UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y SALUD
CARRERA DE DERECHO

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADOS

TÍTULO:

EL PHISHING COMO DELITO INFORMÁTICO EN EL ÁMBITO DE LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y ESPAÑA, 2023

AUTORES:

SUÁREZ LIRIANO DAVID EMANUEL

ROCAFUERTE DEL PEZO ERNESTO RUBÉN

TUTORES:

DR. CRISTÓBAL MACHUCA REYES, MGT

ING. BOLÍVAR SUÁREZ LINDAO

LA LIBERTAD – ECUADOR

2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE CIENCIAS SOCIALES Y SALUD
CARRERA DE DERECHO

TRABAJO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADOS

TÍTULO:

EL PHISHING COMO DELITO INFORMÁTICO EN EL ÁMBITO DE LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y ESPAÑA, 2023

AUTORES:
SUÁREZ LIRIANO DAVID EMANUEL
ROCAFUERTE DEL PEZO ERNESTO RUBÉN

TUTORES:
DR. CRISTÓBAL MACHUCA REYES, MGT
ING. BOLÍVAR SUÁREZ LINDAO

LA LIBERTAD – ECUADOR
2024

La Libertad, junio de 2024

APROBACIÓN DEL TUTOR

CERTIFICAMOS

Que hemos analizado el trabajo de integración curricular con el título **"EL PHISHING COMO DELITO INFORMÁTICO EN EL ÁMBITO DE LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y ESPAÑA, 2023"** presentado por los estudiantes **SUÁREZ LIRIANO DAVID EMANUEL Y ROCAFUERTE DEL PEZO ERNESTO RUBÉN,** portadores de las cédulas de ciudadanía Nº 0928231299 y Nº 0928279173 respectivamente, como requisito previo a optar el título de **ABOGADOS**, y declaramos que luego de haber orientado científica y metodológicamente su desarrollo, el referido proyecto de investigación se encuentra concluido en todas sus partes cumpliendo así con el proceso de acompañamiento determinado en la normativa interna, recomendando se inicien los procesos de evaluación que corresponden.

Atentamente

CRISTOBAL HOMERO MACHUCA REYES
Firmado digitalmente por CRISTOBAL HOMERO MACHUCA REYES

Dr. Cristóbal Machuca Reyes, Mgt.
TUTOR

Ing. Bolívar Suárez Lindao
TUTOR

La Libertad, junio de 2024

CERTIFICACIÓN DE ANTIPLAGIO

En mi calidad de Tutor del Trabajo de Integración Curricular: **"EL PHISHING COMO DELITO INFORMÁTICO EN EL ÁMBITO DE LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y ESPAÑA, 2023"**, correspondiente a los estudiantes **SUÁREZ LIRIANO DAVID EMANUEL Y ROCAFUERTE DEL PEZO ERNESTO RUBÉN**, de la Carrera de Derecho, **CERTIFICO**, que el contenido de dicho trabajo ha sido sometido a la validación en sistema anti plagio COMPILATIO, obteniendo un porcentaje de similitud del 7%, cumpliendo así con los parámetros técnicos requeridos para este tipo de trabajos académicos.

Atentamente

CRISTOBAL HOMERO MACHUCA REYES

Firmado digitalmente por CRISTOBAL HOMERO MACHUCA REYES

Dr. Cristóbal Machuca Reyes, Mgt
TUTOR

VALIDACIÓN GRAMATICAL Y ORTOGRÁFICA

CERTIFICACIÓN DE GRAMATOLOGÍA

Yo Narcisa Josefina Yagual Tumbaco, con C.I. 0907952147, Master Universitario en Formación Internacional especializada del profesorado especialidad en orientación educativa con registro SENESCYT No. 7241104695, por medio del presente CERTIFICO que he revisado la redacción, estilo y ortografía del presente trabajo investigativo elaborado por:

SUÁREZ LIRIANO DAVID EMANUEL **CC. 0928231299**
ROCAFUERTE DEL PEZO ERNESTO RÚBEN **CC. 0928279173**

PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADOS del tema denominado:

"EL PHISHING COMO DELITO INFORMÁTICO EN EL ÁMBITO DE LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y ESPAÑA, 2023",

Por tal efecto he procedido a leer y analizar de manera profunda el estilo y forma del contenido del texto, en donde se denota pulcritud en la escritura en todas sus partes, acentuación precisa, no existe vicios de dicción, hay concreción y exactitud en las ideas

Por lo expuesto, y en uso de mi derecho como especialista en Desarrollo educativo, recomiendo la validez ortográfica del presente proyecto de investigación

Ps. Narcisa Yagual Tumbaco, Msc.
C.I. 090795214-7
Registro de SENESCYT Tercer Nivel Psic. Educ1006-06-669556

Registro de SENESCYT Cuarto Nivel Msc. 7241104695

DECLARATORIA DEL TRABAJO

Nosotros, **DAVID EMANUEL SUÁREZ LIRIANO y ERNESTO RUBÉN ROCAFUERTE DEL PEZO**, estudiantes de la carrera de Derecho de la Universidad Estatal Península de Santa Elena, habiendo cursado la asignatura Unidad de Integración Curricular II, declaramos la autoría del presente trabajo de investigación, de título: **"El phishing como delito informático en el ámbito de las legislaciones de Ecuador, Argentina y España, 2023"**, desarrollada en todas sus partes por las suscritos estudiantes con apego a los requerimientos de la ciencia del derecho, la metodología de la investigación y las normas que regulan los procesos de titulación de la UPSE..

Atentamente

David Emanuel Suárez Liriano
CC. 0928231299

Ernesto Rubén Rocafuerte Del Pezo
CC. 0928279173

APROBACIÓN DEL TRIBUNAL DE GRADO

Ab. Víctor Coronel Ortiz, Mgt.
DIRECTOR DE LA CARRERA
DE DERECHO

Ab. Wilfrido Wasbrum Tinoco, Mgt.
DOCENTE ESPECIALISTA

Dr. Cristóbal Machuca Reyes, Mgt.
TUTOR

Ing. Bolívar Suárez Lindao
TUTOR

Ab. Brenda Reyes Tomalá, Mgt.
DOCENTE

DEDICATORIA

Dedico este trabajo investigativo a Dios, fuente de sabiduría y guía constante en mi vida. A mis padres Isabel Del Pezo y Oswaldo Rocafuerte, por su amor incondicional, el apoyo inquebrantable y sacrificio que han hecho a lo largo de toda mi vida. A mi tía Judith quien me ha impulsado a continuar con mis estudios, A mis amigos, por los momentos inolvidables que hemos compartido juntos y por su apoyo brindado estos años. A mi compañero y amigo de trabajo, por su colaboración, compromiso y valiosa contribución en este proyecto.
A todos ellos le dedico este trabajo como muestra de mi gratitud.

ERNESTO RUBÉN ROCAFUERTE DEL PEZO.

El presente trabajo de Titulación va dedicado a Dios, por darme la oportunidad de alcanzar una nueva meta en mi vida. A mis padres, abuelos y hermanos por ser los pilares fundamentales a lo largo de mi formación académica. A mis catedráticos de la UPSE por su enseñanza y valores impartidos. A mi amigo y compañero de trabajo, quien me dio su confianza para ejecutar este proyecto. Y así mismo, a mis amigos, compañeros que me brindaron su respaldo en su momento oportuno. A todos ellos, les dedico este trabajo como muestra de mi agradecimiento

DAVID EMANUEL SUÁREZ LIRIANO

AGRADECIMIENTO

Al Alma Mater Peninsular "Universidad Estatal Península de Santa Elena", por permitirnos formarnos bajo su tutela. A los docentes que en el transcurso de nuestra formación académica nos impartieron sus conocimientos. A la Ab. Brenda Reyes Tomalá, Mgt, docente de la Unidad de Integración Curricular por su valioso aporte académico y científico en la planificación, ejecución y consolidación de este trabajo investigativo.

A nuestros tutores, Dr. Cristóbal Machuca Reyes, Mgt. y Ing. Bolívar Suárez Lindao quienes, desde su experiencia y visión personal, orientaron nuestros objetivos para llevar a cabo con éxito esta tesis.

ERNESTO ROCAFUERTE Y DAVID SUÁREZ

ÍNDICE GENERAL

PORTADA I
CONTRAPORTADA II
APROBACIÓN DEL TUTOR III
CERTIFICACIÓN DE ANTIPLAGIO IV
VALIDACIÓN GRAMATICAL Y ORTOGRÁFICA V
DECLARATORIA DEL TRABAJO VI
APROBACIÓN DEL TRIBUNAL DE GRADO VII
DEDICATORIA VIII
AGRADECIMIENTO IX
ÍNDICE GENERAL X
ÍNDICE DE TABLAS XII
ÍNDICE DE GRÁFICOS XIII
RESUMEN XIV
ABSTRACT XV
INTRODUCCIÓN 1
CAPÍTULO I 3
EL PROBLEMA DE INVESTIGACIÓN 3
1.1 Planteamiento del Problema 3
1.2 formulación del problema 6
1.3 Objetivos 7
1.4 Justificación de la Investigación 8
1.5 Variables de investigación e Idea a defender 9
CAPÍTULO II 10
MARCO REFERENCIAL 10
2.1 Marco Teórico 10
2.1.1 Historia y generalidades del Phishing 10
2.1.2 Tipos De Phishing 12
2.1.3 Fases Del Phishing 14
2.1.4 Tasa De Ataque 15
2.1.5 El Internet 16
2.1.6 Derecho informático 18

2.1.7 Perspectiva Criminológica De La Delincuencia Informática 27
2.1.8 Política Criminal 32
2.1.9 Ley De Datos Personales 35
2.2 Marco legal 36
2.3 Marco conceptual 44
CAPÍTULO III 46
MARCO METODOLÓGICO 46
3.1 Diseño y tipo de investigación 46
3.2 Recolección de información 47
3.3 Tratamiento de información 48
3.4 Operacionalización De Variables 50
CAPÍTULO IV 52
RESULTADOS Y DISCUSIÓN 52
4.1. Análisis, interpretación y discusión de resultados. 52
4.2. Verificación de la idea a defender 58
CONCLUSIONES 60
RECOMENDACIONES 61
BIBLIOGRAFÍA 62

ÍNDICE DE TABLAS

TABLA # 1 DELITOS INFORMÁTICOS DE ECUADOR 33
TABLA # 2 DELITOS INFORMÁTICOS DE ARGENTINA 34
TABLA # 3 DELITOS INFORMÁTICOS DE ESPAÑA 35
TABLA # 4 POBLACIÓN Y MUESTRA 47
TABLA # 5 OPERACIONALIZACIÓN DE VARIABLES 50
TABLA # 6 CUADRO COMPARATIVO – DERECHO CONSTITUCIONAL 52
TABLA # 7 CUADRO COMPARATIVO – MARCO LEGAL (PRINCIPIOS) 53
TABLA # 8 CUADRO COMPARATIVO CONVENIOS INTERNACIONALES 55
TABLA # 9 CUADRO COMPARATIVO – ANTECEDENTES DEL TIPO PENAL 56
TABLA # 10 CUADRO COMPARATIVO ELEMENTO OBJETIVO DEL TIPO PENAL 56
TABLA # 11 CUADRO COMPARATIVO DE ELEMENTO SUBJETIVO DEL TIPO PENAL .. 57

ÍNDICE DE GRÁFICOS

GRAFICO # 1 15
GRAFICO # 2 15
GRAFICO # 3 FACTORES QUE DIERON ORIGEN A LA CIBERNÉTICA 21

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
CARRERA DE DERECHO

El PHISHING COMO DELITO INFORMÁTICO EN LAS LEGISLACIONES DE ECUADOR, ESPAÑA Y ARGENTINA, 2023

Autores: Rocafuerte del Pezo Ernesto Rubén
Suárez Liriano David Emanuel
Tutores: Dr. Cristóbal Machuca Reyes, Mgt.
Ing. Bolívar Suárez Lindao

RESUMEN

El presente trabajo de investigación se enfoca en la comparación jurídica de las legislaciones de Ecuador, Argentina y España respecto a las regulaciones de los delitos informáticos a través de sus normas penales, y de cómo esto encuadran la conducta del phishing en sus respectivos tipos penales. Dentro de su marco referencial se tuvo en consideración, los antecedentes históricos de cómo surgió el phishing, el origen de esta conducta, de igual manera los tipos de phishing, ya que esta conducta cuenta con varias variantes, la influencia que tuvo el internet a lo largo de los años, la definición del derecho informático, y la defensa que estas proporcionan, considerando, el concepto de delitos informático, de quienes intervienen en el cometimiento de esta conducta, cuál es el bien jurídico y la comparación de la política criminal de cada legislación. El enfoque que se empleo fue el cualitativo, en la cual se busca explorar como los avances tecnológicos y la evolución de sociedad hacen que surjan nuevas conductas delictivas y de cómo los países atienden estos tipos de delitos, que afectan a la sociedad y que derechos se vulneran con su cometimiento. Por lo tanto, los contenidos que se abarcan dentro de este trabajo se centran en comprender que es un delito informático y de cómo se lleva a cabo dentro del ciberespacio con la finalidad de que estos aspectos sean considerados al momento de que se tipifique un delito informático en sus normas penales. En virtud de lo investigado se concluye que, respecto a las demás legislaciones, Ecuador pese a tener dentro de su código orgánico integral penal una sección específica que tratan los delitos informáticos, tales artículos resultan ineficientes y obsoletos, ya que es difícil lograr encuadrar esta conducta en un tipo penal, debido a la variedad de delitos que se encuentran en el mismo.

