castro, 2021)

2.1.4.3 MEDIOS

Los delitos informáticos se materializan de diversas maneras, como es el caso de las imágenes de agresiones sexuales contra menores, la usurpación de identidad, phishing, estafas por internet, entre otros. No obstante, estos riesgos no son los únicos que representan una vulneración a la seguridad informática, también surgen aquellos que se encuentran relacionados con el uso de las redes sociales, por ejemplo; la divulgación de material pornográfico, sexting (manejo de contenido erótico), cyberbullying (acoso a menores a través de medios telemáticos), entre otros. (Ministerio de Educación , 2020)

2.1.4.4 OBJETO

El objeto de los ciberdelitos son las computadoras y diferentes redes de comunicaciones, Es esencial señalar que, se utiliza un dispositivo electrónico como instrumento para el cometimiento del hecho ilícito. Asimismo, puede ser el objetivo un sistema de información o informático que se encuentra contenido en él, como son: La información, los datos y sistemas informáticos. (Guarnizo Portela, 2020)

2.1.5 DEFINICIÓN DE PHISHING

El phishing es considerado como un ataque a la ciberseguridad efectuado por parte de los expertos en informática (phisher) quienes, de manera maliciosa, se encargan de compartir direcciones de correos electrónicos o mensajes suplantando la identidad de una persona o entidad, a fin de manipular a los usuarios, para instalar un contenido malicioso que, al hacer clic en un enlace, permita obtener credenciales de acceso a información confidencial.

De acuerdo a lo que establece la superintendencia de bancos el phishing es considerado como una modalidad que utiliza el envío de un correo electrónico, el cual tiene la apariencia de ser remitido por parte de una institución formal, lo que quiere decir que, utilizan el logotipo de dicha empresa y los colores, con el propósito de obtener datos, cuentas bancarias, números de tarjeta, entre otros.

Los ciberdelincuentes implementan este método para realizar retiros de dinero o efectuar compras no autorizadas por internet, configurándose así, los ataques de phishing. Pese a los avances tecnológicos, se considera complejo poder detectar este tipo de delitos, ya que el medio utilizado para el engaño posee ciertas características que visiblemente lo asemejan a una fuente original conocida por el usuario. (Guaña Moya, y otros, 2022)

El método de phishing es una técnica empleada con el propósito de engañar al usuario capturando su información confidencial para estafarlo. Esta modalidad se efectúa por medio del envío de mensajes, y posteriormente, la llamada del delincuente. Un claro escenario es: Los premios otorgados por parte de los almacenes de cadena u operadores de telefonía celular, las extorsiones por secuestros, entre otras. (Guarnizo Portela, 2020)

Tabla 4

Modalidades del phishing

SMISHING	VISHING
El smishing se encuentra ostentado por los mensajes o texto o mensajes de WhatsApp. Este riesgo latente se produce cuando el cliente es contactado por los métodos anteriormente señalados, momento en el	El vishing hace alusión al tipo de amenaza que correlaciona una llamada telefónica fraudulenta con la información que se obtuvo previamente a través de la web.

<p>cual, el emisor se hace pasar por un agente bancario, quien informa que se ha realizado una compra inusual con su tarjeta de crédito, motivo suficiente para contactarse con la banca, tras haberle proporcionado un número falso. Consecuentemente, el cliente devuelve la llamada, y en ese instante, el ciberdelincuente solicita información confidencial para en teoría efectuar una cancelación de la compra, pero aprovecha para robar su información.</p>	<p>Este método consta de dos pasos. Primero, el delincuente cibernético tiene que haber hackeado información confidencial por medio de una web fraudulenta (phishing) o correo electrónico, para lo cual, requiere un token digital o clave SMS, para validar la operación. Segundo, el impostor llama por teléfono al cliente identificándose, como personal del banco, con la finalidad de que el afectado revele su clave.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(BBVA, 2024)

El cuadro comparativo que antecede permite evidenciar que, el smishing y vishing son considerados como dos modalidades que se consuman por medio de la obtención de información de los usuarios. A pesar de tener distinciones, ambos se caracterizan por la implementación del engaño a las personas haciéndose pasar por entidades de confianza, como los bancos y otras instituciones financieras, para robar su información sensible.

2.1.6 FASES DEL PHISHING

2.1.6.1 PLANIFICACIÓN Y CONFIGURACIÓN

La fase de planificación tiene como finalidad extraer las identificaciones de la víctima y la red a emplear, por medio de un estudio de tráfico. Después de este reconocimiento, se establecen ataques utilizando medios, como sitios web y correos electrónicos con enlaces maliciosos. Estas herramientas se encargan de redirigir al usuario a una página web fraudulenta.

2.1.6.2 ATAQUE DE PHISHING

La fase de ataque se caracteriza por ser una actividad real, en la cual se remiten correos electrónicos fraudulentos a la víctima, solicitando información personal. Generalmente, estas direcciones web poseen una apariencia de entidades bancarias de renombre, por lo tanto, utilizan esa fachada para realizar preguntas para “actualizar” registros.

2.1.6.2 INFILTRACIÓN

La fase de ruptura se establece cuando el afectado realiza un clic en un malware, es decir, un enlace malicioso en su dispositivo, a través de este accionar se genera un acceso al sistema para el atacante. De esta manera, se encontrará facultado para efectuar configuraciones y derechos de acceso.

2.1.6.2 RECOPIACIÓN DE DATOS

Los delincuentes cibernéticos acceden a los sistemas de los usuarios, con el fin de extraer datos confidenciales de sus cuentas bancarias, que previamente fueron obtenidos a través de páginas webs de dudosa procedencia. Como consecuencia, el atacante podrá conseguir fácilmente la información, y posteriormente, efectuar una migración de datos, generando una gran cantidad de pérdidas financieras.

2.1.6.3 EXTRACCIÓN

Esta etapa es conocida por ser la concluyente en el desarrollo del período. Una vez logrado el acceso y la investigación solicitada. Se realiza una exclusión de todas las evidencias pertinentes, como las cuentas ficticias de los sitios web. Para finalizar, se analiza el éxito en la falta de interrupción, esto permite preparar futuros ataques. (Lopez Ocampo, 2023)

2.1.7 BIENES JURÍDICOS VULNERADOS

Los bienes jurídicos vulnerados en el cometimiento del delito de phishing son: El patrimonio, la integridad, la disponibilidad y la confidencialidad, y la seguridad de los sistemas de información y comunicación. Evidentemente, las víctimas resultan perjudicadas y pierden la confianza en el sistema judicial al momento de la propagación de estos hechos delictivos, ya que la información del afectado queda en manos del denunciado, y esta se encuentra propensa a ser divulgada con terceros.

El Código Orgánico Integral Penal, tipifica los ciberdelitos, estos se concretan a través del uso de las nuevas tecnologías, su consumación genera lesiones a los bienes jurídicos protegidos. Dichos actos se pueden clasificar en: el robo, el fraude, las falsificaciones, el espionaje, la clonación de tarjetas de crédito y la suplantación de identidad, entre otros. No obstante, el ordenamiento jurídico ecuatoriano, no determina al sujeto activo de la obligación, lo cual genera que sea de gran complejidad determinar al sujeto activo, y detectar las direcciones IP y cuentas que originaron el ilícito. Es de vital importancia que, el Ecuador forme parte de convenios internacionales, para que exista un mayor soporte a nivel investigativo. (Sempertegui Torres, 2022)

La criminalidad informática se rige por comportamientos típicos que generan una afectación a los sistemas de la información. Recordemos que son susceptibles de ataque todos aquellos soportes lógicos que permiten el procesamiento de la información. Una gran cantidad de legislaciones reconocen a los ciberdelitos como pluriofensivos. Sin embargo, en el Ecuador la protección de los derechos no va de la mano con los avances de la tecnología, usualmente, las sanciones han sido establecidas con respecto a los delitos tradicionales. (Nazario Delgado & Villanueva Sanchez, 2022)

En la misma línea, Villavicencio Terrenos define a la ciberdelincuencia como aquella que se encuentra evidenciada por aquellas conductas orientadas a burlar la seguridad informática, lo cual implica invasiones a computadoras, sistemas de datos o correos por

medio de una clave de acceso; estas conductas se podrán suscitar solo a través de la implementación de las tecnologías de la información. (Villavicencio Terreros, 2014)

2.1.8 TIPOS DE PHISHING

Los tipos de phishing se detallan a continuación:

2.1.8.1 SPEAR PHISHING

Se encuentra direccionado a individuos o grupos específicos. Esta modalidad opera a través de la remisión de un correo electrónico, el cual posee la apariencia de ser obtenido por fuentes confiables. Busca recolectar información confidencial de la víctima.

