UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y POLITICAS

CARRERA DE DERECHO

TEMA:

Phishing y su sanción en el sistema jurídico ecuatoriano.

AUTORA:

Furuki Hatta, Minori

Trabajo de titulación previo a la obtención del grado de ABOGADO DE LOS TRIBUNALES Y JUZGADOS DE LA REPUBLICA DEL ECUADOR

TUTOR:

Dr. Ycaza Mantilla, Andrés Mgs.

Guayaquil, Ecuador

6 de febrero del 2023

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES

Y POLITICAS

CARRERA DE DERECHO

CERTIFICACIÓN

Certificamos que el presente trabajo de titulación, fue realizado en su totalidad por **Furuki Hatta, Minori**, como requerimiento para la obtención del Título de **Abogado de los Tribunales y Juzgados de la República del Ecuador**.

TUTOR

f. _____

Dr. Ycaza Mantilla, Andrés Mgs.

DIRECTOR DE LA CARRERA

f. _____

Guayaquil, a los 6 días del mes de febrero del año 2023

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA CIENCIAS SOCIALES

Y POLITICAS

CARRERA DERECHO

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Furuki Hatta, Minori**

DECLARO QUE:

El Trabajo de Titulación: **Phishing y su sanción en el sistema jurídico ecuatoriano,** previo a la obtención del Título de **Abogado de los Tribunales y Juzgados de la República del Ecuador** ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, a los 6 días del mes de febrero del año 2023

LA AUTORA

f. _____

Furuki Hatta, Minori

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES

Y POLITICAS

CARRERA DE DERECHO

AUTORIZACIÓN

Yo, **Furuki Hatta, Minori**

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **Phishing y su sanción en el sistema jurídico ecuatoriano,** cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, a los 6 días del mes de febrero del año 2023

LA AUTORA:

f. _____

Furuki Hatta, Minori

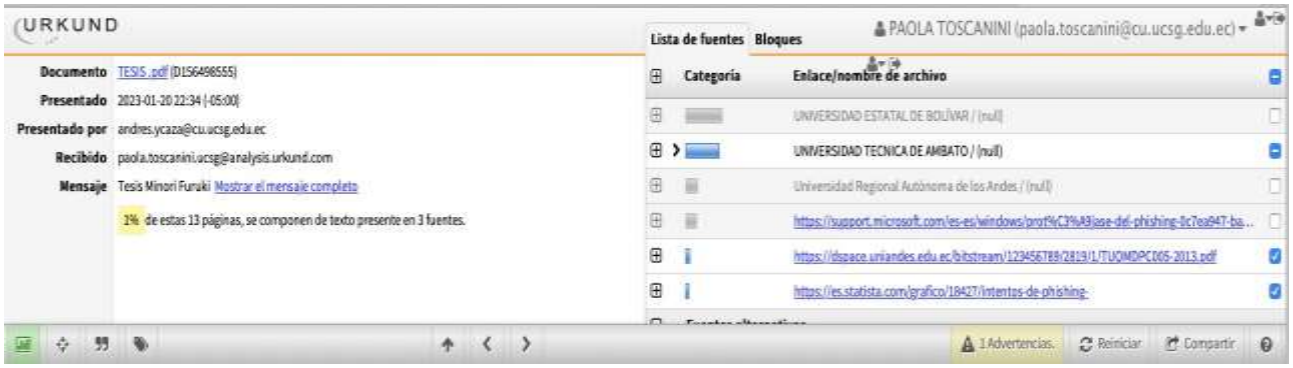
UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES

Y POLITICAS

CARRERA DE DERECHO

REPORTE DE URKUND



f. _____

Dr. Ycaza Mantilla, Andrés Mgs

Tutor

f. _____

Furuki Hatta, Minori

Autora

AGRADECIMIENTO

Quisiera agradecer a Dios y a mi familia por el apoyo que me han otorgado en todo el transcurso de la vida. Estoy muy agradecida también por las amistades y todas aquellas personas que siempre estuvieron ahí para aconsejarme y motivar a cumplir mis metas. Así mismo, estoy agradecida con mi tutor que me ha guiado a culminar el presente trabajo de investigación.

DEDICATORIA

El presente trabajo de investigación está dedicado primeramente a Dios, por permitirme tener a una familia maravillosa y poder disfrutar de cada detalle que la vida nos ofrece. A mi familia, por el apoyo y amor incondicional que siempre me han dado, todas las enseñanzas de la vida y los valores son gracias a mis padres y hermanos. Todo lo que soy y tengo el día de hoy es gracias a ellos.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES

Y POLITICAS

CARRERA DE DERECHO

TRIBUNAL DE SUSTENTACIÓN

f. _____

OPONENTE

f. _____

Dr. LEOPOLDO XAVIER ZAVALA EGAS DECANO

f. _____

Ab. MARITZA REYNOSO GAUTE, Mgs.

COORDINADOR DEL ÁREA

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

Facultad: **Jurisprudencia**

Carrera: **Derecho**

Periodo: **UTE B - 2022**

Fecha: **23 de enero de 2023**

ACTA DE INFORME FINAL

El abajo firmante, docente tutor del Trabajo de Titulación denominado **Phishing y su sanción en el sistema jurídico ecuatoriano,** elaborado por la estudiante ***FURUKI HATTA, MINORI*** certifica que durante el proceso de acompañamiento dicho estudiante ha obtenido la calificación de ***9 (NUEVE),*** lo cual lo califica como ***APTA PARA LA SUSTENTACIÓN.***

f. _____

Dr. Ycaza Mantilla, Andrés Mgs.

ÍNDICE

RESUMEN

La evolución de la tecnología en Ecuador ha sido gradual a lo largo de los años. En los últimos años, el país ha realizado esfuerzos para mejorar la infraestructura tecnológica y fomentar el desarrollo de nuevas industrias tecnológicas. Una de ellas ha sido implementar proyectos para mejorar la conectividad a internet, especialmente en áreas rurales. Así, el gobierno también ha implementado iniciativas para mejorar la infraestructura de internet para fomentar el desarrollo tecnológico en el país.

Sin embargo, todavía hay retos significativos como luchar contra los delitos informáticos. Los delitos informáticos son aquellas personas que utilizan la tecnología para cometer actividades ilícitas y se considera que es un problema mundial en donde las leyes debe actualizarse constantemente puesto que la tecnología es cada vez más innovador por la demanda.