Palabras claves: Derecho informático, Phishing, Delitos informáticos, Política criminal, Bien Jurídico.

ABSTRACT

The present research work focuses on the legal comparison of the legislations of Ecuador, Argentina and Spain regarding the regulations of computer crimes through their criminal regulations, and how this frames the conduct of phishing in their respective criminal types. Within its referential framework, the historical background of how phishing emerged, the origin of this behavior, as well as the types of phishing, since this behavior has several variants, the influence that the Internet had throughout over the years, the definition of computer law, and the defense that they provide, considering the concept of computer crimes, those involved in the commission of this conduct, what the legal right is and the comparison of the criminal policy of each legislation. The approach used was qualitative, which seeks to explore how technological advances and the evolution of society cause new criminal behaviors to emerge and how countries deal with these types of crimes, what affects society and what rights are granted. violate with their commitment. Therefore, the contents covered in this work focus on understanding what a computer crime is and how it is carried out within cyberspace with the aim that these aspects are considered when a computer crime is classified. in its criminal regulations. Based on what has been investigated, it is concluded that, with respect to other legislation, Ecuador, despite having within its comprehensive criminal organic code a specific section that deals with computer crimes, such articles are inefficient and obsolete, since it is difficult to manage this behavior. in a criminal type, due to the variety of crimes found in it.

Keywords: Computer law, Phishing, Computer crimes, Criminal policy, Legal good.

INTRODUCCIÓN

El Phishing es una conducta en el ámbito informático que mediante el engaño busca que las personas ingresen a un enlace, con el fin de robar u obtener los datos personales de los ciudadanos, este comportamiento los estados lo regulan dentro de su respectivo código penal, es por esto que el objetivo principal de este trabajo de investigación es comparar como el estado de Ecuador, Argentina y España atienden este delito informático en su normativa penal.

Por lo que es necesario tener en cuenta aquellos derechos que se encuentran reconocido en la constitución que se relacionen con la protección de los datos personales y de cómo el estado ha establecido artículos específicos en su normativa pernal para regular todo tipo de conductas nuevas que nazcan a través de la informática, de igual forma también es necesario tener leyes especiales y estar suscritos a convenios internacionales que se han sido creado para la protección de los datos personales, en los cuales se dan diferentes conceptos y principios que se encuentran establecidos en los mismos para tener una perspectiva más amplia en cuanto a cómo deben protegerse los países ante un delito informático de esta magnitud, la política criminal que ha adoptado cada estado para regular este tipo de acción en sus respectivos países.

Siendo el objetivo principal de este trabajo, la comparación de los países de Ecuador, Argentina y España en cuanto a cómo regulan o encuadran el phishing dentro de sus normativas penales, en las cuales mediante una matriz de comparación se busca evidenciar diferencias y semejanzas que estos países tienen en los temas abarcados.

La idea a defender se centra en que las legislaciones de España y Argentina regulan de una mejor manera este tipo de delitos a diferencia de Ecuador en la cual se evidencia una falta de especificad en la conducta de phishing.

En su capítulo I, como primer tema a tratar se encuentra la problemática de la investigación en la que se evidencia como surge esta conducta y de cómo es necesaria regularla por cuanto vulnera derechos que se encuentran reconocidos en la constitución, adicionalmente se encuentra la formulación del problema por cuanto existen varios tipos penales que pueden abarcar esta conducta, por consiguiente los objetivos generales y específicos ayudan a mantener estructura de los aspectos que se van a abarcar en este trabajo, de igual manera esta la justificación que guarda relación con la idea a defender y la variable independiente.

En su capítulo II, se encuentran la historia y origen del phishing, los tipos que nacen de esta conducta, sus fases en que se comete, como el internet y tuvo influencia en el surgimiento y aumento de los delitos informáticos, de igual forma como actúa el derecho informático ante un delito informático, su perspectiva criminología en cuanto a los que intervienen en el cometimiento de esta conducta, el bien jurídico que protege y la política criminal de cada

una de las legislaciones. De todos estos aspectos que sean investigados de es necesario tener en cuenta aquellos articulados que son objetos de estudio y de comparación en ámbito penal.

En su capítulo III, se compone del marco metodológico, en la que se evidencia el enfoque de carácter exploratorio de la investigación, asimismo, la recolección de información basado en las normas de las legislaciones de Ecuador, Argentina y España, el método comparativo y exegético, y las técnicas que se utilizaron para comprender el desarrollo de la investigación.

En su capítulo IV, que está compuesto por el análisis de los resultados y el tratamiento en donde mediante el uso de una matriz de comparación se establecen en que diferencias y que similitudes tiene cada una de las legislaciones, para posteriormente verificar si se cumplió o no con la idea a defender, y como último tema el desarrollo de las conclusiones y recomendaciones.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1 Planteamiento del Problema

Con el auge de la tecnología, con la llegada del acceso al internet y la gran facilidad que los medios electrónicos o tecnológicos han brindado a las personas, el internet se ha convertido en el medio por el cual se realiza el cometimiento de la conducta antijurídica denominada phishing, termino informático, que para algunos especialistas es considerado como un delito, ya que, su objetivo principal es la obtención de datos personales y posterior a esto cometer varias conductas.

En la actualidad, los delitos informáticos surgen por el avance de la tecnología, por falta de información de las personas y así mismo por falta de especificidad en las leyes. Si bien es cierto, el delito informático tuvo una gran escala en el 2020 por el confinamiento del COVID, en el cual las personas fueron forzadas a utilizar el internet como una fuente de comunicación y educación, que hoy en día, gracias al gran avance, las personas se han beneficiado en el ámbito tecnológico, pero a pesar de aquello, numerosos delitos informáticos surgieron, como lo es la estafa por medio de enlace o phishing, que se realiza con más frecuencias a través de redes sociales o correo electrónico, que trata de robar y alterar información personal, con el fin de obtener datos financieros.

A pesar de estos problemas, las legislaciones de diferentes países han identificado nuevas conductas jurídicas que son incorporadas como delitos en las normas penales, lo cual ayudan a evitar que estas conductas no queden en la impunidad y así mismo optar por la creación de nuevas normas más especifica que ayuden a proteger los derechos de las personas, dando paso a que nazcan nuevos términos jurídicos como lo es el phishing, que hace referencia al robo de información de todo tipo por medio de enlaces.

Por esta razón, Países como Ecuador, Argentina y España son países que tienen normativas eficientes para contrarrestar el phishing, pero la efectividad del control de estos delitos es diferente.

En Ecuador, el delito contra el phishing se asemeja a la estafa que está establecido en el Art, 186 inc. 2 del Código Orgánico Integral Penal: "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" (Codigo Organico Integral Penal [COIP], 2014).

Así mismo, a los Artículos 190, 230 y 234 del mismo Código, que refiere sobre la Apropiación fraudulenta, Interceptación ilegal de datos, y al Acceso no consentido a un sistema informático. De modo que, hace énfasis al Art 66 numeral 19 de la Constitución del Ecuador, que estable la protección de datos de carácter personal, tal como costa a continuación:

> El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Constitución De La República Del Ecuador [CRE], 2008)

Y a Ley Orgánica De Protección De Datos Personales que establecen medidas y principios para contrarrestar los delitos informáticos.

Sin embrago, es importate mencionar que el Ecuador pese a contar con todas estas normativas, la falta de especificidad de sus normas y de experto en derecho informatico, hace que la política criminal internas no profundice respecto a estas conductas, por lo tanto, ocasiona que los delitos informaticos como es el phishing solo sean de investigación por parte de la fiscalía.

Según datos de la Compañía de ESET en Latinoamérica, "Ecuador lidera la lista con un 8% de detecciones maliciosas de campañas de phishing" (La Nación / Costa Rica / GDA, 2023), pero, estos pueden seguir en aumento si el Ecuador no reconoce estos incidentes.

En cambio, Argentina el delito de phishing, hace alusión al Art 1 de la Ley N° 25.930 y al Art 9 de Ley N° 26.388, que en el Código Penal de la Nación Argentina se incorpora en su art 173 inciso 15, 16, la cual define lo siguiente:

> El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.
>
> El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

De igual manera evoca al Artículo 172, del código penal, que trata sobre la estafa y las diversas formas de fraudes.

Sin embargo, aunque Argentina tenga artículos más eficientes sobre el delito de phishing, "Argentina, se encuentra en el séptimo lugar entre los países que más amenaza de phishing recibe, según informe de la empresa de seguridad ESET informática" (ESET, 2023), además informa que los ataque cada vez son más sistematizado.

No obstante, en España, las normas sobre el delito informático phishing son muy específica, puesto que, en el transcurso del tiempo, España ha optado regulaciones en torno a la gran parte de los tipos de delitos informáticos, tales como lo provee el Código penal en su Artículo 248 y 249 que hace énfasis al delito de la estafa, el cual tiene relación al phishing, de igual manera al convenio de Budapest, a las leyes de protección de datos y a la normativa del Art 18.4 de la Constitución Española, que trata sobre la informática, tal como se detalla a continuación: "el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (CONSTITUCIÓN ESPAÑOLA, 1978). Es por esa razón que este país es uno de los países que tiene más seguridad para detectar los ciberdelitos.

Según un informe realizado de la Empresa ESET, "en el último cuatrimestre de 2022, se observa un importante crecimiento en la detección de campañas de correos electrónicos de phishing en un 26,1%" (Barahona, 2023).

En consecuencia, a lo mencionado, un principal factor que ayuda a que los países de Argentina y España regulen de una mejor manera este tipo de conductas delictivas en las

cual se usen dispositivos electrónicos y a su vez también el internet, es que ambos países cuanta con normativas, leyes más específicas y están ratificado al convenio sobre ciberseguridad que se llevó a cabo en el año 2001 en Budapest, en el que hace mención a una serie de delitos informáticos y establecen definiciones que ayudan al momento de interpretar este tipo de delito.

Por lo abordado, se puede considerar que la esencial amenaza del phishing, es la evolución del internet, que, por su gran escala en la obtención de datos personales y a la vez por la seguridad que brindan al usuario, los ciberdelincuentes buscan métodos más eficientes para atacar a las personas y así obtener o acceder a sus cuentas bancarias. Pero todo esto se puede regular mediante las normativas vigentes de cada país, implementando, más control, en las empresas que cuentan con datos personales, como lo son las redes sociales y entidades bancarias.

1.2 formulación del problema

¿Existe diversidad normativa penal en relación al phishing en España, Ecuador y Argentina?

1.3 Objetivos

Objetivo general

Comparar las legislaciones de España, Argentina y Ecuador en el ámbito de los delitos informáticos con respecto al phishing, mediante el uso de doctrina, considerando las normativas penales de estas legislaciones, y el convenio de Budapest, para la valoración de los tipos penales en la caracterización de la conducta y las sanciones en cada una de las legislaciones.

Objetivos específicos

- Analizar las legislaciones de España, Argentina y Ecuador en el ámbito penal, a través del estudio jurídico e histórico, de conformidad a la regulación del phishing como delito informático.
- Fundamentar jurídicamente aspectos que diferencian a los países de Ecuador, Argentina y España en relación al phishing, usando el método comparativo en cuanto a la regulación que tiene cada una de las legislaciones en el ámbito penal.
- Diagnosticar como la política criminal del Ecuador en relación a los países de Argentina y España atiende este tipo de conductas y lesiones en cuanto al phishing.

1.4 Justificación de la Investigación

La problemática del phishing como delito informático, cada vez es más evidente por la falta de Especificidad en las normas en Ecuador, en comparación a las legislaciones de Argentina y España quienes cuentan con normas más específicas y convenio que sirve para erradicar los delitos informáticos, limita a que estos países no tengan excesivo problema en cuanto al robo y vulneración de datos personales que ocurren por medio del internet.

Este proyecto investigativo se enfoca en las teorías, aportes científicos y comparativo de las legislaciones de Argentina y España puesto a que estos países regulan el phishing de una manera eficiente en sus respectivos códigos penales, y a su vez al estar suscritos o ratificados al convenio de Budapest tienen una definición más apta sobre este tipo de delitos, por lo que es muy importante este convenio para el análisis de las normas que tiene el Ecuador con relación al phishing.

Para el desarrollo de esta investigación se tendrá en cuenta el método analítico comparativo y así fundamentar jurídicamente aspectos que diferencian a cada una de las legislaciones en comparación con la de Ecuador, de cómo regulan este tipo de conductas, y así diagnosticar la falta de normativa en cuanto al cometimiento del delito de phishing en la forma en que se lo realiza.

Conforme a los objetivo de este análisis, se busca evidenciar la falta de normas que existe en el Ecuador, en relación al tipo penal referente al phishing, que trata sobre el robo y vulneración de datos personales, y al mismo tiempo aludiendo a los derechos de libertad establecido en la Constitución de la República del Ecuador en su Art 66 numeral 19 establece "El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección." (CRE, 2008). por lo que es necesario el estudio de otras legislaciones para su comprensión en el tema y de esta manera poder contribuir a que se pueda reconocer estas normas y sean tomadas en consideración respecto al tipo penal de phishing.

1.5 Variables de investigación e Idea a defender

UV: El phishing como delito informático

Idea a defender

Las normas penales de Argentina y España garantizan de manera más efectiva la protección de datos personales de sus ciudadanos con la tipificación del phishing respecto a la falta de especificidad de este comportamiento criminal en la legislación ecuatoriana.

CAPÍTULO II

MARCO REFERENCIAL

2.1 Marco Teórico

2.1.1 Historia y generalidades del Phishing

Historia y Definiciones

Desde la evolución del internet, el phishing es uno de los términos que se utiliza para definir un fraude informático o una estafa informática, el cual tiene como objetivo revelar información personal y financiera con la intención de suplantar la identidad digital de una persona o para la obtención de algún beneficio.