2.1.8.2 WHALE PHISHING/WHALING

Las principales víctimas de este delito son los funcionarios gerenciales de las empresas. Este método opera de manera personalizada, lo que vuelve el mensaje más efectivo. El phishing de ballena se caracteriza por atacar a sujetos adinerados, prominentes o poderosos.

2.1.8.3 SOCIAL PHISH

Es conocido como una herramienta web que es empleada para clonar alguna red social, como es el caso de Twitter, LinkedIn, Facebook, etc, debido a que cuenta con plantillas que generan una copia de la información personal del usuario en la base de datos.

2.1.8.4 SHELLPHISH

Permite que los usuarios puedan acceder a los servicios del sistema operativo del equipo infectado con software malicioso. (Guaña Moya, y otros, 2022)

Los tipos de phishing descritos con antelación demuestran diversas técnicas dirigidas a los perfiles de los afectados, resaltando la importancia de tomar las precauciones pertinentes para no ser víctimas de estos delitos.

2.1.9 AFECTACIÓN DEL PHISHING A LA ESFERA EMPRESARIAL

La seguridad cibernética es reconocida como un reto empresarial para afrontar en la era digital. Las empresas se encuentran propensas a recibir amenazas persistentes a la ciberseguridad, por consiguiente, es necesario establecer medidas de protección eficaz en contra de los delitos informáticos. Sin embargo, para esta acción se debe contemplar la combinación de diversos factores técnicos, capacitaciones, tecnológicos, personales y políticos de la empresa.

En la misma línea, Kevin Mitnick establece la importancia de analizar la ingeniería social, las acciones internas de los empleados, vulnerabilidades técnicas y amenazas cibernéticas que atacan los sistemas operacionales corporativos. Asimismo, se debe tener en consideración la necesidad de aplicar medidas proactivas, en cuanto a la utilización de sistemas actualizados, y tomar decisiones informadas de asignación de recursos con la finalidad de mejorar la seguridad de los archivos digitales y las TIC, así como la información de carácter reservado de la empresa. (Cano & Monsalve Machado, 2023)

2.1.9.1 LA INGENIERA SOCIAL

Se refiere a que la gran cantidad de hackeos empresariales se producen a través de una modalidad orientada a manipular la información confidencial. En virtud de aquello, la única manera de disminuir estos actos es por medio de la realización de capacitaciones sobre la seguridad personal y empresarial ante este tipo de ataques.

2.1.9.2 LAS ACCIONES INTERNAS DE LOS EMPLEADOS

Hace alusión al riesgo que representan las acciones de los trabajadores al poder acceder a información de carácter reservado en las instituciones, donde se pueden suscitar riesgos relacionados con la negligencia, la mala praxis o malicia entre los colaboradores.

2.1.9.3 VULNERABILIDADES TÉCNICAS

Las empresas usualmente presentan vulneraciones técnicas a nivel de redes y sistemas, esto se debe a la utilización de un software sin su respectiva actualización,

falta de parches de seguridad o configuraciones inseguras, las cuales podrán ser explotadas por los hackers.

2.1.9.4 AMENAZAS CIBERNÉTICAS

Existen diversos tipos de ataques a la seguridad de la información, entre ellos se encuentran: el malware, el phishing, ransomware y otras clases de amenazas que representan un riesgo para las redes corporativas, ya que generan un daño significativo.

En definitiva, la seguridad de la información en la esfera empresarial se enfrenta a múltiples desafíos, los cuales necesitan una estrategia efectiva para lograr ser erradicados. En conjunto, la combinación de educación, controles internos, mantenimiento técnico y medidas de protección avanzada es esencial para salvaguardar la información y los activos digitales de las empresas.

2.1.10 CASO PICHINCHA POR "PHISHING"

En el año 2020, se inició una instrucción fiscal en contra de seis procesados. Estos sujetos en su mayoría miembros de una misma institución familiar, investigados por presunta apropiación fraudulenta por medios telemáticos. Durante el período anteriormente mencionado, el fiscal encargado del caso, Hugo Pérez, emitió un dictamen acusatorio en la Unidad Judicial de Pedro Vicente Maldonado, al noroccidente de Quito.

De los seis procesados, cuatro obtuvieron prisión preventiva y dos presentaciones periódicas ante la autoridad competente y la medida cautelar de prohibición de salida del país. Este segundo escenario se configura, debido a que los procesados exceden los 65 años de edad. Los adultos mayores responden a los alias de "Papá" y "Mamá", los otros cuatro son denominados como, "Chino", "Neutrón", "Taz" y "Topo", quienes habrían conformado el grupo de ciberdelincuencia.

Es importante mencionar que, la forma de operar de esta organización se centraba en la utilización de códigos robados y números de tarjetas en Estados Unidos y Europa, con la

finalidad de comprar cuentas de mercadería en plataformas virtuales y de streaming, para posteriormente venderlos, por medio de redes sociales, a la mitad del precio real.

El juez de garantías penales, a través de la audiencia acusatoria admitió la formulación de cargos, en la cual se presentaron veintiséis elementos de convicción en contra de los procesados. Es fundamental precisar que, desde el inicio de la pandemia hasta octubre, esta asociación delincuenciaal habría acumulado unos \$80.000 dólares en sus cuentas bancarias y tres vehículos adquiridos, los cuales fueron incautados en el operativo realizado. (FISCALÍA GENERAL DEL ESTADO, 2020)

El Código Orgánico Integral Penal, en cuanto al delito de apropiación fraudulenta por medios electrónicos establece lo siguiente:

La persona que utilice los sistemas de la información y comunicación, para apropiarse de un bien ajeno sin autorización del titular, con la finalidad de obtener un beneficio monetario a través del uso de plataformas digitales, tendrá una pena privativa de libertad de uno a tres años.

La misma sanción será establecida si la infracción se materializa por medio de la inutilización de sistemas de alarma o guarda, empleo de tarjetas magnéticas, descubrimiento o descifrado de claves secreta, entre otros. (La Asamblea Nacional, 2014)

CAPÍTULO 3

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 MARCO METODOLÓGICO

3.1.2 LA METODOLOGÍA

La palabra metodología tiene su origen en el griego μέθοδος (méthodos), cuyo significado es “método”, y el sufijo “logía”, que proviene de λόγος (lógos) y su tracción guarda relación con “estudio o ciencia”. En ese sentido, se denomina como la ciencia del método. En definitiva, la metodología juega un rol preponderante en el campo de la ciencia, específicamente, en las investigaciones al proporcionar un conjunto de procedimientos de forma sistemática, ordenada y rigurosa para lograr alcanzar los fines propuestos

La metodología determina la manera en la cual el sujeto investigador va a recolectar, ordenar y analizar los datos recabados. Es importante destacar que, la aplicación de las técnicas y métodos adecuados sirven para guiar al investigador, precautelando la validez y pertinencia de la información obtenida. (Guerrero Dávila & Guerrero Dávila, 2020)

3.1.3 LOS MÉTODOS

Los métodos se encuentran encaminados a la comprensión e interpretación de los datos, lo cual permite efectuar un análisis con respecto a los diversos paradigmas y enfoques de investigación. De esta forma, se logra establecer que los métodos de la investigación son una cadena de acciones relacionadas con un objeto conceptual determinado, el cual se rige por reglas que permiten tener avances en el proceso de conocimiento. (Instituto Superior Tecnológico ATLANTIC, 2020)

3.1.4 ENFOQUE DE LA INVESTIGACIÓN

La presente investigación se va a regir por un método cualitativo, este se caracteriza por ser un conjunto de prácticas interpretativas que tienen como propósito efectuar representaciones a través de observaciones, anotaciones, grabaciones y repositorios documentales. Permite tener una comprensión más acertada con relación al objeto de estudio, la información recabada y los criterios de los participantes. (Guzmán, 2021)

La investigación cualitativa es un enfoque metodológico implementado en diferentes disciplinas. Se centra en la comprensión de fenómenos sociales, culturales o individuales desde un panorama descriptivo, cuya finalidad es obtener riqueza en las experiencias humanas. Recordemos que, este método de investigación se basa en datos no numéricos, como la observación, las entrevistas, grupos focales, entre otros.