En el presente trabajo de investigación, analizaremos sobre el phishing, uno de los delitos informáticos más comunes a nivel mundial. Examinaremos de qué manera podemos prevenirlo y si las leyes tipificadas en la ley ecuatoriana realmente sancionan a quienes cometen este delito.

Palabras claves: Phishing, Delito Informático, Tecnología, Internet, Ciberdelincuentes, Estafa

ABSTRACT

The evolution of technology in Ecuador has been gradual over the years. In recent years, the country has made efforts to improve technological infrastructure and encourage the development of new technological industries. One of them has been to implement projects to improve internet connectivity, especially in rural areas. Thus, the government has also implemented initiatives to improve the internet infrastructure to foster technological development in the country.

However, there are still significant challenges such as combating cybercrime. Computer crimes are those people who use technology to commit illegal activities and it is considered to be a global problem where laws must be constantly updated as technology is becoming more and more innovative due to the demand.

In this research paper, we will analyze phishing, one of the most common computer crimes worldwide. We will examine how we can prevent it and if the laws typified in the Ecuadorian law really punish those who commit this crime.

Keywords: Phishing, Computer Crime, Technology, Internet, Cybercriminals, Scam

INTRODUCCIÓN

La tecnología ha tenido un impacto significativo en la sociedad durante varios años. En la actualidad, observamos que la tecnología no sólo ha contribuido en la educación, salud o los servicios públicos, sino también ha facilitado el comercio y otras distintas áreas. Gracias a que la tecnología ha avanzado de una manera drástica nos ha facilitado más nuestras vidas. Por ello, muchos coincidimos que la tecnología definitivamente ha tenido un impacto positivo en la sociedad ya que al aumentar la productividad, nos permite realizar actividades en menos tiempo mejorando la calidad de nuestras vidas.

Así como hay aspectos positivos, también nos enfrentamos a ciertos aspectos negativos cuando hablamos sobre la tecnología. Los dispositivos tecnológicos, como los teléfonos móviles, las tabletas y las computadoras, ya forma parte de nuestras vidas puesto que nos permite trabajar, acceder a la información, comunicar con otras personas y entretenernos desde cualquier parte del mundo. Sin embargo, la dependencia de estos dispositivos puede tener efectos negativos. El problema se presenta cuando las personas hacen mal uso de la tecnología para cometer delitos informáticos. Cada vez son más las personas que han sido víctimas de estos delitos. Un correo electrónico o mensaje que a simple vista parece ser inofensivo nos puede perjudicar si no estamos atentos sobre las distintas formas de estafas que existen hoy en día.

Frente a estos sucesos, analizaremos de qué se trata el phishing, una modalidad de estafa que muchos se vieron afectados a lo largo de los años y que se ha descontrolado. Revisaremos si la legislación ecuatoriana es suficientemente precisa y penaliza el phishing o todavía existe un vacío

CAPITULO I

EL PHISHING

1.1 Definición de Phishing

La etimología de la palabra "phishing" tiene sus raíces en la palabra "fishing", que en inglés significa "pescando". Esta palabra se utiliza para describir la práctica de atrapar a las personas mediante técnicas engañosas, y se refiere al hecho de que los delincuentes cibernéticos están "pescando" información confidencial de las víctimas mediante el uso de correos electrónicos o mensajes de texto fraudulentos.

La palabra "phishing" es un término informático que se deriva de la frase "password fishing", que se refiere a la práctica de intentar atrapar a los usuarios para que compartan sus contraseñas o información personal mediante el uso de técnicas engañosas. Por lo general, se conoce como “phisher” a aquellas personas que cometen este delito.

En un principio fue utilizado como un juego de palabras para describir el atrapar algo, ya que el ataque se hacía mediante correos o mensajes que parecían "legítimos" pero eran trampas. Ahora se utiliza como un término general para describir cualquier intento de obtener información personal mediante engaño.

Algunas entidades bancarias del Ecuador define al phishing como una “modalidad de estafa que consiste en simular ser una persona, empresa o institución para que la víctima confíe y haga una acción, ya sea hacer clic en un enlace que lleva a una página falsa o responder el correo enviando información como usuarios, claves o información personal”.

“El phishing es un tipo de estafa, un fraude que se comete en internet, por medio de los diferentes canales de comunicación o por vía telefónica. En esta modalidad los atacantes, adoptan una falsa identidad, generalmente de alguna institución o empresa, con el objetivo de obtener las credenciales (usuarios y contraseñas) de tus cuentas personales o tarjetas de crédito”.

Microsoft, una de las empresas más dominantes en el mundo de la tecnología, define al phishing como “un ataque que intenta robar su dinero o su identidad, haciendo que divulgue información personal (como números de tarjeta de crédito, información bancaria o contraseñas) en sitios web que fingen ser sitios legítimos. Los ciberdelincuentes suelen fingir ser empresas prestigiosas, amigos o conocidos en un mensaje falso, que contiene un vínculo a un sitio web de phishing”.

Algunos de los tipos de phishing más comunes son: spear phishing, whaling y vishing. Cada uno tiene un enfoque y metodología diferente, pero todos buscan obtener información confidencial o financiera de las víctimas para luego delinquir.

- **Spear phishing:** es una forma altamente personalizada de phishing en la que los atacantes se enfocan en un objetivo específico y utilizan información recolectada previamente para engañar a la víctima y obtener información valiosa. Los ataques de spear phishing son generalmente dirigidos a individuos o a pequeñas empresas y suelen ser muy específicos en el objetivo.

- **Whaling:** es una forma de spear phishing específicamente dirigido a individuos de alto nivel dentro de una organización, como ejecutivos o miembros del consejo, con el objetivo de obtener información confidencial o financiera o causar daño a la organización.

- **Vishing (Voice Phishing):** es una técnica de phishing que se basa en llamadas telefónicas automatizadas o grabaciones de voz para engañar a las víctimas para que revele información personal o financiera, o que realice acciones no deseadas.

1.2 Objetivo del Phishing

El objetivo principal del phishing es obtener información confidencial como contraseñas, números de tarjeta de crédito, información bancaria, etc. Los ataques de phishing son muy sofisticados y se asemejan a correos electrónicos, mensajes de texto, sitios web, que parecen legítimos y provienen de instituciones confiables. Algunos ejemplos son:

- Robo de identidad: Los atacantes pueden utilizar la información obtenida para cometer fraudes o robar identidades, como abrir cuentas bancarias o solicitar créditos a nombre de la víctima.