Según Luis Camacho Losa, en su libro El Delito Informático establece, que el fraude informático es "toda conducta fraudulenta realizada a través o con la ayuda de un sistema informático, por medio de la cual alguien trata de obtener algún beneficio ilícito" (LOSA, 1987).

Con lo antes mencionado, se considera que el fraude informático se lleva a cabo de manera dolosa mediante un sistema digital, y tiene como objetivo la obtención de datos personales, bancarios, financieros, electrónicos, entre otros, de sus victimarios.

El término phishing, tiene origen de la palabra inglesa fishing que significa pescar y hace alusión a la pesca por anzuelo, puesto que la palabra pesca alude a la estafa de los usuarios del internet, y anzuelo a los que ofrecen sus datos o a los que caen en la trampa, hay que hacer énfasis que las personas que practican este delito se lo conocen como phisher.

Según Juan Carlos Valle Matute en su artículo El Delito Informático De Phishing, establece que "El phishing es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima" (MATUTE, 2013).

Por lo tanto, se deduce que el phishing es llamada ingeniería social, porque los ciberdelincuentes en primer lugar investigan a sus víctimas, y una vez que obtienen ciertos datos, proceden a cometer los ataques.

Por otro lado, la palabra F se lo reemplaza por el vocablo ph debido a que los primeros ciberdelincuente eran conocidos como phreaking que hace referencia al aprendizaje, comprensión y al estudio de nuevas tecnologías, de igual manera esta grafía tiene mucha tolerancia debido a que es una abreviatura de password harvesting fishing que traducido en español significa pesca de recolección de contraseñas, por ende la grafía ph se utiliza para la identificación de los ataques que realizan estas comunidades, no obstante, esta grafía también se deriva de la palabra phone que significa teléfono y freak que significa Loco o raro.

La primera mención del phishing, surge en enero de 1996, cuando los primeros hackers o ciberdelincuentes comenzaron a atacar por medio de correos electrónicos, con el objetivo de obtener información a usuarios inocentes. Esto se dio a conocer cuando AOL empresa popular proveedora de internet con sede en New York, sufrió ataque de phishing, en el que los atacantes, utilizaron la mensajería rápida con el objetivo de poder hacerse pasar como empleados de dicha empresa, y a así obtener las credenciales de los usuarios para luego secuestrar sus cuentas y de igual manera para utilizarla para fines específicos

A inicio de los 2000, los ciberdelincuentes, empezaron a enfocarse en la obtención de cuentas bancarias, por lo tanto, los correos electrónicos fraudulentos que eran utilizados para phishing, se comenzaron a utilizar para convencer a los usuarios a que divulguen sus credenciales bancarias. Estos correos que eran utilizados para dicha acción, obtenían la información personal mediante enlace que dirigía a webs o páginas maliciosas que tenían la misma característica del banco, pero el dominio de la página era diferente a la oficial, por ejemplo: bancoguaiaquil.com en vez de bancoguayaquil.com. A raíz de esto, los ciberdelincuentes comenzaron a dirigirse a otros tipos de cuentas, como yahoo!, google, eBay con las únicas finalidades de cometer fraude, robar dinero o enviar spam a otros usuarios.

Según informe de la Dirección Nacional de Ciberseguridad de Argentina define que hoy en día, el phishing se desarrolla con frecuencia en las redes sociales, lo cual establece que “A través de estas plataformas los hackers no sólo podían obtener información crediticia de sus

víctimas sino también sus identidades digitales, con fines variados que van desde la extorsión hasta otros tipos de estafa" (Ciberseguridad, 2021).

Por lo tanto, se deduce que, en la actualidad, con la evolución del internet, la creación de nuevas plataformas digitales, redes sociales, los ciberdelincuentes han creado herramientas y métodos más efectivos para la obtención de información de cuentas bancarias, por lo que se puede expresar que el phishing, aún sigue siendo un problema para los usuarios del internet, pero no obstante existen países que ya cuentan con normas que regulan este tipo de delito informático.

2.1.2 Tipos De Phishing

Dado que, el phishing se define como un método de engaño que se efectúa mediante conocimiento de ingeniería social con la finalidad de hacer que las víctimas muerdan el anzuelo. Existen otros tipos de phishing, que usualmente utilizan los ciberdelincuente o atacante para cometer sus delitos, los cuales son:

Spear phishing

El Spear phishing es unos de los tipos de phishing que utilizan los ciberdelincuentes para que la víctima divulgue información personal, descarguen virus, o que envíen mensaje sin autorización. Este tipo de phishing se realiza mediante campaña, que cada vez son más personalizadas y tienen similitud a la fuente original. Por lo general, están dirigidas a personas o grupos de personas en específicas de una organización, por lo que esto ocasiona un aumento de víctimas.

El Spear phishing comúnmente "trata de capturar a la víctima con un arpón, que es lo que significa "pea" en el idioma inglés" (Ciberseguridad, 2021). Y su mecanismo es enviar un correo electrónico al destinatario, supuestamente de una página confiable, que va direccionada a un sitio web falso que contiene malvare.

Whale phishing/whaling.

El whale/whaling, es un tipo de phishing que tiene como objetivo atacar a peces gordos. Como funcionarios generales o ejecutivos de alto rango. Al igual que el Spear phishing, este tipo se desarrolla mediante un estudio a la víctima, para luego proceder con el ataque.

El whaling phishing “proviene del inglés “pesca de ballenas”, es una variante del spear phishing, pero dirigido a una persona o empresa considerada de influencia” (Ciberseguridad, 2021). Se puede decir que el Whale phishing/whaling es una variante del Spears phishing, pero su finalidad no es obtener datos personales y hacerse pasar por una persona común y corriente sino por una persona considerada y reconocida.

Social phish o Phishing por redes sociales

El social phish, trata de páginas web falsas que tienen las mismas características y plantillas, que las redes sociales pero su dominio es diferente que la oficial, quiere decir, que cambia ciertas palabras en su fuente. Estas páginas tienen la intención de extraer una copia de la información personal por medio de una base de datos, una vez que la víctima agregue su información.

El social phish, comienza por los “phishers que acceden a cuentas de redes sociales y logran que la gente envíe enlaces maliciosos o spam a sus contactos, ya sea a través del servicio de mensajería o en el etiquetado de posteos públicos” (Ciberseguridad, 2021). Este tipo de phishing es muy frecuente hoy en día, ya que los hackers crean métodos más eficientes para engañar a sus víctimas.

Shellphish.

El shellphish es una herramienta que se utiliza para cometer phishing, esta herramienta cuenta con un interfaz donde exponen los servicios que los usuarios acceden con cotidianidad, y de igual manera cuenta con un panel para acceder a los equipos infectados con malware.

Hoy en día aparte de shellphish existen sin número de herramienta que sirven para la obtención y verificación de datos personales.

Pharming

El pharming o Phishing sin sueño, se da mediante navegación del internet, el cual se puede ejecutar por medio de un archivo host de la dirección IP o por el DNS. “El nombre “pharming” viene de la combinación de los términos phishing y pharming, que podríamos traducir como cultivo” (Ciberseguridad, 2021). Generalmente cuando ocurre este tipo de

phishing, los hackers instalan virus a su computadora o redirige a los usuarios a que visiten paginas fraudulenta, todo esto lo ejecutan con el objetivo de robar los datos de la víctima.

2.1.3 Fases Del Phishing

Las fases del phishing surgen en base al estudio analítico de las investigaciones que se han realizado en la lucha para contrarrestar este tipo de delito informático. Por lo tanto, los estudios realizados demuestran que existen varias variantes, de los cuales, seis son las principales que se contemplan con más frecuencias en los delitos de phishing

1. Planificación

La planificación es un rol importante dado que los phisher o delincuentes informáticos, durante esta etapa, investigan a sus víctimas, analizan sus datos personales y planifican cuales medios van utilizar para cometer los ataques.

Se puede decir que el delincuente informático, realiza una división de su tarea para analizar primero a quien o quienes van a llevar a cabo sus ataques.

2. Preparación

En la preparación los phisher, deben de obtener el programa, el sitio web que se va utilizar para sus taques, los contactos de las víctimas, la localización donde van hacer dirigidos los ataques y los equipos que se van a utilizar, teniendo en cuenta que esto pueden variar dependiendo del delito que se va a cometer. Por lo general los delitos que se cometen son dirigidos a una persona determinada, por lo tanto, los ataques que se crean son más genuinos.

3. Ataque

En el ataque en ciertas ocasiones son altas o medias, dado que las víctimas tienen el control de sus acciones, como abrir el correo fraudulento o visitar una página web falsa y brindar sus datos personales.

4. Recolección

La fase de recolección, implica de cómo fue ejecutado la fase anterior, porque de esa se desprende la recolección de datos. En el caso de que la víctima haya seleccionado el correo

fraudulento y agregado sus datos personales en las páginas falsa, hace alusión que los ataques fueron efectivo y por lo tanto colaboraron en la obtención de sus datos.

5. Fraude

Una vez recolectados los datos, posteriormente los delincuentes informáticos cometen la estafa de manera directa o venden sus datos a otros estafadores.

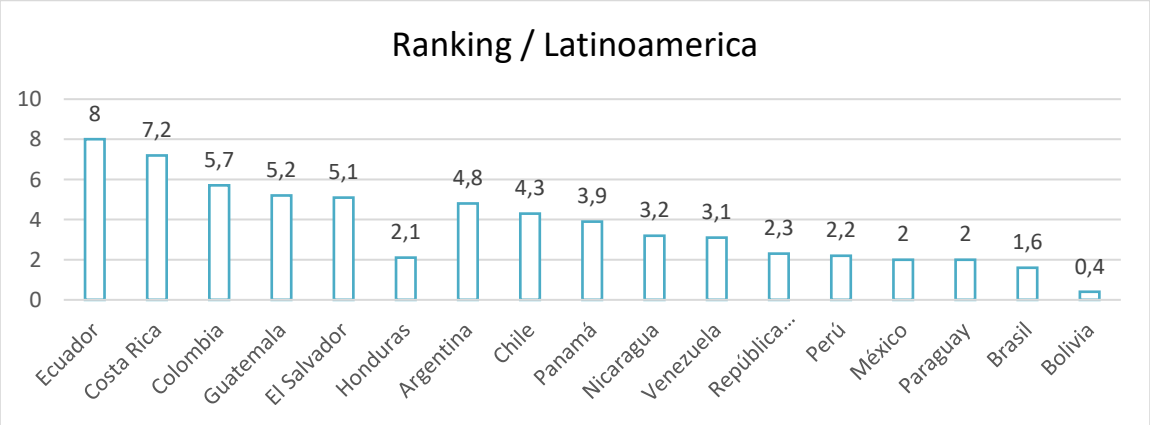
6. Post- Ataque

El post ataque, como última fase, trata de que el delincuente vuelva a ingresar con los datos de la víctima a sus plataformas con el fin de eliminar sus rastros.

2.1.4 Tasa De Ataque

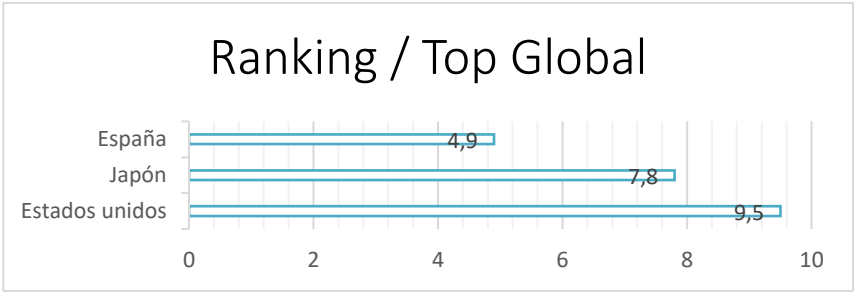
En relación a los ataques informáticos, se evidencia que el phishing es uno de los delitos informáticos más aplicado en los últimos años, debido a la flexibilidad que tiene para engañar a las personas. Tal como se evidencia a continuación:

GRAFICO # 1



Elaborado: David Suárez L – Ernesto Rocafuerte Del P. **Fuente:** ESET

GRAFICO # 2



Elaborado: David Suárez L – Ernesto Rocafuerte Del P. **Fuente:** ESET

De acuerdo al informe de ESET Latinoamérica, Ecuador ocupa el primer lugar en detección de phishing y argentina el séptimo lugar. Pero en el top global se observa que España se encuentra en el tercer lugar de los países que más se detecta el delito de phishing.

2.1.5 El Internet

Internet y su influencia en la sociedad.

El internet llegó al Ecuador en el año de 1992 de la mano de Marcel Laniado de Wind fundador de banco del pacifico, quien producto de unos de viajes fuera del país conoce el internet como un medio de comunicación el cual le ofrecía un sin número de ventajas y que además le resultó algo novedoso y útil, por lo que decidió traer "Era una red que el gobierno norteamericano denominó Arpanet y servía para tener interconectadas las computadoras del ejército, la armada, la aviación y los diferentes departamentos de seguridad y de protección de ese país" (Mite, 2017).

El internet se inició en el Ecuador en el año de 1992, iniciativa de Banco del pacifico de mano de su fundador, quien optó por darle el nombre de EcuaNet siendo el precursor del internet en Ecuador. Así mismo en el año de 1994 se empieza a comercializar el internet a nivel empresarial, debido a que estas vieron un gran potencial en tener este medio de comunicación y que les beneficiaría en ambos ámbitos no solo el de comunicación. En ese mismo año "arrancó la masificación con las ventas residenciales y la introducción de servicios de diseño y almacenamiento de páginas web" (Mite, 2017).