En definitiva, la investigación cualitativa es un instrumento para profundizar la diversidad de vida humana, proporcionando la comprensión de cómo las personas experimentan, sus relaciones y procesos sociales. Por consiguiente, estas premisas generan la formulación de una hipótesis que podrá servir de guía para futuros procesos materia de revisión.

3.1.5 ALCANCE DE INVESTIGACIÓN

El alcance de la investigación aplicado para el proyecto investigativo escogido es el descriptivo, este se encarga de analizar cómo es y de qué manera se manifiesta el fenómeno, sus componentes, características esenciales, y describe la forma en la que se produce el objeto investigado. Esta modalidad se utiliza en la mayor parte de las investigaciones jurídicas, ya que describe el tema de investigación y sus fuentes. (Ramos Galarza, 2020)

Los estudios con alcance descriptivo tienen como propósito enunciar las propiedades, características y cuestiones fundamentales del asunto que se somete a análisis. Recordemos que, el trabajo de los investigadores es describir a detalle cómo se manifiestan diversos hechos o situaciones, por lo tanto, en los estudios descriptivos se efectúa una selección de diferentes cuestiones, a las cuales se les atribuye la denominación de variables, y consecuentemente, se recaba información sobre cada una de ellas.

3.1.6 DELIMITACIÓN DE LA INVESTIGACIÓN

La presente investigación se desarrolla bajo el siguiente contexto; propuesta normativa para disminuir la afectación de delitos que se cometen a través de medios digitales en el sector empresarial en la ciudad de Guayaquil, período 2023. Tomando en consideración aquello, se logra identificar a la población o universo, la cual serían profesionales del derecho.

3.1.7 POBLACIÓN Y MUESTRA

La población es aquella que ha sido constituida por medio de un criterio de selección, en el cual el investigador debe examinar a los sujetos y al lugar de análisis. Se encuentra compuesta por cualquier grupo predeterminado, como pueden ser las personas, los animales, corporaciones o cualquier otra asociación de relevancia para la investigación. (Mucha Hospinal, Chamorro, Oseda Lazo, & Alania Contreras, 2020)

Es esencial determinar de manera concisa la población en el diseño de investigación, debido a que se trata del grupo seleccionado sobre el cual se desea obtener información y resultados. Se considera como una muestra representativa, esto es importante para la fiabilidad y validez de los hallazgos. Adicionalmente, el establecimiento de este segmento emite criterios de inclusión y exclusión.

La muestra en un proyecto investigativo, corresponde a una porción o porcentaje de la población. Es importante aclarar que, este muestreo no se realiza de acuerdo a las convicciones del investigador, sino que busca la representatividad, es decir, que tiene como finalidad que se garantice la inferencia de los resultados de la muestra hacia la población estudiada. El tamaño de esta, se determina con relación a diversos factores, como el margen de error aceptable, la población variable y la naturaleza del estudio. (Mucha Hospinal, Chamorro, Oseda Lazo, & Alania Contreras, 2020)

No obstante, en la tesis planteada se maneja un enfoque de muestra cualitativo, el cual no requiere contar con la categoría de representatividad, debido a que permite estudiar a un individuo o grupo. En este caso, se aplica un muestreo selectivo, intencional o de juicio,

que garantice profundizar, describir y comprender el fenómeno. En ese sentido, se escogió a siete abogados para que sean entrevistados. (Conejero S, 2020)

3.1.7.1 MÉTODOS A NIVEL EMPÍRICO Y TEÓRICO

Los métodos empíricos implementados son, la observación científica, la revisión documental y la entrevista. Por otra parte, los métodos a nivel teórico tales como, el análisis, deducción y síntesis. Asimismo, el *lege ferenda*; es una técnica que posibilita la capacidad de evaluar una normativa legal y su efectividad para regular un entorno social específico, lo cual va a determinar en qué medida se ajusta a las necesidades normativas del momento. Este facilita la comprensión de las áreas que requieren ser modificadas.

3.1.7.2 MÉTODO DE OBSERVACIÓN

La observación científica es un proceso importante y sencillo dentro de la investigación. Consiste en el estudio directo de una realidad, con respecto a una conducta o cosa. La recolección de los datos y su posterior revisión. Estos métodos empíricos son fuentes explicativas sobre las características del objeto. (Software DEL SOL, 2024)

3.1.7.3 ENTREVISTA

La entrevista es un instrumento que consiste en recoger información por medio de un proceso directo de comunicación entre el entrevistado y el entrevistador. Esta técnica permite que el entrevistado responda a las interrogantes planteadas por el encuestador, orientadas hacia las cuestiones que se busca indagar. (Hernández-Rodríguez, Argüelles-Pascual, & Palacios, 2021)

3.1.8 OPERACIONALIZACIÓN DE LAS VARIABLES

Arias, define a la variable como aquella palabra o frase que se encuentra inmersa en el título o tema de investigación. Por lo general, también esta evidenciada dentro del objetivo general, problema de la investigación o hipótesis, mientras que, Hernández-Sampieri y Mendoza las relaciona con la medición, observación e inferencia efectuada con relación a un

análisis de teoría. En ese sentido, las variables son herramientas que sirven para obtener datos sobre una realidad investigada. (Arias Gonzáles, 2021)

La operacionalización de las variables es un paso fundamental en el proceso de investigación, debido a que permite utilizar conceptos para poder realizar mediciones observables y concretas. En el párrafo que antecede se logra apreciar dos enfoques, por una parte, esta Arias, por el contrario, Hernández-Sampieri y Mendoza.

Tabla 5

Enfoque de arias

Identificación en el título o tema	Presencia en objetivos y problemas	Relación con la hipótesis
Esta variable es delimitada desde el comienzo de la investigación en el tema o título, considerando que posee gran relevancia para el análisis.	La variable se encuentra establecida dentro del objetivo general y planteamiento del problema, ya que se encarga de identificar la importancia en la estructura lógica del estudio.	La hipótesis es un elemento que se puede constatar de forma empírica.

Tabla 6*Enfoque de Hernández-Sampieri y Mendoza*

Medición	Observación	Inferencia teórica
Una variable deberá ser medible, ya que de esta manera podrá ser cuantificada.	La observación permite que la variable sea identificada y registrada en el contexto del estudio.	La medición y observación son dos instrumentos que tienen como finalidad realizar inferencias teóricas, a través de la vinculación de los datos recolectados conceptos abstractos de la teoría.

En conclusión, la operacionalización de las variables implica tanto su identificación inicial como su capacidad para ser medidas y observadas empíricamente. La unión de estos enfoques trae consigo que los investigadores puedan diseñar estudios sólidos y útiles para defender la tesis propuesta.

3.1.9 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

El procesamiento de la información tiene como propósito generar datos agrupados y ordenados que le permitan al investigador el estudio de la información de acuerdo con los objetivos, hipótesis e interrogantes del proceso investigativo construido. Este procedimiento colabora en la formulación de las teorías de la cognición humana y explicar distintos factores de la conducta humana. (Bernal , 2010)

ANÁLISIS DE DATOS

3.2 ENTREVISTAS

Profesional entrevistado No. 1

Nombre: Carlos Alberto Carrión Márquez

Abogado de los Tribunales y Juzgados de la República

Años de experiencia: 15 años

1. **¿Considera usted que los delitos cibernéticos son prácticas comunes en el estado ecuatoriano?**

Son prácticas poco comunes por las barreras en el acceso al uso de medios tecnológicos.

2. **¿Podría usted definir el delito de suplantación de identidad?**

Anteponer o utilizar dolosamente una identidad de una tercera persona sin consentimiento de su titular.

3. **¿Conoce los tipos penales que son cometidos a través de medios digitales?**

Sí.

4. **¿Cuáles son los bienes jurídicos protegidos que vulnera la configuración de los delitos cometidos por medios digitales?**

Propiedad e identidad.