- Fraude financiero: Los atacantes utilizan la información obtenida para realizar transacciones fraudulentas, como transferir dinero de las cuentas bancarias de la víctima o utilizar tarjetas de crédito robadas.

- Extorsión: Los atacantes amenazan a las víctimas con publicar o utilizar la información obtenida si no se paga ciertas sumas de dinero.

- Instalar malware: Los atacantes intentan instalar malware (*mal*icious soft*ware*), un software malicioso, en los dispositivos de las víctimas para robar información personal, espiar actividades de las víctimas, o generar ganancias mediante la venta de información obtenida.

- Acceso no autorizado a cuentas: los atacantes utilizan la información obtenida para acceder a cuentas de correo electrónico o bancarias no autorizadas.

En resumen, los atacantes que utilizan el phishing pueden obtener una variedad de beneficios económicos mediante la obtención de información personal o financiera de las víctimas, como robo de identidad, fraude financiero, extorsión, instalar malware, acceso no autorizado a cuentas, y entre muchos otros.

Fuente: (Esferize, 2022)

El phishing es una técnica que ha existido desde hace varios años. Los primeros casos del phishing ocurrieron en los años 90, cuando los delincuentes comenzaron a enviar correos electrónicos fraudulentos a los usuarios de AOL, una empresa de servicios de internet, pidiéndoles que proporcionaran información personal, como sus contraseñas y números de tarjetas de crédito. A medida que la tecnología desarrolló, los delincuentes cibernéticos han empleado técnicas más sofisticadas para crear correos electrónicos y sitios web fraudulentos que parezcan legítimos.

Es importante tener en cuenta que el phishing se ha convertido en una de las principales amenazas de seguridad hoy en día. El ciberseguridad es una de las principales preocupaciones de las organizaciones y de los propios trabajadores ya que al haber más usuarios usando el internet o redes sociales, aumentan los riesgos cibernéticos, dando lugar a reforzar la protección contra estas amenazas. Por ello, debemos conocer sobre estas tendencias utilizadas por los delincuentes cibernéticos para protegernos contra el phishing.

1.3 Método del Phishing

El método de phishing se basa en la creación de una experiencia engañosa para hacer creer al usuario que el contenido o la página web que se encuentran es confiable y así poder solicitar información personal o financiera. Los métodos utilizados en el phishing puede variar dependiendo del tipo de phishing y del objetivo del atacante. Algunos de los métodos más comunes de phishing son:

Correo electrónico

- Los ciberdelincuentes envían correos electrónicos fraudulentos que se hacen pasar por empresas o instituciones conocidas y solicitan información personal o financiera.

Sitios web

- Crean sitios web falsos que se hacen pasar por sitios web legítimos de empresas o instituciones conocidas y solicitan información personal o financiera.

Llamadas telefónicas:

- Hacen llamadas telefónicas fraudulentas que se hacen pasar por empresas o instituciones conocidas y solicitan información personal o financiera.

Mensajes de texto

- Envían mensajes de texto fraudulentos que se hacen pasar por empresas o instituciones conocidas y solicitan información personal o financiera.

Mensajería instantánea

- Utilizan plataformas de mensajería instantánea para engañar a las personas y obtener información personal o financiera.

El proceso de phishing generalmente funciona de la siguiente manera:

1. El ciberdelincuente envía el mensaje engañoso a un gran número de personas, con la esperanza de que algunas de ellas caigan en el engaño y proporcionen información personal o financiera.

2. El destinatario del mensaje engañoso, cree que es de una empresa o institución de confianza y proporciona información personal o financiera, como contraseñas, números de tarjetas de crédito, información bancaria, entre otros.

3. Una vez que el ciberdelincuente tiene acceso a la información personal o financiera, puede utilizarla para sus propios fines maliciosos, como realizar transacciones fraudulentas, robar dinero de las cuentas bancarias, o vender la información en el mercado negro.

Es importante conocer sobre estos tipos de delitos que existe hoy en día y estar alertas ante posibles intentos de phishing. Las tácticas utilizadas en el phishing son cada vez más creíbles, por lo que debemos estar muy pendientes y saber distinguir si son de entes confiables para no caer en las trampas.

Fuente: (Esferize, 2022)

1.4 Determinar si es Phishing

Hay varios pasos que podemos seguir para determinar si un correo electrónico o sitio web es un intento de phishing:

1. **Observar el remitente:** Si el correo electrónico es de un remitente desconocido, es posible que sea un intento de phishing.

2. **Revisar los enlaces:** Si el correo electrónico contiene enlaces, es importante asegurarnos de que esté dirigiendo a sitios web legítimos. Se recomienda copiar el enlace y luego, pegarlo en una ventana del navegador para verificar si el sitio web es confiable.

3. **Buscar errores de ortografía y gramática:** Los correos electrónicos de phishing a menudo contienen errores de ortografía y gramática. Estos correos pueden venir de personas que no hablan el idioma del destinatario con fluidez, por lo que puede tener errores gramaticales.

4. **Buscar alerta de phishing:** En la actualidad existen varias compañías de seguridad informática, empresas de correo electrónico y organizaciones gubernamentales que alertan para ayudar a los usuarios a identificar y evitar intentos de phishing.

En caso de tener alguna sospecha de phishing, es importante no responder al correo electrónico y se recomienda evitar abrir correos de remitentes desconocidos y eliminar de la bandeja de entrada. Debemos recordar que no se debe proporcionar información personal o financiera a través de correo electrónico o en un sitio web cuando hay sospechas de que es un intento de phishing. Tener un buen software de seguridad en el dispositivo y mantenerlo actualizado es unas de las formas para prevenir caer en el phishing. Si uno es víctima de un intento de phishing, se debe cambiar inmediatamente todas las contraseñas y alertar a las instituciones financieras y cualquier otra institución relacionada con la información que haya sido comprometida.

1.5 El Phishing en otros países

El phishing es un problema global y puede afectar a personas en cualquier parte del mundo. Sin embargo, algunos países pueden ser más propensos a los ataques de phishing debido a ciertos factores como la penetración de la tecnología, la regulación y la educación sobre la seguridad en línea. El phishing ha aumentado significativamente en los últimos años debido a varias razones. Una de ellas es el aumento del uso de internet y las redes sociales. Los avances de la tecnología es impresionante. Podemos observar que al igual que la tecnología ha evolucionado, los ciberdelincuentes también están desarrollando nuevas técnicas para engañar a las personas.