Por lo que si bien es cierto que en sus inicio el internet fue de acceso restringido, y que solo podían tenerlos aquellos que disponían de recursos, por lo que lo que afirma lorenzo Trejo es totalmente verídico, sino también es importante mencionar que en esos años las personas no tenían tanto conocimiento de lo que era el internet y para que servía, ya que solo se pensaba que el internet solo se podía utilizar para aquellos que disponían de una computadora y que solo se utilizará para comunicarse unos con otros.

Si bien es cierto el primero precursor de que el internet llegara a Ecuador fue el Fundador de Banco Del Pacifico ya que por interés propio trajo consigo el internet para posteriormente, hacer de esto un negocio. Por lo que al ser un negocio nuevo y novedoso se fueron creando nuevas compañías que ofrecieran este servicio no solo a las grandes empresas, sino que este

tuvo un alcance ya a nivel de la toda la sociedad, sin embargo, estas aún no conocían todo lo que se podía realizar a través del internet. Desde este punto se puede evidenciar que ya no solo las empresas y las personas tenían este servicio, si bien es cierto con el pasar de los años su acceso fue más fácil, ya que no solo se podía conectar a través de internet por medio de una computadora, la tecnología evolucionó a tal punto que los celulares empezaban a tener un mayor impacto en la sociedad, con la llegada de los celulares de tercera generación que estos celulares tienen acceso a internet desde cualquier parte sino que además tenían otras funciones que facilitan su manejo.

> La 3G es tipificada por la convergencia de la voz y datos con acceso inalámbrico a Internet, aplicaciones multimedia y altas transmisiones de datos. Los protocolos empleados en los sistemas 3G soportan más altas velocidades de información enfocados para aplicaciones más allá de la voz, tales como audio (MP3), video en movimiento, videoconferencia y acceso rápido a Internet, sólo por nombrar algunos. (Rodríguez Gámez, Hernández Perdomo, Torno Hidalgo, Rodríguez Romero,, & Rodríguez Romero, 2005)

Por consiguiente, en Argentina "la llegada del internet fue en los años de 1994 en el que ya se podían acceder a enlaces de sitios webs, esta fue una iniciativa por parte de la cancillería de Argentina" (RETAMAR, 2022). Con el objetivo de mantener comunicación con aquellos organismos que se encontraban en el exterior, por otro lado, en España la revista latina de comunicación social menciona que el apogeo del internet en dicho país fue:

> En 1970, apenas existían ordenadores y los pocos que existían estaban localizados en universidades y centros de investigación. Es debido a la evolución del hardware y a la aparición del ordenador personal (IBM coloca en el mercado su PC en 1981 y Apple hace lo mismo con su Macintosh en 1984) y su manejo por usuarios lo que origina el incremento desorbitado de ordenadores conectados a la red. (Contreras, 2001)

Teniendo en cuenta estos antecedentes y que con la llegada del internet en estos países la demanda del uso de este servicio aumentaría con el pasar de los años. Por lo que partiendo de la idea que a partir de los años 2000 en adelante tanto computadoras de escritorio como portátiles (Laptops), y los celulares ya tenían acceso a internet y que podían conectarse desde cualquier lugar ya que un celular lo podía hacer por medio de los datos y mientras que una computadora lo hacía mediante un módem. Por lo que a partir del siglo XX en adelante estos dispositivos tendrán más alcance a nivel social, en donde la curiosidad de las personas hace que surjan nuevas conductas que necesitan ser reguladas, lo que hace que con el pasar de los años conductas que solo se podían cometer dentro de una sociedad se las pueda realizar por

medio de estos dispositivos. Tengamos en cuenta que al mencionar conductas solo se está refiriendo al robo, que consiste en la apropiación de un bien ya sea por medio de la violencia o no, otra conducta que se podía cometer dentro de la sociedad es la estafa, en que se buscaba el beneficio propio o para un tercero, este beneficio puede ser económico. Es así como uniendo varios conceptos nace la conducta del phishing que consiste en robo de los datos personales para luego obtener un beneficio económico.

Sin embargo, es necesario tener en cuenta que el robo de estos datos se realiza por medio de cualquier dispositivo electrónico con acceso a internet.

2.1.6 Derecho informático

El derecho informático es la unión de dos disciplinas completamente diferentes, pero que, con la evolución de los seres humanos, y como la tecnología ha influido tanto en la vida de las personas, a tal punto que la mayoría de las cosas que se realizan a diario, se la podrá realizar con normalidad, pero siempre estará la presencia de la tecnológico como método alterno que le permita ahorrar al usuario tiempo, además que lo puede hacer desde la comodidad de su hogar. Esto se debe que la tecnología se ha vuelto un medio crucial por el cual podemos realizar nuestras actividades de forma más rápida y eficiente, sin embargo, eso no implica que lo podamos realizar de manera segura. Esto ha llevado a que la ciencia del derecho proteja de alguna u otra manera todas conductas y actividades que se puedan realizar por cualquier medio tecnológico, con la creación de normas, por otro lado, la ciencia informática, como aquella que estudia todas las cuestiones, actividades y conceptos en las que se encuentre relacionado con la informática, sin dejar de lado como los datos son almacenados y procesados dentro de este ámbito. La unión estas dos ciencias o disciplinas tiene consigo un factor en común muy importante que es el impacto que tuvo la informática en la sociedad, debido a que al ser un tema nuevo, novedoso y la facilidades que este medio brindaría a sus usuarios, ocasiono que la informática se posicione dentro de la sociedad como una herramienta fundamental, lo que trajo consigo conductas que solo la informática podía entender, así mismo también existieron otros aspectos que la informática podía abarcar y explicar, lo que hizo que surgiera la necesidad de que aquellas conductas que se conocían y que, la informática podía explicar se las regulen a través del derecho.

El Español Peñaranda Quintero manifiesta que el Derecho Informático:

> Es aquella ciencia que trata la Relación del Derecho con la Informática desde el punto de vista de las normas legales y de la Jurisprudencia que van a regular acciones, reglas jurídicas, procesos y relaciones jurídicas entre personas en el amplio mundo de la informática. (Quintero, 2007)

Como se ha mencionado que el derecho informático es la unión de estas dos ciencias, pero cuando se refiere a derecho es imposible, no pensar que ya se refiere a un conjunto de normas que normas que regulan este tipo de acciones que no se encuentra reguladas por el derecho dentro del mundo de la informática y de la tecnología.

El español Antonio Pérez refiere al derecho informático como la ciencia que:

> Estudia una materia de carácter jurídica pero conformada por el sector de normas jurídicas de carácter contemporáneo que buscan la regulación de las nuevas tecnologías y de la información, así como de la comunicación, es decir, del mundo de la informática y de la telemática. (Pérez Luño, 1996)

Este autor español establece al referirse al termino derecho informático se refiere directamente a las normas que se encuentran tipificadas para regular un comportamiento en específico, pero en un mundo completamente diferente que es el derecho informático, en el que se busca proteger aquellas conductas contemporáneas, es decir aquellas conductas que van surgiendo conforme el avance de la sociedad y de la informática va evolucionando, por lo que es importante estar actualizado en estos temas que desconocen y casi ya es un hábito que estas conductas se vean con más frecuencia. Por otro lado, tenemos que Núñez define al derecho informático como la "aplicación del derecho a la informática permitiendo que se adopten o creen soluciones jurídicas a los problemas que surgen en torno al fenómeno informático" (Núñez, 1996, pág. 22). Este concepto es un poco más enfocado a que este derecho debe ser un poco más adaptable a lo que se vive en la sociedad, debido a que conforme avanza la sociedad las conductas que se conocía varían o han evolucionado, dejando así una norma obsoleta o ineficaz, es por esto que se menciona que se deben adoptar o crear soluciones en derecho que pueda ser explicado por la informática, pero sin dejar a un lado la realidad social que se vive.

La cibernética

Esta disciplina abarca varios aspectos que tienen relación entre si por un lado la informática que es aquella que se encarga del manejo de los datos de forma automática y de cómo intervienen los dispositivos como instrumentos. Por otro lado, la cibernética como aquella

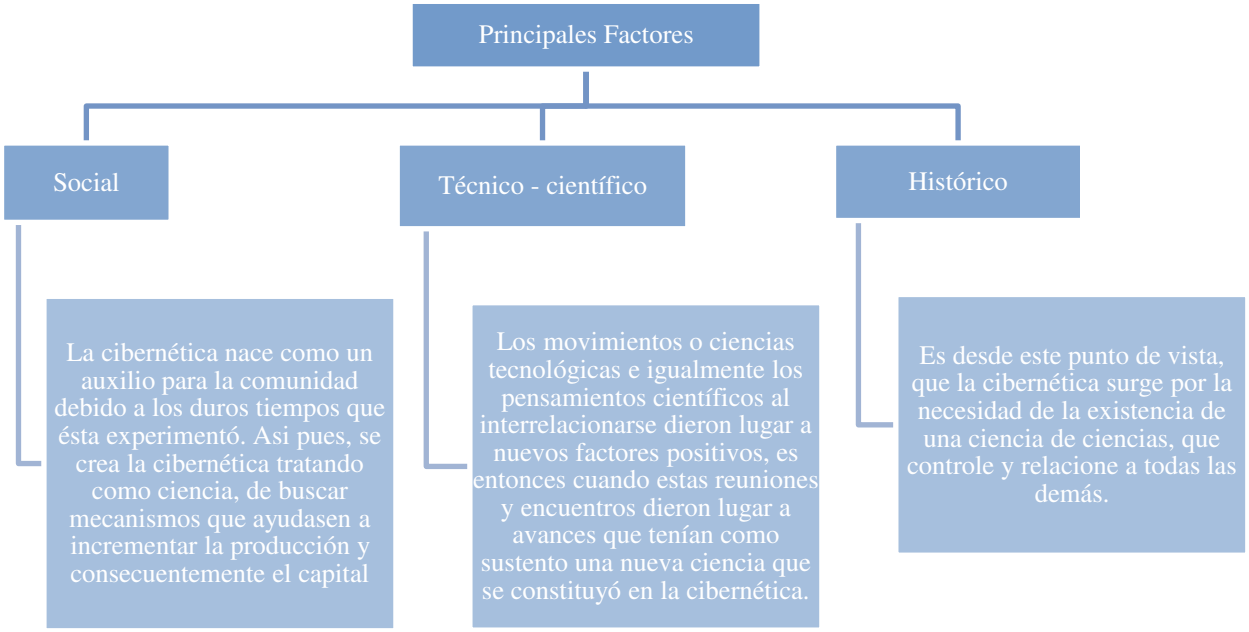
ciencia que estudia la relación que existe entra máquinas y las personas, y de su importancia que esta tiene disciplina al relacionarse con las demás ciencias.

> La cibernética en un stricto sensu se refiere a los mensajes usados entre hombres y máquinas, entre máquinas y hombres y entre máquinas y máquinas, en luto sensu, es la que se determina como la ciencia de ciencias, conformándose entonces en una ciencia general que estudia y relaciona a las demás ciencias. (Flores Salgado, 2015)

Tal como lo manifiesta salgado en su libro "Derecho informático" tiene una gran importancia en cuando a una conducta que puede descrita como un delito, ya que esta disciplina estudia esa relación que existe entre los seres humanos y las personas, también como una maquina puede comunicarse con otra máquina, todo esto gira entorno en cuanto a la relación de las personas y como intervienen las maquinas, así mismo en dicho libro menciona que es un ciencia que relaciona con varias ciencias para tener un mejor alcance y tener una mejor perspectiva en cuanto al objeto de estudio. Esto se lo puede reafirmar de la siguiente manera ya que la cibernética "es primordial para la unión entre derecho e informática, pues la cibernética es la ciencia de las ciencias, y surge como necesidad de obtener una general que estudie y trate la relación de las demás" (Flores Salgado, 2015). Como se ha manifestado con anterioridad esta disciplina se relaciona con otras para tener un mejor alcance en cuanto a un objeto de estudio y de como esta se relaciona de con otras ciencias que se pueden relacionar, partiendo de esta idea se puede decir que la cibernética se conecta primero con la informática, ya que esta estudia cómo se manejan o circulan los datos dentro de un ciberespacio, mientras que la cibernética como tal se centrara en el estudio de como el ser humano o las personas usan las máquinas para lograr este objetivo, y como ultima ciencia que se encuentra conectadas a estas, está el derecho, en la que se busca regular estas nuevas conductas a través de normas.

Relacionando ambas disciplinas con el objeto de estudio tiendo en primer lugar la informática como aquella ciencia que se encargada de manejar los datos personales de todas las personas que navegan por internet, mientas que por otro esta la cibernética esta se centra en el manejo que le dan las personas a los dispositivos electrónicos, de forma específica podemos percibir como estas dos ciencias se relacionan a la conducta del phishing, en donde esta busca obtener los datos de las personas de forma ilegal, usando como medio cualquier dispositivo electrónico y que posterior a esto puede utilizar esos datos de cualquier forma.

GRAFICO # 3 FACTORES QUE DIERON ORIGEN A LA CIBERNÉTICA



Elaborado: David Suárez L – Ernesto Rocafuerte Del P. **Fuente:** Flores Salgado – Delitos Informáticos

En el factor social se constatar que esta ciencia nace como necesidad y para brindar un auxilio debido a los duros tiempo que se vivía en ese tiempo, debido a que se cursaba la segunda guerra mundial, en este tiempo se utilizó la cibernética en la automatización de las armas, pero con mínimo esfuerzo o intervención de las armas, relacionando esto a una época más actual se puede evidenciar la relación que guardan los seres humanos con la máquina, en el que los seres humanos programan a través de ella, y luego la maquina ejecuta siguiendo las indicaciones que le dio la persona, sin dejar a un lado que también puede existir una intervención de la persona al momento de ejecutar las ordenes, pero con mínimo de esfuerzo.