5. **¿Está conforme con el rol que desempeñan las entidades públicas ecuatorianas con respecto a la detección y sanción del phishing?**

No.

6. **¿Considera apropiada la tipificación del delito de “Apropiación fraudulenta por medios electrónicos” contemplada en el Código Orgánico Integral Penal?**

No.

7. **¿Cree que las diversas tipologías del phishing deberían ser tipificadas a nivel normativo?**

Sí.

- 8. ¿Qué opina usted con relación a la viabilidad de aplicación de una propuesta normativa para disminuir los delitos de suplantación de identidad en el sector empresarial?**

La propuesta es interesante porque existen herramientas en el ámbito societario, como el levantamiento del velo societario, que es utilizado durante un proceso judicial o arbitral.

- 9. ¿Cree usted que Ecuador disminuirá su índice en delitos cometidos a través de medios digitales si se suscribe a mayor cantidad de tratados internacionales de intercambio de información tributaria?**

Posiblemente, pero lo más importante es tener los funcionarios idóneos que sepan usarlas y aplicarlas en cada caso concreto. Que "no miren para otro lado" y puedan denunciarlo sin miedo a represalias.

Profesional entrevistado No. 2

Nombre: Andrés Rodrigo Jácome Cobo

Abogado de los Tribunales y Juzgados de la República

Años de experiencia: 20 años

1. ¿Considera usted que los delitos cibernéticos son prácticas comunes en el estado ecuatoriano?

Con el desarrollo de la tecnología y su apropiación por parte de las personas de toda edad se ha ido incrementado cada vez más el cometimiento de delitos cibernéticos dentro de la sociedad ecuatoriana. Esta tendencia es incremental por la facilidad que brindan los medios tecnológicos, las deficiencias y desconocimiento que tienen los usuarios de plataformas, y sistemas de información.

2. ¿Podría usted definir el delito de suplantación de identidad?

Consiste en una actividad fraudulenta donde los delincuentes, utilizando sin autorización y de manera ilegal la identidad de otras personas o instituciones, se hacen pasar por ellas, con el propósito de obtener beneficios o recursos económicos de manera ilegal.

3. ¿Conoce los tipos penales que son cometidos a través de medios digitales?

Conforme los tipos penales descritos en el Código Integral Penal los delitos que se cometen a través de medios digitales son alrededor de 18 que están claramente identificados. Sin embargo, hay delitos que conforme a lo establecido en el COIP se podrían cometer a través de cualquier medio, lo que implica que también podrían ser parte, en algún momento, de los delitos cometidos por medios digitales.

4. ¿Cuáles son los bienes jurídicos protegidos que vulnera la configuración de los delitos cometidos por medios digitales?

Principalmente los bienes jurídicos vulnerados son los derechos de libertad, a la intimidad personal e integridad sexual y reproductiva, a la propiedad en todas sus formas

(incluye la propiedad intelectual), derechos contra el Buen Vivir (a la seguridad de los activos de los sistemas de información y comunicación) y contra el Estado.

5. ¿Está conforme con el rol que desempeñan las entidades públicas ecuatorianas con respecto a la detección y sanción del phishing?

La responsabilidad sobre la detección, control y sanción no solamente recae en el accionar de las entidades y autoridades públicas, ya que este delito se produce en razón del desconocimiento o ingenuidad de las personas que suministran información y datos sin observar las mínimas recomendaciones de seguridad. Por su parte, las entidades públicas deben realizar mayores campañas y fortalecer los educación y capacitación en materia de ciberseguridad.

6. ¿Considera apropiada la tipificación del delito de “Apropiación fraudulenta por medios electrónicos” contemplada en el Código Orgánico Integral Penal?

Me parece que la sanción prevista no necesariamente guarda relación con el beneficio que pudiere obtener el delincuente. Creo particularmente que la sanción debería estar entre 5 y 7 años.

7. ¿Cree que las diversas tipologías del phishing deberían ser tipificadas a nivel normativo?

No, ya que la tecnología cambia a cada día y por tanto no es conveniente establecer infracciones en función de las diversas formas que se comenten los delitos.

8. ¿Qué opina usted con relación a la viabilidad de aplicación de una propuesta normativa para disminuir los delitos de suplantación de identidad en el sector empresarial?

Innecesaria, ya la sanción a dicha conducta debe ser aplicada en todos los sectores de la sociedad.

- 9. ¿Cree usted que Ecuador disminuirá su índice en delitos cometidos a través de medios digitales si se suscribe a mayor cantidad de tratados internacionales de intercambio de información tributaria?**

Si, la cooperación internacional fortalecería el esquema preventivo, investigativo y sancionatorio por lo que habría un verdadero desincentivo para el cometimiento de estas conductas.

Profesional entrevistado No. 3

Nombre: Luis Alberto Quintero Angulo

Abogado de los Tribunales y Juzgados de la República

Maestría en derecho laboral

Años de experiencia: 14 años

- 1. ¿Considera usted que los delitos cibernéticos son prácticas comunes en el estado ecuatoriano?**

En la actualidad, claramente sí.

- 2. ¿Podría usted definir el delito de suplantación de identidad?**

Una especie de fraude en línea, usurpación de funciones o nombres y que en sí constituye el delito como tal, al utilizarse la identidad de otra persona.

- 3. ¿Conoce los tipos penales que son cometidos a través de medios digitales?**

Usurpación de identidad, distribución de imágenes sexuales con menores, estafa y phishing.

- 4. ¿Cuáles son los bienes jurídicos protegidos que vulnera la configuración de los delitos cometidos por medios digitales?**

Derecho a la identidad, derechos patrimoniales, entre otros.

- 5. ¿Está conforme con el rol que desempeñan las entidades públicas ecuatorianas con respecto a la detección y sanción del phishing?**

En nuestro país no existe una cultura de prevención de adquisición fraudulenta de información personal confidencial o phishing, las entidades públicas y las privadas se generan un avance en este sentido, no protegen adecuadamente los datos de los usuarios o clientes.

- 6. ¿Considera apropiada la tipificación del delito de “Apropiación fraudulenta por medios electrónicos” contemplada en el Código Orgánico Integral Penal?**

Creo que a esa norma le toca actualizarse. Por ejemplo, la especificación de los medios digitales actuales como aplicaciones, inteligencia artificial, entre otras.

7. ¿Cree que las diversas tipologías del phishing deberían ser tipificadas a nivel normativo?

Considero que sí ya que en materia penal se aplica el principio de tipicidad o legalidad, por lo tanto, al no estar normado podría perderse la capacidad de sanción.

8. ¿Qué opina usted con relación a la viabilidad de aplicación de una propuesta normativa para disminuir los delitos de suplantación de identidad en el sector empresarial?

Sería interesante, y además de aplicar una reforma legal o inclusión de un texto legal, debería incluirse la forma de aplicación y la ejecución de dicha figura, determinándose la entidad competente y hasta, de ser posible, quien debe financiarla

9. ¿Cree usted que Ecuador disminuirá su índice en delitos cometidos a través de medios digitales si se suscribe a mayor cantidad de tratados internacionales de intercambio de información tributaria?

Disminución de delitos podría ser con la ayuda de varios factores de aplicación interna, no solamente con la suscripción de un tratado internacional, ya que los controles empiezan a la interna.

Profesional entrevistado No. 4**Nombre:** Alex López Ávila

Abogado de los Tribunales y Juzgados de la República

Años de experiencia: 15 años

1. **¿Considera usted que los delitos cibernéticos son prácticas comunes en el estado ecuatoriano?**

Sí.

2. **¿Podría usted definir el delito de suplantación de identidad?**

Quien públicamente tome el nombre de otra persona.

3. **¿Conoce los tipos penales que son cometidos a través de medios digitales?**

Sí.

4. **¿Cuáles son los bienes jurídicos protegidos que vulnera la configuración de los delitos cometidos por medios digitales?**

Depende el delito, por cuanto existe un capítulo especial sobre estos delitos, no se agotan los mismos en ese capítulo.

5. **¿Está conforme con el rol que desempeñan las entidades públicas ecuatorianas con respecto a la detección y sanción del phishing?**

No.

6. **¿Considera apropiada la tipificación del delito de “Apropiación fraudulenta por medios electrónicos” contemplada en el Código Orgánico Integral Penal?**

Sí.