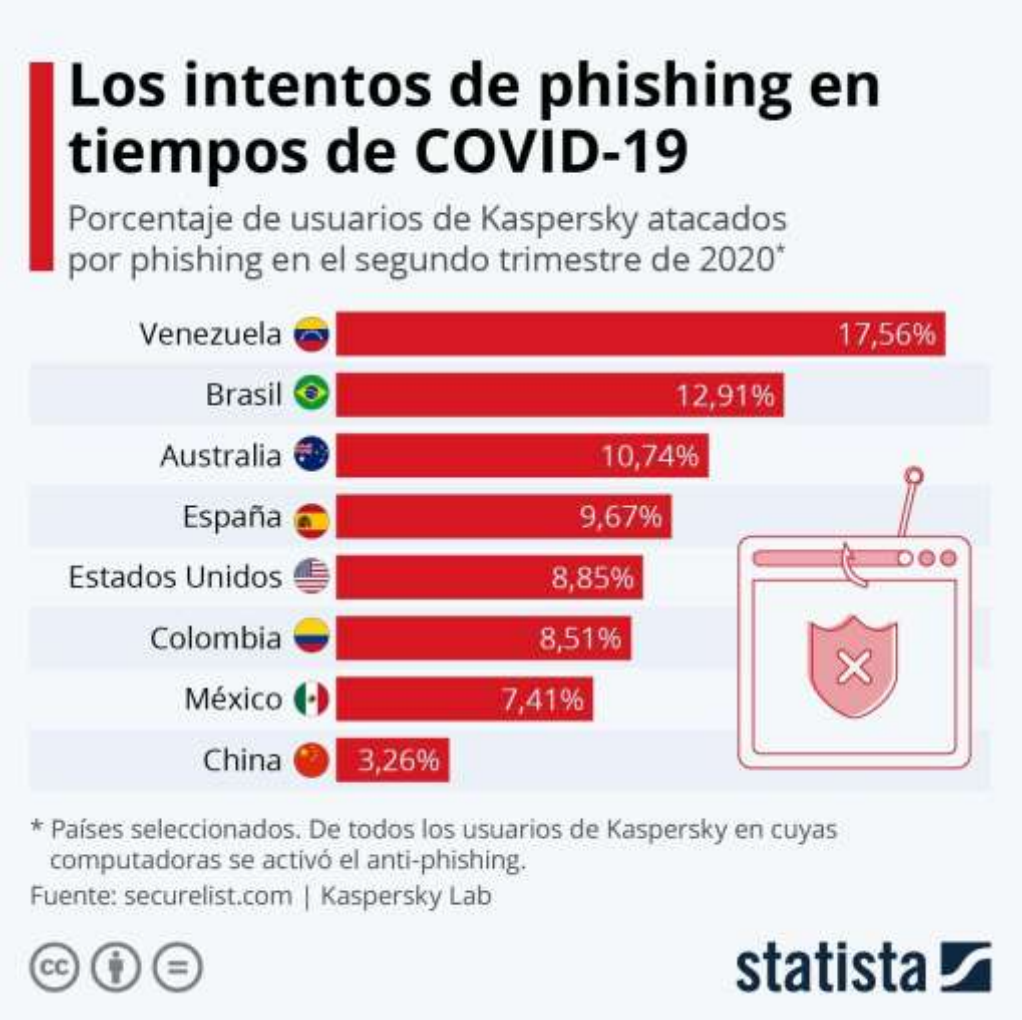
Según algunas investigaciones, los países más afectados por el phishing son Estados Unidos, China, India, Brasil, Rusia, entre otros. Cabe señalar que esto puede variar a medida que los ciberdelincuentes buscan nuevos blancos y se adaptan a las medidas de seguridad en diferentes países. Es importante mencionar que el phishing no sólo ataca a los entes sino también busca afectar a organizaciones y empresas grandes o pequeñas de cualquier parte del mundo. Las empresas grandes se ven obligados a actualizar su seguridad constantemente puesto que los ciberdelincuentes utilizan diversas técnicas para obtener y robar información confidencial o monetizar la información obtenida.

Muchos recordamos que en la pandemia de COVID-19, existían restricciones y hubo el aumento de uso de la tecnología para trabajar desde casa o recibir clases a través de plataformas online. En la pandemia también se ha generado una gran cantidad de información y noticias relacionadas con el COVID-19, incluyendo información sobre el estado de la salud, los protocolos de seguridad, las medidas de emergencia, las vacunas, etc.

Nuestro medio de comunicación básicamente fue por medio de estos dispositivos tecnológicos y fue de esta manera, que los ciberdelincuentes se aprovecharon para crear correos electrónicos y sitios web fraudulentos que se asemejan a los de empresas o instituciones confiables para cometer el delito de

phishing y muchos otros delitos más. La pandemia de COVID-19 definitivamente fue un gran impacto no sólo en la economía del mundo, sino por el gran aumento de casos de phishing, ya que los ciberdelincuentes se han aprovechado del miedo y las preocupaciones de las personas por la situación.

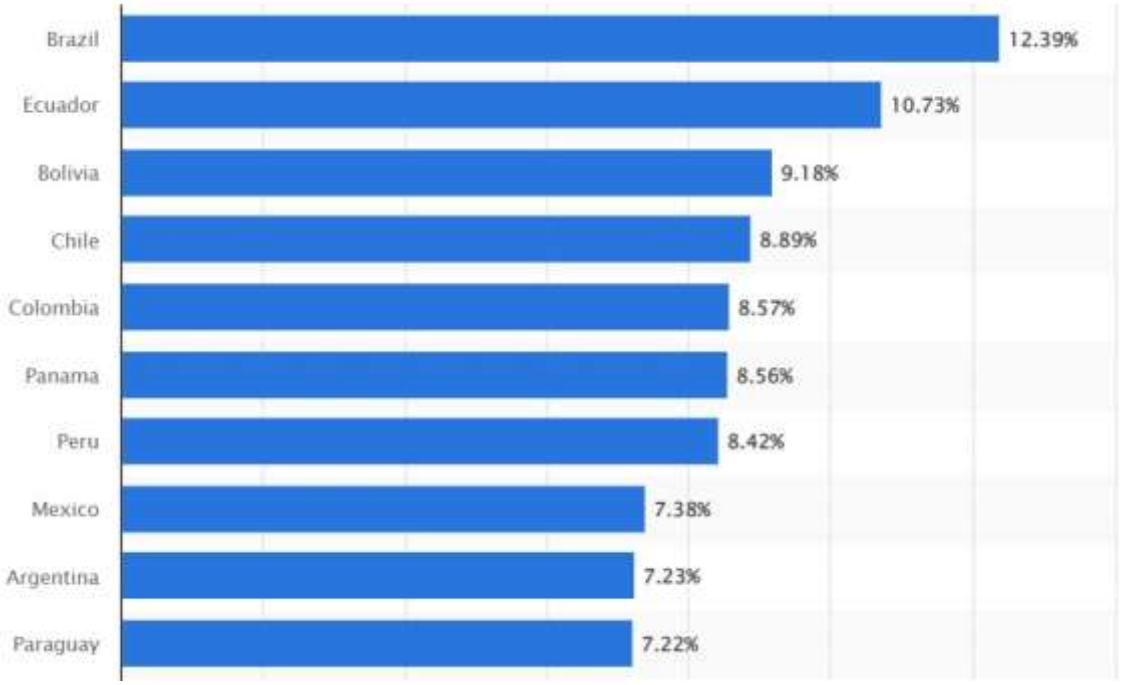
En el segundo trimestre del 2020, observamos que hubo un aumento de intento de phishing. De acuerdo a Statista, un portal de estadísticas de mercado, los países más afectados en tiempos de COVID-19 fueron Venezuela, Brasil y Australia.