Por otro lado tenemos el factor técnico – científico si bien es cierto la cibernética nace como una ciencia la cual trata de ayudar a los seres humanos en varios aspectos, es así como a través de una disciplina que a través de un objeto de estudio busca relacionar con otras ciencias para tener un mejor contraste de lo puede significar un nuevo de estudio y como este se relaciona con otras ciencias, siendo así de suma importancia aplicar los conocimientos científicos, y de cómo la cibernética ayudo en aspectos medicinales o en la producción de las grandes empresas, así mismo no se pudo dejar de lado el avance de la tecnología y de cómo afectaría a la sociedad, además del impacto que esta tuviese con las demás disciplinas o ciencias.

El factor histórico es un poco más sencillo explicar ya que esta ciencia nace por la necesidad que exista una ciencia que relacione a las otras, y estos se puede evidenciar a lo largo de la historia como se relaciona una con otras, la cibernética no solo busca comparar o relacionar una ciencia con otra, esta puede relacionar varias ciencias en un mismo tema de estudio, un claro ejemplo seria la informática, el derecho y la cibernética.

Teorías de la cibernética que se relacionan con el objeto de estudio

Estas teorías es de suma importancia analizar para entender cómo se relacionan el ámbito informático y dentro del derecho.

Siendo teoría quien solo se centra en cómo es maneja la información y de cómo los sistemas informáticos la procesan, debido a que el ciberespacio es mundo amplio en el que se la información viaja a gran velocidad y que esta puede tener varios destinos es por eso que esta teoría se centra en esto.

Por otro lado, está la "Teoría de los algoritmos, tiene como finalidad la formulación de reglas y procedimientos para solucionar un problema concreto en las computadoras" (Flores Salgado, 2015). Este concepto aplicado en derecho se lo evidencia en conceptos o en procedimientos que nacen de la informática debe ser regulado su uso por normas, ya que estas conductas pueden ser ocupadas de una forma que ayude a la sociedad, mientras que por otro puede perjudicar que no se regule su uso, esta teoría tiene una relación con "la teoría de la regulación o de control que abarca la regulación automática de los sistemas activos o dinámicos" (Flores Salgado, 2015). Recapitulando estas tres teorías se centra en un área en especifica siendo la teoría de la información en los datos, la de algoritmos en los procedimientos o conceptos que dé están se derivan, y por último la de control, que como su nombre lo indica está centrada en un control y que exista una regulación.

Delito informático

Buscar un concepto o una definición de lo que es el delito informático de forma exacta representa un problema, ya que a lo largo de la historia se puede evidenciar que con forme avanza la sociedad quedan aspectos aislados u obsoletos que no ingresan dentro de las definiciones o conceptos que buscan dar los especialistas, para poder explicar lo que quiere abarcar intentando buscar una definición que se acople de forma tan precisa dentro de un

país, teniendo en cuenta los aspectos sociales, económicos y culturales, por lo que es casi imposible encontrar una definición que se ajuste a la realidad dentro de un contexto en específico, un claro ejemplo es el surgimiento de la inteligencia artificial o la IA, ya que al ser un tema nuevo no se encuentra regulado su uso en ningún país. Lo mismo pasa con las conductas que van surgiendo conforme va evolucionando la tecnología y que se desconoce dentro del derecho informático, y por cuanto dichos conductas no constituirían un delito, un claro ejemplo de una nueva conducta dentro del ámbito informático es el phishing.

El Autor Felipe Villavicencio Terreros define a los Delitos informáticos como "aquellas conductas dirigidas a burlar los sistemas de dispositivos de seguridad, esto es, invasiones a computadoras, correos o sistemas de datas mediante una clave de acceso; conductas típicas que únicamente pueden ser cometidas a través de la tecnología" (Terreros, 2014). El autor Felipe Villavicencio da una definición más enfocada a los ataques que pueden darse burlando el sistema de seguridad o atacando la seguridad que estos poseen para para poder acceder a estos, por otro lado, también menciona que son conductas típicas, sin embargo, considero que se está limitando a aquellas conductas que conocen al momento, es decir que no se toman en cuenta las que son pocas conocidas, o que se desconocen, como lo es el phishing que es una conducta nueva y que se desconoce o no se encuentran reguladas por algún cuerpo normativo.

Por otro lado, Mühlen manifiesta que el delito informático "ha de comprender todo comportamiento delictivo en el que la computadora es el instrumento o el objetivo del hecho" (Mühlen, citado por Felipe Villavicencio 2014, p.3). Este define de al delito informático de una forma más amplia, ya hace mención que este compre a todo el comportamiento que nazca o que se pueda cometer por medio de una computador, es decir que la computadora es el medio o el instrumento por el cual se va cometer el acto delictivo, pero este a su vez este limita a aquellos dispositivos, por el que se puede cometer estas conductas, pues se deja a un lado los celulares y otros dispositivos, dentro de esta definición de tomando en cuenta la definición de Felipe Villavicencio se puede evidenciar que no está tomando en cuenta lo que es internet, ya que este servicio puede representar un factor importante por el que se puede realizar la conducta o no .

Así mismo María Gabriela Acosta, Merck Milko Benavides, Nelson Patricio García plantean que "los delitos informáticos, son actos ilícitos cometidos mediante el uso inadecuado de la

tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o gadgets" (Acosta, Benavides, & Garcia, 2020). Estos autores dan una definición más enfocada en derecho, así mismo mencionan que este tipo de actos son cometidos mediante el mal uso de la tecnología, es decir que abarca todo lo que a tecnología se refiera, sin embargo al mencionar a que se está atentando contra la información de terceras personas, que se encuentre almacenada en un servidor da a entender que se está refiriendo a una institución o una empresa, la cual trabaja con el uso de los datos de las personas, por lo que no abarca cuando la persona quien va a cometer el acta delictivo lo hará de forma directa, entonces esta definición es un poco más enfocada, al ámbito empresarial o institucional, por otro lado también menciona un aspecto muy importante que debe ser protegida como lo son datos personales ya que estos datos pueden ser objeto de robo, y que con estos mismos se puede suplantar la identidad e incluso robar.

La autora María de la Luz Lima, denomina al delito informático como:

> Un delito electrónico, plantea que el mismo en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin. (Lima, 1984)

Esta definición es más amplia y puede estar sujeta a la interpretación, ya que dicha definición no se limita en cuanto a la forma y el uso que se le puede dar a las computadoras o a la tecnología en sí, al contrario, da una perspectiva más grande de lo que puede llegar a ser considerado como un delito informático.

Importancia y Características

La importancia de tener una definición o percepción de los que son los delitos informáticos radica en tratar de estos tipos de conductas encuadren dentro de un ámbito delictivo, como es de conocimiento las conductas que se realizan por medio de un medio tecnológico, encuadrarían dentro de los delitos informáticos, así mismo como sabemos existen aspectos o fenómenos que harán que el cometimiento de estas conductas ilícitas aumenten o disminuyan.

Fernando Villavicencio Torres indica cuales son las principales características o problemas que se encuentran relacionado dentro del mundo informático y que a través de su desconocimiento se vulnere algún tipo de derechos. Siendo la primera característica "La falta de jerarquía en la red, que permite establecer sistemas de control, lo que dificulta la verificación de la información que circula por este medio" (Terreros, 2014). Esta primera característica da entender que no se le da una debida importancia a los datos que circulan en el internet, por lo que, al no existir el interés suficiente, no se toman medidas para controlar la información lo que ocasiona que la información que circula en la red o dentro del internet no se la pueda categorizar como una fuente confiable o no confiable, ocasionando que las personas accedan a links de internet sin conocer si estos de verdad garantizaran su seguridad al momento de estar visitando tal sitio web. En consideración al no tener un organismo o una institución que ejerza control sobre estos sitios donde reposa la información de los usuarios y que no tengan la seguridad necesaria para su protección, las barreras que estos sistemas usan para su protección sean fácil de acceder para alguien que conozca de informática o programación.

Por otro lado, se encuentra la segunda característica esta más enfocado al aspecto dentro de la sociedad y económico en donde esta menciona que: "El creciente número de usuarios, y la facilidad de acceso al medio tecnológico" (Terreros, 2014). Como se ha podido evidenciar a lo largo de la historia y hasta la actualidad, el mundo y la sociedad se encamina a un mundo en el que gran parte de las actividades que realizamos a diario, se van a poder a realizar a través de un medio tecnológico que tenga acceso a internet. Sin dejar a un lado aquellos aspectos que nacen de forma natural y que no se pueden controlar de alguna u otra manera, un claro ejemplo es la pandemia del COVID - 19 que cambio la forma de vivir de los seres humanos y los acercó más a la tecnología, usándolo como un medio de comunicación, herramienta de trabajo, educación entre otros aspectos que se pueden realizar a través del uso de la tecnología. Esto ocasiono que aumente el número de usuarios que tenían acceso a internet y que de aquí en adelante este número aumente, así mismo en la actualidad existen planes muy económicos para que las personas accedan a este servicio, sin dejar atrás que también existen puntos en donde acceso a internet es gratuito, así mismo existen celulares muy económicos por el cual se pueden conectar a internet.

Así mismo otro problema que encontramos dentro del delito informático, tenemos uno que esta más relacionado al momento en que se comete algún tipo de delito y no se puede

encontrar al responsable de la comisión de dicha conducta esta característica manifiesta que: "El anonimato de los cibernautas que dificulta su persecución tras la comisión de un delito a través de este medio" (Terreros, 2014). Este punto es muy importante analizar debido a que dentro del mundo de internet, poder tener o crearse una cuenta es muy fácil, así mismo se aplica dentro de lo que es la creación de una red social, existen aspectos que pueden que pueden ayudar a identificar si una cuenta es falsa o no, un claro ejemplo es que dentro de las páginas Web lo primero que uno debe percatarse es el nombre de dominio ya que aquellos que falsifican dicho nombre de una página, no lo pueden hacer de igual manera, tendrán que cambiar una letra o aumentar algo. Respecto a los que son redes sociales se lo puede diferenciar por el tiempo en que han sido creadas o por la actividad que han tenido a lo largo de los años, así mismo existe lo que es la verificación, pero solo lo adquieren personas conocidas es decir famosa o que tengan dinero para cancelar dicho valor que cuesta tener esta verificación, con respecto a los correos revisar si es la empresa misma quien lo envía, estos son factores que pueden ayudar a identificar si es una cuenta verdadera o falsa. El anonimato es punto muy importante tener en cuenta ya que como se mencionó se pueden crear cuentas, correos electrónicos, redes sociales, entre otros sin que lo haga con sus verdaderos datos, esto es una ventaja para el delincuente ya que, a través de esto, lo que veo es una brecha o un vacío legal para poder cometer una infracción un claro ejemplo es phishing ya que quien lo realiza lo hace desde el anonimato. El acceso a internet también le ofrece una oportunidad ya que lo puede realizar desde un lugar público en donde se conectan varias personas al día lo que hace difícil su localización, así mismo también se puede conectar a una red ajena a la suya, el vpn también le ofrece una ventaja para poder camuflarse y que no lo puedan encontrar ya que esto le permite conectarse dentro del mismo país, haciendo creer que están fuera o que lo hacen de otro país.

Como último punto tenemos: "La facilidad de acceso a la información para alterar datos, destruir sistemas informáticos" (Terreros, 2014). Este punto esta más relacionado con el aquella persona que comete el delito, pero es necesario tener en cuenta que esta persona tiene un nombre propio y es el hacker:

> Son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables. Conocido como delincuente silencioso o tecnológico. Les gusta indagar por todas partes y conocer el funcionamiento de los sistemas informáticos. Son personas que realizan esta actividad como reto intelectual, sin producir daño alguno con la única finalidad de descifrar y conocer los sistemas informáticos. (Terreros, 2014)

Teniendo en cuenta esta definición es necesario conocer que existen hacker que solo vulneran un sistema informático por afición, y otros que lo hacen como un trabajo ya que lo hacen, para luego vender la información a un tercero. Por otro lado, tenemos a aquellas personas que realizan la sustracción de información por medio de técnicas, dentro de la conducta de phishing tenemos el método o técnica que se realiza para la obtención de datos de una persona

> La ingeniería social es una técnica de ciberataque para obtener información confidencial como datos personales, financieros o contraseñas. También se considera ingeniería social a pedir información de autenticación como usuario y clave como un favor a un compañero de trabajo. (Villegas Cubas, 2021)

Esta definición se relacionado con lo que es la conducta del phishing solo respecto para la obtención de información de todo tipo, por lo que esta técnica es muy utilizada para la el robo de datos, pero esta conducta no se encuentra inmiscuida con lo que es phishing, como su misma palabra lo dice es una técnica que se utiliza para la obtención de datos personales, esto lo hacen haciéndose pasar por otra persona, ya que una vez obtenida la información o datos personales, estos ignoran a la víctima o simplemente lo bloquean.

2.1.7 Perspectiva Criminológica De La Delincuencia Informática

Deducir el significado de perspectiva criminológica es hacer alusión a la delincuencia informática que trata sobre modalidades delictivas realizadas por computador, precisamente en su modo de operar y de sus funciones. Sin embargo, la perspectiva criminológica en la delincuencia informática, también alude al delincuente informático, y a la víctima, puesto que han sido objeto de estudio en la dogmática penal, para comprender los fenómenos de la delincuencia informática y a la vez para su desarrollo.