7. **¿Cree que las diversas tipologías del phishing deberían ser tipificadas a nivel normativo?**

No, ya que es un medio para cometer varios delitos, de distintos bienes jurídicos.

8. **¿Qué opina usted con relación a la viabilidad de aplicación de una propuesta normativa para disminuir los delitos de suplantación de identidad en el sector empresarial?**

Considero que sería un mecanismo viable de aplicación.

- 9. ¿Cree usted que Ecuador disminuirá su índice en delitos cometidos a través de medios digitales si se suscribe a mayor cantidad de tratados internacionales de intercambio de información tributaria?**

No.

Profesional entrevistado No. 5

Nombre: Alfredo Andrés Coello Zambrano

Abogado de los Tribunales y Juzgados de la República

Años de experiencia: 10 años

1. ¿Considera usted que los delitos cibernéticos son prácticas comunes en el estado ecuatoriano?

Los delitos cibernéticos son una práctica común en Ecuador, impulsada por la creciente conectividad digital y las sofisticadas técnicas de los ciberdelincuentes. Los delitos más frecuentes incluyen el phishing, la creación de sitios web fraudulentos, el robo de datos personales y bancarios mediante enlaces maliciosos, y la suplantación de identidad en redes sociales.

2. ¿Podría usted definir el delito de suplantación de identidad?

Casos de suplantación de identidad en Ecuador involucran diversas actividades fraudulentas, como la obtención de créditos o la realización de compras utilizando documentos falsificados.

3. ¿Conoce los tipos penales que son cometidos a través de medios digitales?

Suplantación de identidad Phishing Fraude informático Acceso no autorizado a sistemas informáticos Pornografía infantil Hackeo de cuentas.

4. ¿Cuáles son los bienes jurídicos protegidos que vulnera la configuración de los delitos cometidos por medios digitales?

La identidad personal El patrimonio La integridad y privacidad de la información La libertad y seguridad personal La dignidad y la integridad moral La seguridad de los sistemas y datos informáticos.

5. ¿Está conforme con el rol que desempeñan las entidades públicas ecuatorianas con respecto a la detección y sanción del phishing?

Aunque las entidades públicas ecuatorianas han tomado medidas importantes para combatir el phishing, todavía hay margen para mejorar en términos de capacidad de respuesta, eficacia de las tecnologías de autenticación y disponibilidad de recursos especializados. A pesar de los esfuerzos, la capacidad de las entidades para detectar y responder a los incidentes de phishing aún enfrenta limitaciones. Los ciberdelincuentes continúan evolucionando sus tácticas, utilizando métodos cada vez más sofisticados para evadir la detección. Aunque se utilizan estándares como SPF, DKIM y DMARC para la autenticación de correos electrónicos, los atacantes a menudo encuentran formas de eludir estos mecanismos.

6. ¿Considera apropiada la tipificación del delito de “Apropiación fraudulenta por medios electrónicos” contemplada en el Código Orgánico Integral Penal?

Es apropiada y se alinea con las necesidades actuales de protección contra delitos informáticos. Esta medida no solo moderniza el marco legal, sino que también fortalece la protección del patrimonio de los ciudadanos y mejora la capacidad de respuesta frente a la ciberdelincuencia. Este delito protege de manera efectiva el patrimonio de las personas, considerando que las transacciones financieras y otras operaciones económicas se realizan cada vez más en el ámbito digital.

7. ¿Cree que las diversas tipologías del phishing deberían ser tipificadas a nivel normativo?

Sí, tipificar las diversas tipologías del phishing en la legislación ecuatoriana puede mejorar la efectividad de la lucha contra este delito, proporcionar mayor claridad en los procesos judiciales, y ofrecer una mejor protección y concienciación a la población.

8. ¿Qué opina usted con relación a la viabilidad de aplicación de una propuesta normativa para disminuir los delitos de suplantación de identidad en el sector empresarial?

Su éxito dependerá de una implementación cuidadosa que considere los costos, la necesidad de capacitación, la colaboración entre sectores y la capacidad de adaptación a nuevos desafíos tecnológicos. Una normativa específica puede obligar a las empresas a implementar medidas de seguridad más robustas para proteger los datos personales y empresariales.

9. ¿Cree usted que Ecuador disminuirá su índice en delitos cometidos a través de medios digitales si se suscribe a mayor cantidad de tratados internacionales de intercambio de información tributaria?

Si. La mejora en la cooperación internacional, la adopción de buenas prácticas y el fortalecimiento de la legislación pueden contribuir a una disminución de los delitos cometidos a través de medios digitales en Ecuador. La cooperación internacional mediante el intercambio de información tributaria puede ayudar a identificar y rastrear flujos financieros ilícitos que suelen estar asociados con actividades delictivas digitales, como el fraude fiscal y el lavado de dinero.

Profesional entrevistado No. 6

Nombre: Washington Manuel Salvador Quiñónez

Abogado de los Tribunales y Juzgados de la República

Años de experiencia: 25 años

1. ¿Considera usted que los delitos cibernéticos son prácticas comunes en el estado ecuatoriano?

En la actualidad los ciberdelitos se volvieron comunes, toda vez, que se cometen con frecuencia y cada día hay más personas afectadas.

2. ¿Podría usted definir el delito de suplantación de identidad?

Básicamente es falsificar la identidad de una persona. Sacar ventaja haciéndose pasar por una persona en común.

3. ¿Conoce los tipos penales que son cometidos a través de medios digitales?

Suplantación de identidad, Phishing y Carding,

4. ¿Cuáles son los bienes jurídicos protegidos que vulnera la configuración de los delitos cometidos por medios digitales?

La vida, la libertad, el patrimonio, la seguridad y la salud.

5. ¿Está conforme con el rol que desempeñan las entidades públicas ecuatorianas con respecto a la detección y sanción del phishing?

Si, en la actualidad las instituciones financieras aplican mediada preventivas con el Objetivo de evitar este tipo de delitos.

6. ¿Considera apropiada la tipificación del delito de “Apropiación fraudulenta por medios electrónicos” contemplada en el Código Orgánico Integral Penal?

Si, estoy de acuerdo con la pena pronostica de libertad establecida en el COIP para este tipo de delitos.

7. ¿Cree que las diversas tipologías del phishing deberían ser tipificadas a nivel normativo?

Si, considero que debería aplicarse de manera general para generalizar este tipo de delitos.

8. ¿Qué opina usted con relación a la viabilidad de aplicación de una propuesta normativa para disminuir los delitos de suplantación de identidad en el sector empresarial?

Considero viable que se regularice y se generalice una normativa expresa para evitar que se cometan este tipo de delitos.

9. ¿Cree usted que Ecuador disminuirá su índice en delitos cometidos a través de medios digitales si se suscribe a mayor cantidad de tratados internacionales de intercambio de información tributaria?

No, más bien sería robustecer las medidas preventivas que se aplican en la actualidad. Endurecer la pena privativa de libertad para los ciberdelitos.

Profesional entrevistado No. 7

Nombre: David Sebastián Vergara Solís

Abogado de los Tribunales y Juzgados de la República

Años de experiencia: 10 años

1. ¿Considera usted que los delitos cibernéticos son prácticas comunes en el estado ecuatoriano?

Son prácticas comunes. Cada año se denuncian aproximadamente 2000 delitos informáticos en fiscalía. sin embargo, muchas víctimas no denuncian los delitos informáticos por desconocimiento o por falta de interés o falta de confianza en el sistema de justicia.

2. ¿Podría usted definir el delito de suplantación de identidad?

Es la conducta por la cual una persona suplanta la identidad de otra persona, con el propósito de obtener un aprovechamiento ilegítimo.

3. ¿Conoce los tipos penales que son cometidos a través de medios digitales?

Dentro de la doctrina, se menciona que los delitos electrónicos o informáticos propios son aquellos que solamente pueden ser cometidos por medios digitales. por ejemplo, el acceso no consentido a un sistema informático (hacking).

¿Cuáles son los bienes jurídicos protegidos que vulnera la configuración de los delitos cometidos por medios digitales?

Existen muchos bienes jurídicos protegidos que pueden ser vulnerados por un delito informático, siendo los principales: La integridad del sistema informático, la privacidad, intimidad, buen nombre, honor, reputación, propiedad, propiedad intelectual, integridad sexual de menores, etc.