Fuente: (Statista, 2020)

Mientras que, los países de América Latina y el Caribe más afectados por los ataques de phishing en el año 2021 fueron Brasil, Ecuador y Bolivia. Es sorprendente que Ecuador se encuentra en el

segundo país de América Latina con mayores ataques de phishing. Muchos hemos escuchado de amigos cercanos, familiares o conocidos que durante la pandemia han sido víctimas de este método.



Dmitry Bestuzhev, director del Equipo de Investigación y Análisis de Kaspersky para América Latina, señala que los ataques cibernéticos en Latinoamérica han aumentado un 24% en lo que va de año en comparación con los primeros 8 meses de 2020. El crecimiento de los ciberataques se refleja en todos los países de la región, con la excepción de Costa Rica.

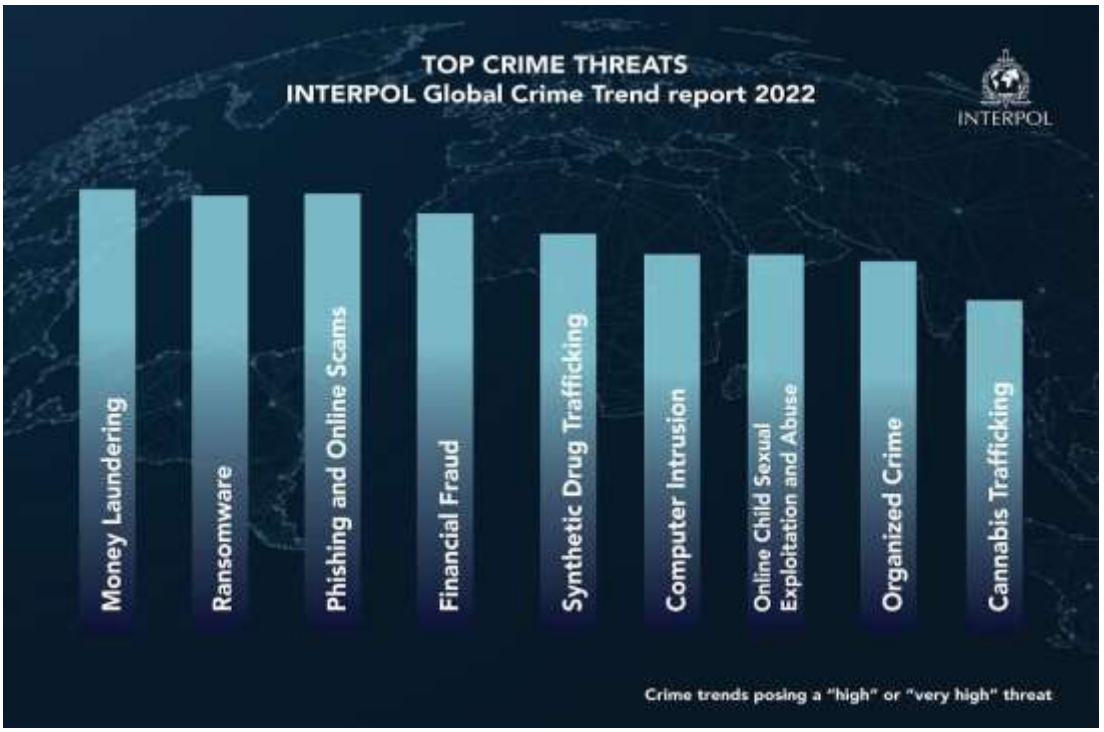
Bestuzhev sostiene que, lamentablemente, "los internautas latinoamericanos le abren la puerta a las ciberamenazas a través de programas piratas, permitiendo que los cibercriminales obtengan control total de los dispositivos infectados". Es por ello que Ecuador es el primer país más afectado con un alza del 75%, seguido por Perú (+71%), Panamá (+60%), Guatemala (+43%) y Venezuela (+29 %).

“Un 44% de las empresas declara haber sido víctima de algún ataque a sus sistemas informáticos; sin embargo, sólo el 17% de los profesionales es consciente de ello. Por tipo de empresa, las medianas y grandes son las más atacadas, ya que el 56% afirma haber recibido algún ciberataque en el

último año”. (itreseller, 2021)

Un comunicado publicado por la INTEROL en octubre del 2022, indica que los delitos financieros y los cometidos por internet son los que más preocupan a la policía de todo el mundo.

El Secretario General de la INTERPOL sostiene su preocupación: “Entender las tendencias de la delincuencia y anticiparse a ellas es un fundamento básico de la labor policial, y el informe de INTERPOL sobre las tendencias de la delincuencia a escala mundial ofrece una imagen única de la situación tal y como la ven los funcionarios policiales de todo el mundo”. (Jürgen Stock, 2022)



Fuente: (INTERPOL, 2022)

La división de Inteligencia de Amenazas de Check Point, ha publicado un reporte de phishing del año 2022 (enero-marzo) en el cual nos muestra cuáles han sido las marcas que los ciberdelincuentes suplantaron para intentar robar información personal o credenciales de pago. De acuerdo a las estadísticas, podemos observar que LinkedIn, una red social que permite que los usuarios puedan crear perfiles

para así incrementar los contactos con otros profesionales y buscar empleos, fueron los más afectados con intentos de phishing durante el primer trimestre del 2022. Se cree que la causa principal fue la pandemia, puesto que el número de desempleos aumentó drásticamente y así como muchos usuarios crearon perfiles en busca de empleos, los ciberdelincuentes también se aprovecharon de dicha situación para cometer delitos.