No obstante, a pesar del significado y las característica que tiene la perspectiva criminológica, hay que enfatizar, que la delincuencia informática y la existencia de conductas integradas, tanto como el objeto material, el bien jurídico, entre otros; existen rasgos comunes que se aproxima a la realidad, pues la dificulta que se debe confrontar para el estudio criminológico en la delincuencia informática, es la falta de datos suficiente, debido a que según experto, las cifras negras que se presenta sosteniblemente, es superior a los demás datos de la criminalidad, siendo así que en los países donde se han descubierto y se

han detectado numerosos casos de delincuencia informática, aseguran que los datos recopilados solo representan la punta del iceberg.

Por lo tanto, para el estudio criminológico de la delincuencia informática, se necesita de otras legislaciones, para tomar medidas que ayuden afrontar y prevenir la delincuencia informática.

El delincuente informático

EL delincuente informático, es aquella persona que tiene la habilidad en el manejo de los sistemas informáticos y es el principal actor de vulneración y obtención de datos personales. Por lo general, la definición de delincuente informático es un tema muy controversial, dado que a lo largo de la historia al delincuente informático se lo ha catalogado como una persona inteligente, motivada que tiene un gran intelecto en el mundo de la informática y no como un delincuente.

Por otro lado, el paradigma delincuente informático, nace de un adolescente inofensivo estadounidense de familia de clase media, que no tenía conocimiento que sus actos fueran ilegales, por lo tanto, se hace mención al síndrome de Robin Hood, porque el delincuente se describía como una persona mayor de edad entre 20 a 30 años, el cual era muy carismático, inteligente, terrorista, que no tenía antecedentes penales y sus ataques solo iban dirigidos a personas adineradas.

Pero esta definición fue cambiando, puesto que, según estudios realizado en 1986 las personas que cometían los delitos más grabes como manipulación, procesamiento de datos, actos de espionaje, eran personas de edad superior que trabajaban en la misma empresa o persona que operaban desde el extranjero, pero que no tenían un gran intelecto en la informática.

Con relación a la convicción sobre el síndrome de Robin Hood, Luis Camacho, sostiene que:

> Se denomina así a la creencia en cierto modo patológica de que mientras que robar a una persona física que tiene sus problemas y necesidades materiales como todo hijo de vecino es un hecho inmoral e imperdonable, robar a una institución como la banca que gana decenas de miles de millones al año es casi un acto social que contribuye a una más justa distribución de la riqueza. (LOSA, 1987)

Es decir que los delincuentes informáticos más se interesan por robar a las personas adineradas y no a las personas de escasos recursos. Sin embargo, existen personas que señalan que esto es un mito, pues hoy en día la gran mayoría de delitos informático se dan en personas de cualquier clase social, por lo tanto, los delitos que se comenten, se enlistan como delito de cuello blanco, porque tienen relación con la criminalidad económica y al phishing, ya que la gran mayoría de los delitos son de estafa.

Es importante mencionar que en la actualidad los delincuentes informáticos utilizan, herramientas alternas como computadoras virtuales y VPN, los cuales le permiten ocultar y a la vez cambiar su dirección IP para que no sean descubiertos.

La víctima

Se refiere a todos lo que han sido afectado mediante un sistema informático, por lo que hace énfasis a las empresas, instituciones publica, compañías de seguro y bancos, dado que, en estos sectores, operan personas jurídicas que tienen un alto tráfico de índice económico.

La mayor víctima en los casos de delitos informáticos son los bancos, puesto que mantienen una gran influencia de personas que tienen sus ahorros en estas empresas. Una cualidad de los ciberataques y que temen los bancos, son las consecuencias desfavorables en su imagen y en su reputación, debido a la gran publicidad emergente que ocasionan los ciberdelincuentes.

Tomando en consideración lo ante mencionado, se sostiene que la gran mayoría de víctimas de ciberataques no son dirigidas a personas naturales, si no a personas jurídicas que son reconocidas, como las grandes empresas.

Respecto al modus operandi Luz Gutiérrez Francés en su libro Fraude informático y estafa, afirma que, “buen número de los delitos vinculados a la informática se deben a la ausencia de medidas de seguridad y de controles adecuados para la protección de los sistemas informáticos” (Francés, 1991). Ya que Frecuentemente los delitos informáticos, ocurren porque estas empresas no cuentan con seguridad suficiente, a causa del costo elevado para mantener su seguridad, o por problemas negligente del programador, lo que ocasiona que la falta de control no sea tan estable a la hora de prevenir los ataques informáticos.

Por otro lado, la falta de denuncia por parte de las víctimas hace que estos delitos no sean tan reconocidos y por lo tanto no se puedan regular, pues se necesita del estudio criminológico y los métodos operandi para desarrollar sistemas y medidas idóneas.

Los Hechos

Los hechos, es evidente que la gran mayoría de delitos criminológico nace de manipulación de computadora, pues de esta se desprende, el hurto, el espionaje, y el sabotaje, lo cuales ocasionan un daño económico mediato e impalpable.

Es importante evidenciar que los fraudes cometidos en la manipulación de computadora se diferencian en:

1. Manipulación de datos de entrada, que trata sobre la sustracción de datos, lo cual es muy común porque es fácil de realizar, pero difícil de encontrar.
2. Manipulación de hardware, que consiste en la manipulación en la unidad principal del procesador, o de la memoria principal donde se almacena los datos.
3. Manipulación de programas, que se basa en la modificación de una aplicación existente con el fin de engañar a su víctima y obtener información. Estos programas son difíciles de detectar, debido a que los ciberdelincuentes son muy cautos a la hora de la creación.
4. Y la manipulación por acceso a la consola, que trata sobre equipos y sistemas alterados por el mal usos en su mecánica, por lo tanto, para su manejo se necesita del uso del hardware para así poder manipular y obtener los datos del equipo.

En relación a los hechos, y con lo antes mencionado existen hechos evidentes donde se utilizan estas manipulaciones, como es el caso del phishing, que, para su manejo y obtención de datos, se necesita de la manipulación del sistema informático, de modo que los ataques se ven reflejado en las empresas y en los bancos, debido al gran índice de personas que estas mantienen.

Descubrimiento y pruebas de los hechos

Los descubrimientos de los delitos informático se dan en países desarrollado, dado que, en aquellos países fue la cuna de la tecnología, de allí por los problemas que estos ocasionaban,

se tomaron medidas, y se comenzó en la creación de normas que permitieron regular cualquier acto ilícito cometido mediante sistema informático.

Por lo tanto, una prueba de los hechos, se puede tomar como referencia a Estados Unidos, puesto que, es uno de los países desarrollado donde más delincuencia informática ha existido a lo largo de la historia, por lo tanto, la experiencia que tiene, en cuanto al estudio de los casos y en los juicios de los ciberdelitos, es muy satisfactoria, en comparación a otros países, por lo que sus estudios en cuento a estos delitos, sirve como guía para las demás legislaciones.

Bien Jurídico Protegido

El bien jurídico protegido, hace referencia a un objeto valioso de protección jurídica que busca preservar, salvaguardar el interés a través de las normativas y sanciones. De tal manera que se cree que el bien jurídico en el contexto de los delitos informáticos puede ser definido como importancia crucial en la sociedad, para el estudio da la estafa o del phishing, dado que en varias legislaciones el bien protegido, en relación al phishing, es la protección de datos personales, y la seguridad Informática contra el acceso ilícito y el uso fraudulente por partes de terceros.

Por ende, debido a que el phishing implica el uso fraudulento de contraseñas, datos confidenciales, con el objetivo de modificar o robar información personal, afectaría la seguridad de los usuarios en líneas, por lo tanto, en consecuencia, a los delitos informáticos, las regulaciones y leyes suelen ser diseñada en tipos penales para de esta manera proteger los bienes jurídicos.

El patrimonio como objeto jurídico del Phishing

En el ámbito de la figura delictiva, el phishing no ingresa como derecho de propiedad, sino como otro elemento del patrimonio, debido a que se asemeja a los delitos de estafa, hurto y robo. Por lo tanto, es necesario señalar que el bien jurídico puede permitir una característica con respecto al patrimonio, de modo que, para el estudio de esta figura se han optado en establecer la diferencia entre los delitos que perjudican a las personas en relación a un bien concreto, y a aquellos que ocasionan una disminución económica del patrimonio.

Es por eso, que la estafa en el ámbito del engaño, el patrimonio que se tutela es universal, mientras que en el hurto y en el robo, existe un carácter factico debido a su relación entre las cosas susceptible pecuniaria y al sujeto.

Tal es el caso que la primera lesión se basa en la disminución patrimonial y la segunda lección para incitar los bienes concreto.

Por ende, el phishing, puede implicar varios problemas en los bienes jurídico, pues el phishing trata de la obtención de datos personales por medio de estafa, lo cual tiene como objetivo vulnerar el patrimonio de una persona para acceder a sus cuentas bancarias.

Para Catalina Fabiola Flores Cáceres el phishing "engloba por sí sola un desvalor, pues es posible vincularlo directamente con bienes jurídicos protegidos por el ordenamiento, sea por significar un peligro o una efectiva vulneración de los mismos (Cáceres, 2017). En virtud a esto, el phishing también se le considera una vulneración al bien jurídico, debido a la manipulación fraudulenta y a las informaciones que los phisher o ciberdelincuentes obtienen. Asimismo, se lo cataloga a las formas de operar, pues los ciberdelincuentes usan programas maliciosos con el único objetivo de obtener datos de sus víctimas.

Por lo tanto, se debe de tener presente, que este delito se ha definido como una conducta reprochable y antijurídica, debido a que perjudica el orden social, no solo atentando al patrimonio si no a la información personal y la intimidad.

2.1.8 Política Criminal

En el ámbito de los delitos informáticos es importante conocer, que los aspectos fundamentales para asegurar que un estado pueda enfrentar eficazmente la delincuencia a través de política criminal es la comprensión y la implementación de estrategias específicas.

Es por esto que ante una necesidad de regular la conductas que con la llegada del internet surgieron, los estados o gobiernos se vieron en la obligación de crear normas que regulen dichas conductas, además que también implementaron estrategias para combatir la ciberdelincuencia, así mismo se crearon instituciones especializadas en materia informática, con el fin de prevenir conductas nuevas que puedan surgir, sancionar a aquellos que vayan en contra de los intereses de gobierno y de la sociedad, además de controlar las acciones que

pueden ejercer sus ciudadanos sin incurrir en la vulneración de derechos de las demás personas con el fin de obtener un beneficio propio.

Es importante tener en cuenta que la política criminal lo puede ejercer un gobierno de forma independente pero también la puede ejercer de forma conjunta con países que tengan una mejor regulación en ciberseguridad y de que medidas toman cuando surgen este tipo de conductas, es decir que también se debe tener en cuenta la cooperación internacional.

Ecuador

Los delitos informáticos en Ecuador se encuentran regulado en una ley específica siendo esta el Código Orgánico integral penal que busca proteger a sus ciudadanos a través de normas que tengan una sanción para quien vulnere derechos de los demás ciudadanos, dentro del mismo se encuentra una sección en la que se detalla varios delitos informáticos entre estos tenemos:

TABLA # 1 DELITOS INFORMÁTICOS DE ECUADOR

Articulo	Tipo penal	Sanción
186	Estafa	5 a 7 años
190	Apropiación fráudenla por medios electrónicos	1 a 3 años
229	Revelación ilegal de base de datos	1 a 3 años
230	Interceptación ilegal de datos	3 a 5 años
231	Transferencia electrónica de activo patrimonial	3 a 5 años
232	Ataque a la integridad de sistemas informáticos	3 a 5 años
233	Delitos contra la información pública reservada legalmente	5 a 7 años
234	Acceso no consentido a un sistema informático, telemático o de comunicaciones	3 a 5 años
234.1	Falsificación informática	3 a 5 años

Elaborado por: Autores **Fuente:** COIP

Por otro lado, la fiscalía también goza del apoyo dentro de la policía nacional de una Unidad especializada para la investigación del cometimiento de este tipo delitos, esta se la denomina la Unidad De Delitos informáticos y Tecnológicos. Esta unidad ayuda en la persecución de los infractores además que también forma y brinda capacitación especializada en todo lo

referente a la ciberseguridad y delitos informáticos, esta también es la encargada de desarrollar protocolos de seguridad para combatir la delincuencia en el ciberespacio.

Ecuador es participe de varias iniciativas para la cooperación internacional, esto lo realiza con el fin de colaborar con otros países.

Argentina

De igual forma en Argentina se encuentra regulado todo tipo de delito informático en su código penal, entre los delitos que se encuentran tipificados en la legislación argentina tenemos:

TABLA # 2 DELITOS INFORMÁTICOS DE ARGENTINA

Artículo	Tipo penal	Sanción
153	Acceso ilegitimo a sistemas informáticos	15 días a 6 meses
157	Falsificación informática	1 mes a 2 años
172 173	Estafa	1 mes a 6 años

Elaborado por: Autores **Fuente:** Código penal de Argentina

Este se encuentra suscripto al convenio de Budapest, en el cual se tratan varios aspectos referentes a la ciberseguridad, en cual se establecen definiciones, pautas para regular las conductas ilícitas además de la colaboración internacional entre sus países miembros.