¿Está conforme con el rol que desempeñan las entidades públicas ecuatorianas con respecto a la detección y sanción del phishing?

Las instituciones del estado deberían tener más acción para combatir el delito informático. Su actividad es muy tibia.

¿Considera apropiada la tipificación del delito de “Apropiación fraudulenta por medios electrónicos” contemplada en el Código Orgánico Integral Penal?

“Art. 190.- Apropiación fraudulenta por medios electrónicos”.

No tengo ningún comentario de crítica a la redacción del artículo.

¿Cree que las diversas tipologías del phishing deberían ser tipificadas a nivel normativo?

La conducta de phishing si debería ser considerada como un delito autónomo, ya que es bastante común como técnica para obtener información personal y dinero ilícito, por lo que debería ser sancionada como una conducta penal como mecanismo de política criminal para la prevención general de dicho acto.

¿Qué opina usted con relación a la viabilidad de aplicación de una propuesta normativa para disminuir los delitos de suplantación de identidad en el sector empresarial?

Si es factible, ya que muchas veces se suplanta la identidad de compañías y empresas, por lo que se las investiga cuando en realidad no tienen asunto en la conducta ilícita. por lo tanto, debería ser un eximente de responsabilidad si estas empresas han adoptado mecanismos para alertar al público cuando existan una suplantación de identidad. por ejemplo, podría ser que se considere como eximente el envío masivo de un correo electrónico de alerta sobre un posible phishing.

¿Cree usted que Ecuador disminuirá su índice en delitos cometidos a través de medios digitales si se suscribe a mayor cantidad de tratados internacionales de intercambio de información tributaria?

Es más recomendable que el ecuador suscriba tratados internacionales, en especial el convenio sobre la ciberdelincuencia de Budapest, para armonizar la legislación y tener

mecanismos de cooperación entre los países suscriptores, para la prueba y juzgamiento de los delitos electrónicos, ya que los mismos son transnacionales.

3.3 DISCUSIÓN DE RESULTADOS

Tabla 7

Análisis de entrevistas

INTERROGANTE PLANTEADA	CONCLUSIONES OBTENIDAS
<p>¿Considera usted que los delitos cibernéticos son prácticas comunes en el estado ecuatoriano?</p>	<p>Se evidencia una notoria inclinación mayoritaria en cuanto a la catalogación de los delitos cibernéticos como prácticas comunes, debido a que estos guardan relación con la constante actualización de los sistemas de la información y su facilidad de acceso. Es relevante mencionar que las diversas tipologías de los delitos informáticos se materializan por la falta de denuncias realizadas por parte de la totalidad de las víctimas, quienes por desconocimiento o falta de interés lo dejan pasar desapercibido. No obstante, de lo que se conoce, alrededor de 2000 personas sufren por este delito cada año y han sido puestos en conocimiento de la Fiscalía General del Estado.</p>
<p>¿Podría usted definir el delito de suplantación de identidad?</p>	<p>La suplantación de identidad es considerada como una práctica ilegal que</p>

	<p>tiene como propósito obtener una apropiación fraudulenta por medios telemáticos que ocasione un beneficio para el infractor o un tercero, como la obtención de créditos o la realización de compras utilizando documentos falsificados.</p>
<p>¿Conoce los tipos penales que son cometidos a través de medios digitales?</p>	<p>Existen una gran cantidad de delitos informáticos estos únicamente pueden ser cometidos por medios digitales. Por ejemplo; El acceso no consentido a un sistema informático (Hacking), suplantación de identidad (Phishing), fraude informático, estafa, distribución de imágenes sexuales con menores, entre otros.</p>
<p>¿Cuáles son los bienes jurídicos protegidos que vulnera la configuración de los delitos cometidos por medios digitales?</p>	<p>Los bienes jurídicos protegidos que pueden ser vulnerados por un delito informático son: La integridad de los sistemas y datos informáticos, la intimidad, el patrimonio, la propiedad intelectual, el honor, el buen nombre, y la integridad sexual y reproductiva.</p>
<p>¿Está conforme con el rol que desempeñan las entidades públicas ecuatorianas con respecto a la detección y sanción del phishing?</p>	<p>Las entidades públicas ecuatorianas cumplen con su rol de detección, control y sanción, pero deben fortalecer su accionar, ya que pese a las medidas</p>

	<p>adoptadas se siguen cometiendo los ciberdelitos. No obstante, la responsabilidad de la materialización de estos delitos no es solo una situación propia de la falta de acción estatal, sino que también incide la inobservancia de los usuarios a las recomendaciones mínimas en cuanto a la seguridad al momento de suministrar información personal por medio de plataformas digitales.</p> <p>En la misma línea, es pertinente que las organizaciones públicas y privadas protejan adecuadamente los datos de los clientes o usuarios, para evitar vulneraciones al sistema informático, lo cual demuestra que en el estado ecuatoriano no se evidencia una cultura preventiva.</p> <p>A pesar de los esfuerzos para la detección y sanción, estos delitos cibernéticos aun enfrentan diversas limitaciones, en virtud de que los delincuentes cada vez utilizan métodos más sofisticados.</p>
<p>¿Considera apropiada la tipificación del delito de “Apropiación fraudulenta</p>	<p>Hay dos vertientes en cuanto a la pregunta planteada. Por una parte, se</p>

<p>por medios electrónicos” contemplada en el Código Orgánico Integral Penal?</p>	<p>considera que la tipificación del artículo 190 del Código Orgánico Integral Penal es adecuada, ya que se alinea a las necesidades actuales de protección contra los delitos informáticos, y también mejora la capacidad de respuesta frente a los ciberdelitos, mientras que, el resto de los entrevistados consideran que si sería viable establecer una pena privativa de libertad más rigurosa y especificar los medios digitales actuales utilizados para realizar estas prácticas ilegales.</p>
<p>¿Cree que las diversas tipologías del phishing deberían ser tipificadas a nivel normativo?</p>	<p>En cuanto a las diversas tipologías de phishing se establecieron dos criterios:</p> <ol style="list-style-type: none"> 1) Se considera esencial efectuar la tipificación de estos delitos, debido a que día a día se configuran nuevas modalidades que afectan a diversos bienes jurídicos protegidos. 2) Es necesaria la reglamentación de los delitos en materia penal por el principio de legalidad, con el propósito de realizar una lucha efectiva en contra del phishing, ya que este es autónomo y muy común.
<p>¿Qué opina usted con relación a la viabilidad de aplicación de una propuesta normativa para disminuir</p>	<p>La propuesta normativa para disminuir los delitos de suplantación de identidad en el sector empresarial tuvo gran acogida</p>

<p>los delitos de suplantación de identidad en el sector empresarial?</p>	<p>entre los participantes. En definitiva, se estableció la innovación en cuanto a la aplicación de una reforma o texto legal orientado a combatir el phishing, lo cual solo podrá ser posible a través de la cooperación entre sectores, las capacitaciones pertinentes al personal y la adaptación a nuevos desafíos tecnológicos. Otro aspecto fundamental debe ser eximir de responsabilidad a las empresas que han adoptado mecanismos para alertar al público sobre las posibles amenazas cibernéticas.</p>
<p>¿Cree usted que Ecuador disminuirá su índice en delitos cometidos a través de medios digitales si se suscribe a mayor cantidad de tratados internacionales de intercambio de información tributaria?</p>	<p>Se evidenciaron posturas divididas entre los expertos. En virtud de que, una parte considera que el real inconveniente de prevención y detección de los delitos radica en la falta de rigurosidad normativa a nivel interno, y en otra perspectiva, relacionan los criterios de mejora con la adopción de buenas prácticas y la cooperación internacional, como es el caso del tratado de Budapest, para armonizar la legislación y tener un mecanismo entre países suscriptores en cuanto a las prueba y juzgamiento.</p>

Fuente: Elaboración propia

CAPÍTULO 4

4.1 CONCLUSIONES

El incremento en el uso de los sistemas digitales ha ocasionado una creciente brecha de frecuencia y sofisticación en el cometimiento de los delitos electrónicos. Esta problemática afecta de manera notoria a las organizaciones corporativas en la ciudad de Guayaquil, en virtud de que, los criminales encuentran nuevas formas de aplicar modalidades delictivas por medio de la tecnología. La materialización de deficiencias normativas adecuadas y actualizadas genera una situación grave, debido a que los atacantes ejecutan sabotajes empresariales con relativa impunidad.