Según el Reporte de Defensa Digital de Microsoft 2022, los esquemas de phishing de credenciales están en aumento y se mantienen como una amenaza importante para los usuarios en todas partes. Se considera que el phishing es el método de ataque preferido por los ciberdelincuentes ya que pueden adquirir un valor significativo al robar y vender con éxito el acceso a cuentas robadas.

CAPITULO II

EL PHISHING EN ECUADOR

2.1 Seguridad Cibernética en Ecuador

Ecuador ha experimentado un crecimiento en el sector de tecnología en los últimos años. Existen varias empresas de tecnología en el país que ofrecen servicios y soluciones a clientes locales e internacionales. Además, se ha desarrollado una industria emergente de tecnologías de la información y comunicación (TIC), y el gobierno ha implementado iniciativas para mejorar la infraestructura de internet y promover el desarrollo de habilidades en TIC. También existen varias universidades y escuelas en Ecuador que ofrecen programas educativos en tecnología. Sin embargo, todavía hay retos significativos para el desarrollo de la tecnología en el país, como la falta de inversión y la ausencia de recursos.

ESET, una compañía de software especializada en ciberseguridad, señala que el Ecuador se encuentra entre los 10 países de América Latina más afectados por software malicioso (Informe anual de esta firma; Security Report Latinoamérica 2020).

De acuerdo al Índice Global de Ciberseguridad (GCI), publicado el 9 de julio del 2019, Ecuador se encuentra en el puesto 98 de 193 países, esto significa que no contamos con la suficiente seguridad cibernética y que somos vulnerables ante las amenazas cibernéticas a nivel mundial. Kaspersky Lab, una compañía internacional dedicada a la seguridad informática, sostuvo que en el reporte realizado en el 2020, Ecuador se encontraba en el puesto número 89 de los países que más han recibido ataques cibernéticos en el mundo.

Fuente: (Índice Global de Ciberseguridad, 2019)

En un artículo publicado el 11 de enero de 2022 del diario El Comercio, informa que por la pandemia, la posibilidad de sufrir un ciberataque ha aumentado y que en el Ecuador los ciberdelincuentes operan de las siguientes 4 formas:

- **Phishing:** los usuarios proporcionan datos personales o contraseñas a través de enlaces. De esta manera, los ciberdelincuentes acceden a las cuentas bancarias y sustraen el dinero.

- **Infectar computadoras y celulares:** el virus informático roba datos personales o bancarios a través de enlaces maliciosos.

- **Crear sitios web fraudulentos o plataformas de comercio electrónico:** se comercializa diversos productos, el comprador realiza el pago por medio de transferencia bancaria, pero nunca recibe el pedido.

- **Hackear cuentas de redes sociales:** para sustraer la identidad de las víctimas y pedir dinero a sus familiares o amigos cercanos.

2.2 Acceso al Internet en Ecuador

En el Art. Art. 39 del COIP (Código Orgánico Integral Penal) indica sobre el acceso al conocimiento libre y seguro en entornos digitales e informáticos, señalando que el acceso universal, libre y seguro al conocimiento en entornos digitales es un derecho de los ciudadanos. El Estado generará las condiciones necesarias para garantizar progresivamente la universalización del acceso a las tecnologías de la información y comunicación, priorizando el uso de tecnologías libres, bajo los principios de: soberanía tecnológica, seguridad, neutralidad de la red, acceso libre y sin restricciones a la información y precautelando la privacidad. Estas condiciones serán respetadas sin perjuicio del proveedor del servicio. Los organismos de control competente vigilarán que se cumplan con estas condiciones.

En el Art. 40 del Código Orgánico de la Economía Social de los Conocimientos habla sobre el acceso a internet: “El Estado garantizará el acceso universal al servicio público de internet en los términos previstos en la Constitución de la República. Los organismos competentes vigilarán que el precio de este servicio sea equitativo, y establecerán los mecanismos de control y regulación correspondientes. Las universidades y escuelas politécnicas deberán poner a disposición acceso a internet inalámbrico libre y gratuito en toda el área de sus sedes y extensiones. Los gobiernos autónomos descentralizados deberán poner a disposición libre y gratuita de la ciudadanía, acceso a internet inalámbrico en los espacios públicos de concurrencia masiva destinados al ocio y entretenimiento, de acuerdo a las condiciones que establezca el reglamento correspondiente”.

En la encuesta realizada por el Instituto Nacional de Estadísticas y Censos (INEC) en el 2019, se evidencia que en los últimos años hubo un incremento en los hogares con acceso al internet. A nivel nacional, los hogares que tuvieron acceso a internet fue de 45.5% en donde los niños,

niñas y adolescentes entre 5 y 17 años son quienes utilizan el internet en su mayor parte desde su hogar con un 64.5%. El acceso a la tecnología tiene muchos aspectos positivos, sin embargo, la exposición al mundo digital sin medidas de seguridad, puede implicar muchos riesgos, en particular, para niños, niñas y adolescentes.

El MINTEL (Ministerio de Telecomunicaciones y de la Sociedad de la Información), a través de la Subsecretaría de Fomento de la Sociedad de la Información y Economía Digital, desarrolló la Agenda de Transformación Digital del Ecuador 2022 - 2025, aprobada y publicada mediante Acuerdo Ministerial en el Registro Oficial Nº 198 el Lunes 28 de noviembre de 2022.

La formulación de la Política para la Transformación Digital está liderada por el MINTEL en el cual su enfoque es promover el uso efectivo y seguro de las tecnologías de la información y comunicación brindando grandes oportunidades para una mejor calidad de vida y para la innovación, el crecimiento económico y la sostenibilidad. De acuerdo a los estudios, se reportaron 15,639 puntos wifi, distribuidos en 126 cantones, hasta el mes de julio del 2022, esto significa que el 57% de los cantones cuentan con puntos wifi instalados, lo cual ha permitido incrementar el acceso al servicio de internet de la población

Tema	Categoría	Tipo de Equipamiento	Porcentaje
	Porcentaje de personas que tienen celular activado y teléfono inteligente, hombres	Celular Activado	65,20%
		Smartphone	80,50%
	Porcentaje de personas que tienen celular activado y teléfono inteligente, mujeres	Celular Activado	60,70%
		Smartphone	83,20%

Fuente: (MINTEL, 2021)

2.3 Legislación Ecuatoriana

En el Ecuador, los delitos informáticos son sancionados desde el 2009. Antonio Perez Luño, en su libro Manual de Informática y Derecho define al delito informático como “aquel conjunto de conductas criminales que se realizan a través del ordenador electrónico o que afectan al funcionamiento de los sistemas informáticos”.