Argentina ha dispuesto varias instituciones en la cual, los ciudadanos pueden interponer sus denuncias, cuando hayan sido víctimas de un delito informático, estas instituciones son:

- Unidad Fiscal Especializada en Ciberdelincuencia (UFECI)
- Centro de Asistencia a las Víctimas de Delitos (CENAVID).
- Dirección Nacional de Protección de Datos Personales
- Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFED y CI)

Cada una de estas instituciones se encuentran dentro de su portal web en la cual también se pone a conocimiento sus números celulares, dirección y su respectivo correo para reportar si ha sido víctima de un delito informático. Dentro de su portal Web de la nación argentina, su

ministerio de justicia ha puesto en conocimiento una sección de definiciones para cada uno de los delitos informáticos, también se encuentra un link de reporte de páginas que no son confiables o que han sido diseñadas con el fin o la práctica del Phishing, pone a disposición un reporte o formulario de enlaces de Google.

España

Dentro del código penal español se establecen normas que ayudan a regular los delitos informáticos para la protección de sus ciudadanos, estos son:

TABLA # 3 DELITOS INFORMÁTICOS DE ESPAÑA

Artículo	Tipo penal	Sanción
248	Estafa	1 a 3 meses
255	Fraude informático	3 a 12 meses

Elaborado por: Autores **Fuente:** Código penal español

Las instituciones que ayudan a regular este tipo de delitos en España son:

- Brigada Central de Investigación Tecnológica (BCIT) de la Policía Nacional.
- Grupo de Delitos Telemáticos (GDT) de la Guardia Civil.

Siendo la primera la encargada de investigar y perseguir a los delincuentes informáticos y presentarlo a la justicia para que sean sancionados, por otro lado el Grupo de delitos informáticos de la guardia civil es una instituciones de apoyo para la investigación de los delitos que comentan a través de los medios electrónicos y del ciberespacio, esta institución también realiza patrullas en la red para que sus usuarios naveguen de forma segura a través del internet, ambas instituciones tienen su respectivo portal web en donde dan a conocer todas sus atribuciones y funciones. España al realizar patrullajes en los portales web permite identificar un sin número de páginas maliciosas por lo que su índice que registro frente a los delitos informáticos es mayor ya que detectan la mayoría de delitos a tiempo.

2.1.9 Ley De Datos Personales

La ley de datos personales es una normativa legal, que establece principios, derechos y obligaciones con el objetivo de proteger la privacidad de los individuos con respecto a su

información personal. Se caracteriza por su definición, principios, derechos de los titulares y por sus obligaciones.

Es así que, en Ecuador la ley de datos se la conocen, como Ley Orgánica de Protección de Datos Personales, y se fundamenta en la protección de los derechos de privacidad de los individuos y regulación al manejo adecuado, en cuanto a sus datos personales, promoviendo así la confianza y la seguridad en el entorno digital.

En Argentina, como Ley de Protección de los Datos Personales, que se justifica en proteger la privacidad de los individuos y establecer los principios y procedimientos que deben seguir las entidades públicas y privadas al recolectar, procesar, almacenar y compartir datos personales.

En España, como Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales que estipula que su objetivo general es actualizar y adaptar normativas legales en su Reglamento General de Protección de Datos para fortalecer los derechos de sus ciudadanos

2.2 Marco legal

Constitución De La República Del Ecuador

La constitución del Ecuador del año 2008, fue propuesta por el entonces presidente de la Republica Rafael Correa Delgado, esta fue redactada por la Asamblea constituyente que sesiono en el 2007 y 2008, entrando en vigor el 10 de octubre del mismo año. Esta constitución se diferencia de los anteriores cuerpos normativos, al establecer que el Ecuador es un estado constitucional de derechos y de justicia, además de que es un estado independiente, plurinacional y laico entre otras características que hacen que sea una constitución garantista de derechos además que esta constitución busca que exista una armonía entre los derechos de los ciudadanos y de la naturaleza, por eso también se hace referencia a que es un constitución verde por estos aspectos que toma ante la naturaleza.

Uno de los derechos que se establecen en la Constitución es el de la protección de datos personales, ya estos al ser datos que manejan los usuarios, y la filtración de sus datos

conllevaría a una vulneración de derechos, es por eso que en el siguiente artículo se establece lo siguiente:

> Art. 66.- Se reconoce y garantizará a las personas:
> 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

El derecho a la protección de datos personales busca que aquella información que se maneja por el mundo del internet o que son manejados por una empresa, lo hagan de una manera correcta, ya que estos datos son puestos a manos de un tercero para que se encargue de su protección, es por eso que la seguridad que manejen estas empresas, paginas, aplicaciones entre otras instituciones que trabajen con el almacenamiento de datos, deben poseer una seguridad alta para así evitar la fuga de estos datos manteniendo la confidencialidad y la protección de datos.

Constitución de la Nación Argentina

Argentina adoptó su primera constitución en el año 1853 la cual tenía el nombre de confederación de Argentina, esta constitución ha sido reformando a lo largo de todos estos años, la última reforma fue en el año de 1994 la cual tuvo como nombre Constitución de la nación de argentina, en esta última se reconocieron derechos humanos, aspectos que ayudaban a mantener la paz interna, además que también se adoptaron cambios en su forma de gobierno entre otros temas. Esta constitución más actualizada protege los datos de una persona.

> Artículo 43. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.

Dentro de este articulado el derecho a la protección de datos personales no solo tiene una postura en la que reconoce este derecho, sino que a su vez le da la potestad de interponga una acción para la protección de datos personales, así mismo también permite la actualización de los mismos, su protección no solo se centra en aquellos datos que reposan en alguna institución pública, se busca que tanto la pública y la privada protejan de igual

manera, sin que exista discriminación alguna, al momento de reclamar el cumplimiento de este derecho constitucional.

Por otro lado, permite que los ciudadanos interpongan acciones judiciales para la protección de los mismos, basado en el principio de consentimiento ya que sin dicho consentimiento se vulnerarían más derechos como la privacidad, accesibilidad entre otros.

Constitución Española

La Constitución Española enmendada el 31 de octubre de 1978 por LAS CORTES GENERALES y ratificada el 29 de diciembre del mismo año, es una constitución garantista de normas, derechos fundamentales y libertades públicas, de principios elemental frente a los poderes públicos, y de organización institucional y territorial del estado, que ayudan a fundamentar el reconocimiento de los valores democrático, la libertad, justicia, igualdad y pluralismo político de los derechos autónomo de las nacionalidades y regionales que la integran.

Por lo tanto, la Constitución Española al tener un cuerpo normativo amplio, que protege a las personas naturales y jurídicas, ayuda a que los problemas que existen en la actualidad vinculada a los datos personales y digitales, se regulen bajo el concepto del siguiente artículo:

> Art 18. Derecho a la intimidad Inviolabilidad del domicilio
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

En consecuencia, el artículo 18.4 de la constitución, ayuda a prevenir el robo de datos, que se exponen a la hora de comprar por internet, de emitir una factura electrónica, realizar marketing, el envío de correos o mensaje instantáneo, todo lo que implique intercambio de datos personales, a fin de preservar los derechos de los niños, jóvenes, adolescentes, adultos, adultos mayores y personas fallecidas.

Convenio De Budapest

El convenio de Budapest, es un tratado internacional, creado en el año 2001 por el consejo de Europa, que trata de establecer directrices para contrarrestar los delitos informáticos de los países y estados que la conforma, además ayuda a que estos países cooperen

internacionalmente y generen nuevos marcos legales armónico en caso de un ataque cibernético.

Este convenio que entró en vigor en el año 2004, actualmente está conformado por 66 países entre ellos Argentina y España, por lo que el Ecuador no se encuentra suscrito en este tratado internacional, que se enfoca en dar recomendaciones basado en los derechos humano, protegiendo la seguridad informática, los datos personales, la propiedad intelectual, y que establece medidas preventivas y punibles para cualquier clase de delitos informático como la sustracción de datos personales, acceso no autorizado y la vulneración de información personal.

Es importante señalar que, los países que conforma este convenio se comprometen a cooperar en la investigación y el enjuiciamiento en relación a los delitos informáticos, que son importante para erradicar los problemas de un mundo que cada vez se vuelve más interconectado.

En referencia al delito de la estafa cibernética o phishing, este convenio habla de las generalidades de los delitos informático por lo tanto los artículos que se asemejan son los siguientes:

> Articulo 4 - Ataques a la integridad de los datos
> 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.
> 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.
> Articulo 5 - Ataques a la integridad del sistema
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
> Artículo 7 - Falsificación informática
> Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Estos artículos establecen, que cada país debe de tener medidas legislativas con respecto a la criminalización de la interferencia ilícita en relación al phishing, que trata de borrar, dañar o suprimir datos, al momento de atacar, además nos muestra que este convenio constituye un rol importante a la hora de adoptar medidas que se sean necesarias para combatir la ciberdelincuencia que emanan los países que conforman el convenio. y a la vez buscando contrarrestar y enunciando que cualquier ataque de índole cibernético sea de intención dolosa debido a que lo ciberdelincuente saben de los problemas que pueden ocasionar.

Como finalidad se puede afirmar que el Art 4, 5 y 7 del convenio de Budapest tiene relación con la estafa debido que el phishing se trata de la falsificación alteración y ataques de datos informático con el único objetivo de obtener todos tus datos personales para luego alterarlas o extorsionar.

Código Orgánico integral Penal (Ecuador)

El código orgánico integral penal que entró en vigencia el 10 de febrero de 2014, con este código se busca proteger aspectos importantes como lo son la seguridad jurídica, ya que este código proporciona un marco legal que es de fácil entendimiento, así mismo busca proteger todos los derechos humanos que se encuentran consagrados en la constitución a través del ius puniendi, por otro lado, también busca prevenir y sancionar delitos a futuro.

> Art. 186.- 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:
> 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.

El código orgánico integral penal en su artículo 186 se encuentra tipificado el delito de estafa esta acción es realizada por una persona para su propio beneficio o el de un tercero, este delito consiste inducir a la persona a que realice un acto en concreto, y que este le pueda perjudicar, dentro de este artículo se encuentran agravantes que serán sancionada con el máximo de la pena, en su numeral dos se hace referencia al cometimiento de esta conducta por medio de los dispositivos electrónicos sin embargo en este numeral se es claro al

mencionar que este se aplicara cuando se trate de un cajero automático, por lo que no habla de forma clara de lo que vendría a ser el phishing, pero es importante mencionar que dentro de este artículo se encuentran varios aspectos importantes como son los verbos rectores que permiten identificar o encuadrar un tipo penal.

> 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.

Por otro lado, el articulo 190 es el que más se asemeja a la conducta del phishing cubre en su mayoría lo que el delito de estafa no lo hace, pero se está dejando a un lado el uso de las redes sociales, ya al hacer mención a las redes electrónicas dan a entender a la infraestructura que esta tiene para poder comunicarse con otro tipo de red. Es importante conocer que esta conducta no busca solo apropiarse de un bien, sino que también busca el recolectar información para posterior suplantar la identidad, o una vez obtenido los datos personales aplicar la ingeniería social para poder obtener un beneficio.

> Art. 230.- Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:
>
> 2. La persona que ilegítimamente diseñe, desarrolle, ejecute, produzca, programe o envíe contenido digital, códigos de accesos o contraseñas, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente al que quiere acceder.

El articulado 230 en su numeral dos sobre la interceptación ilegal de datos, establece una pena severa para aquellos que comentan este tipo de delitos. Lo que más busca proteger es la integridad y la seguridad de información que reposa dentro de un sistema informático, en dicho articulado se encuentran establecidos varios verbos rectores, con el fin regular de una mejor forma los actos ilícitos que de estas puedan desarrollarse, teniendo en cuentas varios aspectos.

La parte más fundamental dentro de este articulado teniendo en cuenta la conducta del phishing, es la de inducir o redirigir a una persona a otra dirección que no sea la original, por lo que el spam o correos malicioso serian un claro ejemplo de conductas que son reguladas dentro de este artículo.

> 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.

Este artículo se centra en el acceso no consentido a un sistema informático, esta normativa busca proteger los derechos de las personas o ciudadanos que se encuentren navegando a través de un portal web, que se supone que es seguro, sin embargo, al ser tan idéntico que el portal web original es difícil diferenciarlos, por lo que estas normas regulan este tipo de conductas que las puede realizar un delincuente informático para su beneficio, debido a que en los portales web manejan un sin número de información personal para aquellos que gran parte de sus acciones diarias lo realizan a través de internet o de los portales web, por lo que el objetivo de este artículo es salvaguardar la protección a los datos personales.

Código Penal De La Nación Argentina

El código penal de argentina entro en vigencia en el año de 1922 sin embargo este código ha tenido varias reformas a lo largo de todos estos años, y estas reformas han ayudado a que se regule ciertas conductas, la ley 26.388 del código penal fue sancionada en el 4 de junio de 2008 y fue promulgada de hecho el 24 de junio del mismo año, este código penal argentino trajo reformas en el derecho informático tratando de compensar ciertos vacíos legales que la ley anterior no regulaba.

> ARTICULO 172. - Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño.

En el código penal de Argentina en artículo 172, se detalla de una forma diferente a lo vendría a ser el delito de estafa en Ecuador, por otro lado, también se está dejando a un lado la intervención de un tercero.

> ARTICULO 173.- Sin perjuicio de la disposición general del artículo precedente, se considerarán casos especiales de defraudación y sufrirán la pena que él establece:
>
> 15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no autorizado de sus datos, aunque lo hiciere por medio de una operación automática.
>
> 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

En el artículo 173 en su numeral 15 también establece el tipo de defraudación de que se puede cometer por medio del robo de una tarjeta de crédito, falsificación, perdida entre otras formas por las cuales puedan obtener la misma. Además, en este numeral no se toman en cuenta aquellas técnicas de puedan llevar a cabo por medio de un cajero automático.