Los ciberdelitos no solo afectan a la seguridad de la información organizacional, sino que también, traen consigo una afectación a la esfera económica. Las empresas sufren grandes pérdidas financieras por las extorsiones, los fraudes y los costos relacionados con la recuperación y el fortalecimiento de la seguridad informática. Otro aspecto relevante a destacar, es que los inconvenientes de vulneraciones a los sistemas de la información pueden dañar la reputación de las corporaciones, disminuyendo la confianza de sus clientes y socios comerciales.

La adecuación de la normativa legal vigente favorece la cooperación entre las entidades gubernamentales de vigilancia, lo cual ocasiona que existan respuestas eficaces ante los incidentes que se suscitan en índole telemática. Las entidades empresariales requieren del establecimiento de medidas de prevención, detección y represión. Asimismo, las leyes pueden promover la implementación de mejores prácticas de seguridad ante las contingencias, promoviendo la resiliencia del ámbito empresarial de la ciudad de Guayaquil con relación a los ciberdelitos.

La suplantación de identidad se ha transformado en uno de los riesgos más latentes y refinados en la esfera corporativa de Guayaquil. Esta conducta criminal, abarca desde el phishing hasta la creación de perfiles falsos en redes sociales y el acceso no consentido a sistemas empresariales, lo cual constituye un hecho revolucionario. La falta de educación y conciencia acerca de la seguridad cibernética entre los colaboradores y altos mandos de las

empresas genera la problemática estudiada, ya que incrementa la posibilidad de ser víctimas de vulneraciones.

La propagación del phishing acarrea consecuencias operativas y económicas graves para la corporación. Estos delitos pueden ocasionar menoscabo en los datos de carácter confidencial, la interrupción de operaciones críticas y el desvío de fondos. Además, la recuperación de la confianza en los clientes será un suceso complejo.

La lucha contra la suplantación de identidad necesita una cooperación entre la esfera empresarial, las autoridades legislativas y los proveedores de servicios de tecnología. Esto abarca los canales de comunicación y coordinación entre las corporaciones, la gestión de denuncia rápida ante las fuerzas del orden y las respuestas en cuanto a cuestiones de phishing.

Es importante conocer y catalogar las diferentes tipologías de los ciberdelitos que generan una afectación al sector empresarial en la ciudad de Guayaquil. Entre los delitos identificados se encuentran, phishing, smishing, vishing, spear phishing, whale phishing, social phish y shellphish. La determinación a detalle de estos modus operandi delincuenciales permite combatir este tipo de delitos.

La concientización y capacitación frecuente a los colaboradores es esencial para evitar la propagación de los delitos electrónicos. En ese sentido, el personal deberá estar educado para tratar amenazas en el entorno digital de manera emergente. De esta manera, se podrá crear un ambiente más seguro y confiable en la ciudad de Guayaquil.

En definitiva, la implementación de medios tecnológicos, es importante para prevenir la configuración de delitos electrónicos, lo cual será posible por medio de la utilización de sistemas avanzados de seguridad y detección ante los ataques ocasionados por parte de los delincuentes cibernéticos. La reforma propuesta propone mejorar la adopción de prácticas conjuntas de aplicación en beneficio del sector empresarial.

4.2 RECOMENDACIÓN / PROPUESTA

La presente propuesta tiene como finalidad establecer una reforma al Código Orgánico Integral Penal. En virtud de que se considera esencial agregar un inciso al tipo penal de apropiación fraudulenta por medios electrónicos contemplado en el artículo 190 encamado a sancionar las conductas penalmente relevantes que se configuran en la esfera empresarial.

Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes. (REPÚBLICA DEL ECUADOR ASAMBLEA NACIONAL, 2014)

Inciso agregado:

En caso de que una persona incurra en una circunstancia lesiva para el sector empresarial, específicamente, por medio de la apropiación fraudulenta por medios electrónicos, la cual evidencie una pérdida económica significativa para la empresa que como resultado genere una disminución del 10% de los ingresos anuales, será sancionada con una pena privativa de libertad de tres a cinco años.

En definitiva, se recomienda la aplicación de este inciso, debido a que la esfera empresarial no se encuentra delimitada en este tipo penal, lo cual implica que se realice su respectiva distinción en cuanto a la configuración de la Apropiación fraudulenta por medios electrónicos. Si bien es cierto, el ámbito organizacional trae consigo varias condicionantes, dentro de las cuales se destaca el acceso de grandes sumas monetarias. En ese sentido, es fundamental aumentar la rigurosidad de la pena para las personas que lesionan este bien jurídico protegido del patrimonio.

4.3 BIBLIOGRAFÍA

- Alcívar Trejo, C., Calderón Cisneros, J., Blanc Pihuave, G., & Duchi Ortega, B. (08 de diciembre de 2016). ANÁLISIS ESPACIAL DE LOS DELITOS Y APLICACIÓN DE LA NORMATIVA JURÍDICA ECUATORIANA. 86. Obtenido de <https://libros.ecotec.edu.ec/index.php/editorial/catalog/book/32>
- Arias Gonzáles, J. L. (1 de octubre de 2021). *Guía para elaborar la operacionalización*. Obtenido de <file:///C:/Users/HP/Downloads/admin,+02.+Gu%C3%ADa.pdf>
- BBVA. (2024). 'Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas? Obtenido de <https://www.bbva.com/es/innovacion/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/>
- Bernal , C. A. (2010). *Proceso de investigación científica*. Obtenido de <http://librodigital.sangregorio.edu.ec/librosusgp/B0061.pdf>
- Blossiers Mazzini, C. M. (2018). *Metodología de la investigación científica. Pautas metodológicas para elaborar un proyecto de investigación*.
- Cano, W. D., & Monsalve Machado, S. (2023). *CIBERSEGURIDAD, RETO EMPRESARIAL PARA AFRONTAR LA ERA DE LA DIGITALIZACION ACTUAL*. Obtenido de <https://repository.upb.edu.co/bitstream/handle/20.500.11912/11318/Ciberseguridad%2c%20reto%20empresarial%20para%20afrontar%20la%20era%20de%20la%20digitalizaci%c3%b3n%20actual.pdf?sequence=1&isAllowed=y>
- Conejero S, J. (2020). *UNA APROXIMACIÓN A LA INVESTIGACION CUALITATIVA*. Obtenido de <https://www.neumologia-pediatrica.cl/index.php/NP/article/view/57/57>
- FISCALÍA GENERAL DEL ESTADO. (2020). *Fiscalía abrió instrucción fiscal contra 6 procesados por presunto "phishing"*. Obtenido de <https://www.fiscalia.gob.ec/fiscalia-abrio-instruccion-fiscal-contr-6-procesados-por-presunto-phishing/>

- Guaña Moya, J., Chiluisa Chiluisa, M., Jaramillo-Flores, P., Naranjo Villota, D., Mora Zambrano, E., & Larrea Torres, L. (2022). *Ataques de phishing y cómo prevenirlos*. Obtenido de <https://13deabril.edu.ec/wp-content/uploads/2022/10/13-Ataques-de-phishing-y-como-prevenirlos.pdf>
- Guarnizo Portela, M. P. (04 de mayo de 2020). *La naturaleza jurídica de los delitos informáticos en Colombia*. Obtenido de <https://repository.unad.edu.co/handle/10596/41392>
- Guerrero Dávila, G., & Guerrero Dávila, M. C. (2020). *Metología de la investigación*. Obtenido de <https://books.google.es/books?hl=es&lr=&id=sJstEAAQBAJ&oi=fnd&pg=PP1&dq=metodolog%C3%ADa+en+pdf&ots=-j3f4-2ZMq&sig=KlArCMC6sviQdJrkOsNKC9QYssQ>
- Guzmán, V. (31 de diciembre de 2021). *El método cualitativo y su aporte a la investigación en las ciencias sociales*. Obtenido de <https://revistagestionar.com/index.php/rg/article/view/17/47>
- Hernández-Rodríguez, A., Argüelles-Pascual, V., & Palacios, R. (2021). *Métodos empíricos de la investigación*. Obtenido de <https://repository.uaeh.edu.mx/revistas/index.php/huejutla/article/view/6701/7600>
- Instituto Superior Tecnológico ATLANTIC. (30 de junio de 2020). *Paradigmas, enfoques y métodos de investigación: análisis teórico*. Obtenido de <https://drive.google.com/file/d/1v17S1dPpkES8zUwyfenm0Jn6PmzAsKMO/view>
- Iñahuazo López, A. J. (16 de enero de 2024). *Estudio jurídico y doctrinario sobre el ciberdelito denominado phishing y la falta de normativa legal que regule los delitos informáticos*. Recuperado el 2024, de <https://dspace.unl.edu.ec/jspui/handle/123456789/28767>

La Asamblea Nacional. (02 de febrero de 2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL*.