Rodrigo Rivera-Morales, en su libro Los Medios Informáticos: Tratamiento Procesal sostiene que “Los medios informáticos, en la mayoría de legislaciones, no se encuentran regulados en forma expresa dentro de las normas procesales”. En el artículo 5 numeral 1 del COIP menciona sobre el Principio de Legalidad: no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho.

En nuestro país, se considera que el phishing es un delito informático y se cree que está regulado por el COIP. En las noticias de Ecuador informan que el delito de phishing tiene una pena de 3 a 5 años de prisión. En las siguientes líneas, analizaremos si en la ley ecuatoriana se encuentra tipificado el phishing como un delito.

Es importante mencionar que en el artículo 75, numeral 3 de la Consitución de la República del Ecuador indica: “Nadie podrá ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no esté tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio de cada procedimiento”.

Revisando los artículos 186, 212, 232 y 234 del COIP, obervamos que en ninguno de los artículos utiliza el término “phishing”. Al leer algunas demandas relacionado a este delito, nos damos cuenta que en nuestra

legislación, la figura del “phishing” se asemeja más a la suplantación de identidad y estafa. En el Art. 212 del COIP define a la suplantación de identidad como “la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años”.

Art. 186 (COIP).- Estafa.- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir
información de tarjetas de crédito, débito, pago o similares.
3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.
4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor.
6. A través de una compañía de origen ficticio, induzca a error a otra persona, con el fin de realizar un acto que perjudique su patrimonio o el de un tercero.

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años. Al revisar los artículos del COIP sobre los ciberataques, notamos que la legislación ecuatoriana, no tiene una ley clara en donde especifica el delito de phishing como tal.

En la Ley Orgánica Reformatoria del Código Orgánico Integral Penal para Prevenir y Combatir la Violencia Sexual Digital y Fortalecer la Lucha contra los Delitos Informáticos publicado el 30 de agosto del 2021 menciona que en los artículos 230, 232 y 234 del COIP debe sustituirse.

En los artículos se especifica que la persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento o comportamiento no deseado, o suprima total o parcialmente contenido digital, sistemas informáticos, etc. será sancionada con pena privativa de libertad de 3 a 5 años. La pena será sancionada con igual a la persona que diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos, programas o sistemas informáticos maliciosos o destinados a causar los efectos señalados anteriormente. También menciona que la misma sanción debe aplicarse la persona que introduce, modifica, elimina o suprime contenido digital o interfiere de cualquier otra forma en el tratamiento informático de datos.

Cabe recalcar que en el Ecuador, ninguna de las leyes son claras cuando se trata del delito de phishing y podemos entender que no existe una norma como tal que sancione este delito. Si con el transcurso de los años hemos visto que este tipo de delitos aumentaron signifcativamente, es sumamente importante que el delito esté tipificado claramente en la ley.

Hemos observado que gran parte de la población ecuatoriana tiene acceso al internet y cuentan con algún dispositivo electrónico. A pesar de que la tecnología nos ha aportado bastante y ha mejorado la calidad de nuestras vidas, la realidad es que aún hay muchas personas que desconocen el peligro que puede tener el mundo del internet. Es importante estar siempre alerta e informarnos constantemente de las estrategias que cometen los ciberdelincuentes en el phishing. La mejor prevención contra el phishing es educarnos y ser precavido en todo momento.

CONCLUSIONES

- El internet ha facilitado muchas cosas en nuestra vida, ya sea para comunicarnos, acceder a informaciones, trabajar desde cualquier parte del mundo y ha aportado bastante en el comercio y la educación. En Ecuador se ha hecho esfuerzos para mejorar su infraestructura tecnológica y fomentar el desarrollo de nuevas industrias tecnológicas. En las últimas décadas, la tecnología ha avanzado de una manera sorprendente y se cree que seguirá evolucioando. Seguramente existirán desafíos y áreas en las que se debe mejorar para que se controle en lo mejor posible los delitos como el phishing. Es necesario que el país invierta en la investigación, desarrollo y seguridad con respecto a este tema. Los ciberdelincuentes siempre estarán en busca de países vulnerables que no tienen medidas que proteja contra los ciberataques.

- En el presente trabajo de investigación se puede concluir que en la legislación ecuatoriana, no cumple con el objetivo de sancionar el delito de phishing. Hemos revisado que existe algunas clases de phishing y la modalidad es diferente para cada uno. Para frenar este delito no va a ser una tarea sencilla y requerirá de algunos años poder combatir, pero se puede tratar de minimizar el número de víctimas si las leyes son más claros para así poder sancionar a los delincuentes. En muchos casos las personas no denuncian a las autoridades competentes cuando caen en este tipo de delito. Es importante alertar y denunciar este tipo de delito para que otros no caigan en lo mismo.

- Así como la tecnología seguirá innovando, las leyes también debe actualizarse para penalizar quienes cometen ciberataques. El internet y la tecnología es una herramienta muy poderosa y favorable cuando se utiliza de manera responsable y consciente. A pesar de que en la

legislación ecuatoriana no existen leyes adecuadas para sancionar el phishing, podemos comenzar tomando las medidas preventivas necesarias, informándonos de los delitos relacionados al mundo de la tecnología y estar pendiente de todo.

RECOMENDACIONES

Tenemos claro que el phishing es una técnica utilizada por los delincuentes cibernéticos para obtener información confidencial, haciendo uso de correos electrónicos, mensajes de texto fraudulentos, enlaces, entre otros. Por más que se mejore la seguridad cibernética, los ciberdelincuentes buscarán siempre la manera para delinquir. Un experto en seguridad informática sostuvo “Si Ud. piensa que la tecnología puede resolver sus problemas de seguridad, entonces Ud. no entiende los problemas de seguridad y tampoco entiende la tecnología”. (Schneier, 2004). Tener un software o contratar un servicio de seguridad para proteger los sistemas informáticos, redes y datos contra ataques maliciosos, no nos asegura al 100% que jamás seremos víctimas del phishing u otros delitos similares.

Al revisar la legislación de nuestro país pudimos observar que hay muchas leyes que no está detallado y hay un vacío con este tipo de delitos. Para que el phishing sea calificado como un delito, debe estar tipificado en la ley tal como lo indica el principio de legalidad (Nullum Crimen Nulla Poena Sine Lege). La legislación actual sanciona a aquellas personas que cometen el delito de suplantación de identidad, robo de información, estafas, etc. pero no se usa el término “phishing”. Considero que es importante que en la ley estén tipificado las ditintas clases de phishing y otros delitos informáticos para así poder sancionar a aquellas personas que han cometido este delito.

En la actualidad no existe una legislación penal adecuada con respecto al pishing pero debemos hacer el esfuerzo para controlar y frenar este delito. Muchos se vieron afectados más en pandemia por es uso masivo de los dispositivos tecnológicos. Para que delitos como el phishing no quede en la impunidad, es necesario que en la ley esté escrito detalladamente estos delitos y así tomar medidas preventivas para evitar que este tipo de delitos aumenten.

REFERENCIAS

Altmark. (2012). Tratado de Derecho Informático, Tomo lll

Rivera-Morales, R. (2008). Los Medios Informáticos: Tratamiento Social

Acurio del Pino, S. (2009). Perfil sobre los Delitos Informáticos en el Ecuador

Perez, L. (1996). Manual de Informática y Derecho

Constitución de la República del Ecuador. (2008). Registro Oficial suplemento 449 de 20-octubre-2008.

Código Orgánico Integral Penal. (2014). Registro Oficial sumplemento No. 180 de 10-febrero-2014.

Código Orgánico de la Economía Social de los Conocimientos. (2016). Registro Oficial suplemento 899 de 9-diciembre-2016.

INEC Tecnologías de la Información y Comunicación, 2020. (2020). https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2020/202012_Principales_resultados_Multiproposito_TIC.pdf

Acuerdo Nro. MINTEL-MINTEL-2022-0031 Registro Oficial Nº 198 Lunes 28 de noviembre de 2022. (2022). http://www.edicioneslegales-informacionadicional.com/webmaster/directorio/RO198_2022.pdf

ESET. (2020). Security Report Latinoamerica 2020 https://security-report.eset-la.com/

Statista. (2022). https://es.statista.com/grafico/18427/intentos-de-phishing-durante-la-pandemia/

Esferize. (2022). https://www.esferize.com/

INTERPOL. (2022). https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2022/Los-delitos-financieros-y-los-cometidos-por-Internet-son-los-que-mas-preocupan-a-la-policia-de-todo-el-mundo-segun-un-nuevo-informe-de-INTERPOL

El Comercio. (2023). Ciberdelincuentes operan de cuatro formas en El Ecuador. https://www.elcomercio.com/actualidad/seguridad/Ciberdelincuencia-Ecuador-organizaciones-delictivas-victimas.html

Ecuavisa. (2023). "Trabajos" en Amazon o Mercado Libre, la nueva modalidad de estafa en Ecuador. https://www.ecuavisa.com/noticias/seguridad/estafa-ciberdelitos-whatsapp-ecuador-YA4156450

El Comercio. (2022). 3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020. https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

El Universo. (2022). Alerta con lo que le depositan como décimo o bonificaciones que los ciberdelincuentes están activados en diciembre en Ecuador: bancos hacen advertencias. https://www.eluniverso.com/noticias/informes/alerta-con-lo-que-le-depositan-como-decimo-o-bonificaciones-que-los-ciberdelincuentes-estan-activados-en-diciembre-en-ecuador-bancos-hacen-advertencias-nota/

Infobae. (2021). Los ciberataques en Latinoamérica han aumentado un 24 % este año. https://www.infobae.com/america/agencias/2021/08/31/los-ciberataques-en-latinoamerica-han-aumentado-un-24-este-ano/

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Furuki Hatta, Minori** con C.C: # 0916482185 autora del trabajo de titulación: **Phishing y su sanción en el sistema jurídico ecuatoriano,** previo a la obtención del título de **Abogado de los Tribunales y Juzgados de la República del Ecuador** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 6 de febrero del 2023

f. _____

Nombre: **Furuki Hatta, Minori**

C.C: **0916482185**

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Phishing y su sanción en el sistema jurídico ecuatoriano.		
AUTORA	Furuki Hatta Minori		
TUTOR	Dr. Ycaza Mantilla Andrés Patricio Mgs.		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Facultad de Jurisprudencia, Ciencias Sociales y Políticas		
CARRERA:	Carrera de Derecho		
TITULO OBTENIDO:	Abogado de los Tribunales y Juzgados de la República del		
FECHA DE PUBLICACIÓN:	6 de febrero del 2023	**No. DE PÁGINAS:**	27
ÁREAS TEMÁTICAS:	Derecho Informático, Legislación Ecuatoriana, Seguridad Jurídica		
PALABRAS CLAVES/ KEYWORDS:	Phishing, Delito Informático, Tecnología, Internet, Ciberdelincuentes, Estafa		

RESUMEN:

La evolución de la tecnología en Ecuador ha sido gradual a lo largo de los años. En los últimos años, el país ha realizado esfuerzos para mejorar la infraestructura tecnológica y fomentar el desarrollo de nuevas industrias tecnológicas. Una de ellas ha sido implementar proyectos para mejorar la conectividad a internet, especialmente en áreas rurales. Así, el gobierno también ha implementado iniciativas para mejorar la infraestructura de internet para fomentar el desarrollo tecnológico en el país. Sin embargo, todavía hay retos significativos como luchar contra los delitos informáticos. Los delitos informáticos son aquellas personas que utilizan la tecnología para cometer actividades ilícitas y se considera que es un problema mundial en donde las leyes debe actualizarse constantemente puesto que la tecnología es cada vez más innovador por la demanda. En el presente trabajo de investigación, analizaremos sobre el phishing, uno de los delitos informáticos más comunes a nivel mundial. Examinaremos de qué manera podemos prevenirlo y si las leyes tipificadas en la ley ecuatoriana realmente sancionan a quienes cometen este delito.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:**+593-4-2222024	E-mail: minori.furuki@cu.ucsg.edu.ec
CONTACTO CON LA INSTITUCIÓN (COORDINADOR DEL PROCESO UTE):	Nombre: Reynoso Gaute, Maritza	
	Teléfono: +593-4-2222024	
	E-mail: maritza.reynoso@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	