Obtenido de <https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf>

Lopez Ocampo, H. I. (2023). *Medidas de seguridad bancarias para mitigar la vulneración de derechos de los usuarios frente al phishing en el sistema financiero*. Obtenido de

https://tesis.usat.edu.pe/bitstream/20.500.12423/6891/1/TL_LopezOcampoHuillari.pdf

Ministerio de Educación . (7 de agosto de 2020). *Delitos informáticos* . Obtenido de

[https://recursos.educacion.gob.ec/art2/#:~:text=Los%20delitos%20inform%C3%A1ticos%20se%20presentan,personal%20confidencial\)%2C%20entre%20otros.](https://recursos.educacion.gob.ec/art2/#:~:text=Los%20delitos%20inform%C3%A1ticos%20se%20presentan,personal%20confidencial)%2C%20entre%20otros.)

Montiel Rojas, A. (1999). *DELITO Y SUS CLASES*. Michoacan, México. Obtenido de

<https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadelia/Cap2.htm>

Mucha Hospinal, L. F., Chamorro, M. R., Oseda Lazo, M. E., & Alania Contreras, R. D. (31 de diciembre de 2020). *Evaluación de procedimientos empleados para determinar la población y muestra en trabajos de investigación de posgrado*. Obtenido de

<http://revistas.udh.edu.pe/index.php/udh/article/view/253e/23>

Nascimento Fernández, L. D. (10 de junio de 2021). *PHISHING: ASPECTOS TÉCNICOS Y PROCESALES DEL DELITO ESTRELLA EN TIEMPOS DE PANDEMIA*. Obtenido de

<https://burjcdigital.urjc.es/bitstream/handle/10115/17989/TFG%20VERSI%c3%93N%20FINAL.pdf?sequence=1&isAllowed=y>

Obtenido de

Nazario Delgado, N. Y., & Villanueva Sanchez, L. V. (2022). *FRAUDE INFORMÁTICO EN LA MODALIDAD DE PHISHING Y LA NECESARIA ACTUALIZACIÓN DE LA LEGISLACIÓN PARA UNA EFICIENTE PERSECUCIÓN Y SANCIÓN PENAL*.

Obtenido de

<https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10002/Nazario%20Delg>

ado%20Nora%20%26%20Villanueva%20Sanchez%20Lucia.pdf?sequence=6&isAllowed=y

Ramos Galarza, C. (diciembre de 2020). *LOS ALCANCES DE UNA INVESTIGACIÓN*.

Obtenido de <https://dialnet.unirioja.es/servlet/articulo?codigo=7746475>

REPÚBLICA DEL ECUADOR ASAMBLEA NACIONAL. (2014). *CÓDIGO ORGÁNICO*

INTEGRAL PENAL. Quito, Ecuador: Lexis S.A. Obtenido de

<https://www.igualdadgenero.gob.ec/wp-content/uploads/2023/03/CODIGO-ORGANICO-INTEGRAL-PENAL-COIP.pdf>

Ruiz Castro, N. E. (02 de septiembre de 2021). *LA GLOBALIZACIÓN Y SU EFECTO EN*

LOS DELITOS INFORMÁTICOS. Obtenido de

<https://oldri.ues.edu.sv/id/eprint/25008/>

Saltos Salgado, M. F., Robalino Villafuerte, J. L., & Pazmiño Salazar, L. D. (07 de enero de

2021). *ANÁLISIS CONCEPTUAL DEL DELITO INFORMÁTICO EN ECUADOR*.

Obtenido de <http://scielo.sld.cu/pdf/rc/v17n78/1990-8644-rc-17-78-343.pdf>

SciELO. (02 de Febrero de 2021). *Análisis conceptual del delito informático en Ecuador*.

Obtenido de [http://scielo.sld.cu/scielo.php?pid=s1990-](http://scielo.sld.cu/scielo.php?pid=s1990-86442021000100343&script=sci_arttext)

[86442021000100343&script=sci_arttext](http://scielo.sld.cu/scielo.php?pid=s1990-86442021000100343&script=sci_arttext)

Sempertegui Torres, M. P. (2022). *DELITO DE APROPIACIÓN FRAUDULENTO POR*

MEDIOS ELECTRÓNICOS BAJO LA MODALIDAD DE PHISING DENTRO DEL

MARCO JURÍDICO ECUATORIANO. Obtenido de

<http://dspace.uazuay.edu.ec/handle/datos/12380>

Software DEL SOL. (2024). *Métodos de investigación*. Obtenido de

[https://www.sdelsol.com/blog/tendencias/metodos-de-](https://www.sdelsol.com/blog/tendencias/metodos-de-investigacion/#:~:text=El%20m%C3%A9todo%20emp%C3%ADrico%20consiste%20en,%2C%20una%20conducta%2C%20etc.)

[investigacion/#:~:text=El%20m%C3%A9todo%20emp%C3%ADrico%20consiste%20en,%2C%20una%20conducta%2C%20etc.\)](https://www.sdelsol.com/blog/tendencias/metodos-de-investigacion/#:~:text=El%20m%C3%A9todo%20emp%C3%ADrico%20consiste%20en,%2C%20una%20conducta%2C%20etc.)

Universidad Ecotec. (2016). *Análisis espacial de los delitos y aplicación de la normativa jurídica ecuatoriana*. Obtenido de <https://fdocuments.ec/document/analisis-espacial-de-los-delitos-y-aplicacion-de-titulo-analisis-espacial.html?page=1>

Villavicencio Terreros, F. (2014). *Delitos Informáticos*. Obtenido de <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630>

Zaffaroni, R. (2006). *Manual de Derecho Penal*. Buenos Aires: Ediar.

4.4 ANEXOS

Solicitudes de entrevistas

Su experiencia y conocimiento serían de gran ayuda para enriquecer esta investigación. Le adjunto el enlace para que pueda rellenar el formulario de la entrevista: <https://forms.gle/A2jgvKSkEZmpj5f7>

La información proporcionada será tratada con total confidencialidad y utilizada únicamente con fines académicos. Estoy segura de que su participación será de gran aporte para mi proyecto.

Agradezco de antemano su atención y quedo a la espera de su amable respuesta.

Saludos cordiales,



CARLOS ALBERTO CARRION MARQUEZ

para mí ▾

jue, 6 jun, 14:12 ☆ ↶ ⋮

Buenas tardes:

Ya envié el cuestionario cumplimentado. Gracias por la confianza.

Atentamente,

Ab. Carlos Carrión Márquez, Mgtr.
DOCENTE

Activar Windows
Ve a Configuración para activar Windows.

Entrevista para Proyecto Integrador Recibidos x



ESPERANZA FRANCESCA VERA BARBERAN

jue, 6 jun, 13:34

Estimado abogado Luis Quintero Angulo: Le saluda Esperanza Vera, estudiante de la carrera de Derecho en la Universidad de Ecotec. Tuve el honor de ser



QUINTERO ANGULO LUIS ALBERTO

jue, 6 jun, 19:20

Buenas noches, revisé el formulario y contesté las preguntas, espero le sean de ayuda. Cuidese y éxitos en su profesión. Atte., Abg. Luis Quintero Angulo



ESPERANZA FRANCESCA VERA BARBERAN <espvera@est.ecotec.edu.ec>

jue, 6 jun, 20:23 ☆ ↶

para QUINTERO ▾

Buenas noches Abogado,
Muchas gracias por su ayuda.

Saludos.