Del mismo modo, el numeral 16 de dicho artículo solo hace mención al funcionamiento de un sistema informático y la transición de datos, se deja a un lado varios aspectos que, si cubre la legislación ecuatoriana, sin embargo, en esta tampoco se menciona nada referente al uso de las redes sociales.

Código Penal (España)

El código penal español que entró en vigencia el 24 de mayo de 1996, en el transcurso de los años ha sufrido modificaciones debido a los nuevos delitos que se presentan cotidianamente. Eventualmente se puede evidenciar, que, en la actualidad, el avance tecnológico ha creado nuevas clases de delitos, como lo son la estafas y robos de datos personales por medio del internet, lo que ha generado, que el código penal español implemente o que utilice los siguientes artículos:

> Artículo 248.1
> Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

El artículo 248, hace alusión a la estafa clásica, que en el delito informático esta se implementa por las técnicas de ingeniería social que busca engañar a las personas vía mensajería instantánea, llamada o por correos electrónico, con la única finalidad de obtener información de la víctima, poder instalar un malware, o para ingresar en sus cuentas bancaria, todo esto se le conoces como phishing.

> Artículo 249
>
> 1. También se consideran reos de estafa y serán castigados con la pena de prisión de seis meses a tres años:
>
> a) Los que, con ánimo de lucro, obstaculizando o interfiriendo indebidamente en el funcionamiento de un sistema de información o introduciendo, alterando, borrando, transmitiendo o suprimiendo indebidamente datos informáticos o valiéndose de cualquier otra manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

De igual manera el artículo 249.1.a menciona el delito de estafa dentro del ámbito informático y a su vez establece la prisión que puede obtener el ciberdelincuente si comenten esta clase de delito. Lo que implica que esta ley también se puede sancionar el delito informático phishing debido a que se considera un delito mutable y tiene relación con la estafa clásica y la estafa informática.

2.3 Marco conceptual

Datos personales: Es aquella información que permite identificar a una persona, estos datos pueden ser nombre, dirección, correos electrónicos, cuentas bancarias, entre otros que en lo que reposen datos personales de una persona tanto de forma directa como indirecta.

Tratamiento: Es la operación en que se realice para tratar, organizar, estructuración, extracción, consultas, uso, difusión entre otros métodos que impliquen el manejo de datos personales, estos pueden ser tratado mediante la autorización del titular o no.

Titular: Persona física de las cual se obtiene los datos, así mismo también puede ser la persona jurídica de la cual se obtengan datos.

Tercero: Persona ajena que busca obtener algo para su beneficio, no tiene nada que ver con el titular ni con la persona que maneja los datos para su debida protección.

Acción: Medida que toma una persona ya sea judicial o administrativa para hacer un reclamo y que se respeten sus derechos.

Consentimiento: Es el permiso que otorga el titular de forma voluntaria a que sus datos sean tratados de una forma correcta.

Informática: Ciencia que estudia el desarrollo de nuevas tecnologías de forma tangible e intangible de un sistema informático y de cómo se aplican en la computación.

Ataque cibernético: Es un intento intencionado por el cual un tercero de forma deliberada busca burlar, dañar y acceder a un sistema de forma ilegal e ilegítima con el fin de obtener un beneficio para sí mismo.

Phishing: Es una conducta delictiva por el cual un delincuente informático busca mediante el engaño, que las personas accedan a un enlace con el fin de que las víctimas revelen información personal.

Sistema informático: Conjunto que forman el ser humano, hardware y software, para procesar, almacenar y manipular la información

Redes electrónicas: Sistema de comunicación por el cual se transfiere la información desde una computadora a los servidores, estos lo pueden hacer de forma limitada en un espacio a través de una red LAM (Local), mientras que la red WAM permite que la información se transfiera de forma más amplia, que viaje de un continente a otra.

Ardid: Medio desconocido por el cual busca cumplir su objetivo, Artimaña que ha encontrado para conseguir algo para su beneficio.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Diseño y tipo de investigación

La presente investigación denominada el phishing como delito informático se lo realizo mediante un enfoque de investigación cualitativa, la cual permitió explicar las similitudes y diferencias del fenómeno de los delitos informáticos de las legislaciones de Ecuador, Argentina y España, respecto a la nueva conducta delictiva que nacen por el avance de la tecnología.

Es así, que, mediante una observación a través de sus normativas, se permitió apreciar la falta de tipicidad y especificidad, de Ecuador a diferencia de Argentina y España, en cuento al nuevo comportamiento de los delitos informáticos relacionado al phishing. Ya que los derechos que se encuentran reconocidos en la carta magna del Ecuador y las nuevas acciones, vulneran los derechos de protección de datos personales, intimidad y a la vida privada misma que se encuentra garantizados, de modo que se analizó y comparo las legislaciones de Argentina y España que tratan de este tema y de sus políticas criminales.

Asimismo, este proyecto de investigación se lo realizo mediante un estudio de carácter exploratorio, ya que este tema es muy poco investigado y analizado por lo que fue necesario realizar una investigación a fondo respecto al phishing, y de los nuevos hábitos informáticos que necesitan ser regulados. Por lo cual este proyecto de investigación significo un tema novedoso a la hora del estudio ya que se basó en la investigación del mundo informático.

Bajo este concepto el autor Carlos Méndez define lo siguiente:

> El estudio exploratorio tiene una utilidad especial: permite al investigador formular hipótesis de primero y segundos grados, las cuales pueden ser relevantes en el nivel más profundo del estudio propuesto; se considera una etapa de inicio en la investigación. En la práctica es más difícil, pues es la iniciación en el conocimiento científico. (Carlos Eduardo Méndez Álvarez, 1995)

3.2 Recolección de información

El presente proyecto de investigación Titulado "EL PHISHING COMO DELITO INFORMÁTICO EN EL ÁMBITO DE LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y ESPAÑA, 2023". Se estableció que la población que se ponderó, fue las normas de cada uno de los respectivos países Argentina, Ecuador y España para realizar un estudio comparado, el cual se consideraron aspectos sociales, histórico, jurídico de conformidad con el delito informático phishing.

Dentro de la muestra, se utilizó la muestra no probabilística, el cual se divide en tres aspectos, criterio, conveniencia y cuotas. En el que el tipo de investigación que se consideró para este presente estudio, fue la conveniencia por la facilidad al acceso a la información y por las normas que constituyen un conjunto de población absoluta.

En el libro "Guía Metodológica de proyectos de investigación social" determina la muestra por conveniencia "como muestra en función de los intereses del objeto de estudio, en función de accesibilidad y a la conveniencia" (GALLO & TOMALA, 2015). Haciendo así alusión al método, que se usó para esta investigación.

TABLA # 4 POBLACIÓN Y MUESTRA

Constitución de la República del Ecuador	1
Código Orgánico integral Penal (Ecuador)	1
Constitución de la Nación Argentina	1
Código Penal de la Nación Argentina	1
Ley 26.388 de Delito informático (Argentina)	1
Constitución Española	1
Código Penal (España)	1
Convenio Budapest	1
TOTAL	8

Elaborado: David Suárez L – Ernesto Rocafuerte del P.

Además, dentro del proyecto de investigación se aplicó el método comparado, puesto que el mencionado método fue ideal para poder realizar esta investigación, el cual permitió destacar y clasificar cuestiones que surgen de la comparación de los cuerpos normativos de Ecuador, España y Argentina, es así que se tuvo en cuenta sus normas constitucionales, para identificar donde están ubicado los derechos de los ciudadanos, del mismo modo los cuerpos penales,

como las normas sancionatorias para determinar donde se encuentran aquellas conductas y asimismo, se contrasto las leyes de protección de datos con el fin de conocer los principios generales. Es importante hacer mención que para este método se recurrió a dos fases la primera la observación del problema jurídico y la segunda etapa la comparación.

Tal como lo describe el Dr. Carlos Manuel Villabella Armengo, "El método de derecho comparado, permite cotejar dos objetivos jurídicos pertenecientes a un mismo dominio, tales como conceptos, instituciones, normas, procedimientos, entre otros. Lo cual posibilita destacar semejanzas, establecer clasificaciones y descubrir tendencias" (Armengo, 2015).

De igual manera se empleó, el método exegético jurídico ya que este método, consiste en el análisis de documento o normas legales mediante revisión en su redacción y regulación, es decir, que el método exegético en está presente investigación, se orientó al análisis profundo de las normas legales, lo que lo hizo muy esencial, para recabar información jurídica de las legislaciones de Ecuador, Argentina y España, considerando los requisitos y reglas gramaticales que ayudo a evitar errores o alteraciones en la presente investigación, a fin de lograr un entendimiento más claro y accesible al lector.

Bajo esta perspectiva, se adoptó la técnica de comparación, debido a que el estudio de investigación, se fundamentó en la comparación de normas penales, constitucionales y leyes conexas, para la identificación de aspectos similares relacionas al phishing. También se empleó la técnica documental que se centra en examinar los textos, bibliografía desde un punto de vista social, doctrinario y legislativo en fuentes confidenciales, por lo tanto, esta técnica permito entender la recopilación de información, compresión del análisis jurídico del Phishing como delito informático en el Ámbito de las Legislaciones de Ecuador, Argentina y España, y así mismo ayudo a conocer los progresos en cuanto a la disminución de los delitos de phishing.

3.3 Tratamiento de información

El presente estudio comparativo se desarrolló mediante ficha bibliográfica, revista científicas, libros, fuentes doctrinarias y citas, con el fin de obtener un análisis estructurado de la investigación. Por otro lado, mediante el instrumento de comparación exegético se logró recabar información jurídica sobre el delito informático phishing, en las legislaciones de Ecuador, Argentina y España, en la que se sustentó la comparación de sus normativas,

del mismo modo se desarrolló una matriz de comparación de las tres legislaciones permitiendo identificar la diferencias y semejanzas de cada uno de los países.

En base a estas técnicas, instrumento, y métodos, se logró este proyecto de estudio.

3.4 Operacionalización De Variables

TABLA # 5 OPERACIONALIZACIÓN DE VARIABLES

Titulo	Variables	Conceptos	Dimensiones	Indicadores	Ítems	Técnica
EL PHISHING COMO DELITO INFORMÁTICO EN EL ÁMBITO DE LAS LEGISLACIONES DE ECUADOR, ARGENTINA Y ESPAÑA, 2023	Variable independiente: El phishing como delito informático	El phishing es una técnica maliciosa utilizada por ciberdelincuentes para engañar a usuarios de internet y obtener información confidencial, como contraseñas, información financiera, datos personales, o incluso acceso a sistemas informáticos. Este tipo de ataque se lleva a cabo mediante el envío de mensajes electrónicos fraudulentos, como correos electrónicos, mensajes de texto o llamadas telefónicas, que parecen ser legítimos y provienen de fuentes confiables, como bancos, empresas, organizaciones	Marco constitucional y legal	Derechos relacionados a la protección de datos personales	Derecho a la intimidad y vida privada	Matriz de comparación
					Derecho a la protección de los datos personales	Matriz de comparación
				Principios que regulan la protección de los datos personales	Consentimiento	Matriz de comparación
					Finalidad	Matriz de comparación
					Calidad de datos	Matriz de comparación
					Seguridad	Matriz de comparación
					Confidencialidad	Matriz de comparación
					Responsabilidad	Matriz de comparación
					Acceso y rectificación	Matriz de comparación
					Exactitud y Limitación	Matriz de comparación
					Rendición de cuentas	Matriz de comparación
			Marco internacional	Convenios internacionales vinculados a la protección de los datos personales	Convenio de Budapest	Matriz de comparación

		gubernamentales o servicios en línea.	Tipo penal	Origen	Antecedentes	Matriz de comparación
				Elementos subjetivos del tipo penal	Dolo/culpa	Matriz de comparación
				Elementos Objetivos del tipo penal	Denominación del tipo penal	Matriz de comparación
					Verbo rector	Matriz de comparación
					Bien Jurídico	Matriz de comparación
					Sanción	Matriz de comparación
					Sujeto Activo	Matriz de comparación
					Sujeto Pasivo	Matriz de comparación
			Métodos de ataques en relación al delito informático phishing	Tipos de métodos	¿Cuáles son los métodos más eficientes para el cometimiento de este delito?	Ficha Bibliográfica
				Tipicidad en los ataques	¿Qué tan eficaz es la regulación de las legislaciones de ecuador, argentina y España, ¿en relación a los delitos informáticos?	Ficha Bibliográfica
				Tasa de ataques	¿Cómo se ha incrementado los ataques informáticos en la actualidad?	Ficha Bibliográfica
				Efecto en la privacidad	¿Cómo los ataques informáticos, perjudican la privacidad de las personas?	Ficha Bibliográfica

Elaborado por: Autores

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. Análisis, interpretación y discusión de resultados.

TABLA # 6 CUADRO COMPARATIVO – DERECHO CONSTITUCIONAL

Criterio	Conceptualización	Ecuador	Argentina	España
Marco constitucional	Protección de los derechos que se encuentran reconocido en cada una de las constituciones y que son objeto de protección por parte de los estados.	El artículo 66 -referente a los derechos a la Intimidad y a la Privacidad: Este artículo establece que "se reconoce y garantizará el derecho a la intimidad y a la privacidad, así como a la protección de los datos personales". Además, especifica que la intimidad y la privacidad de las personas son inviolables, y que ninguna autoridad puede vulnerar estos derechos.	Artículo 43. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos.	La Constitución reconoce el derecho a la intimidad personal y familiar en su artículo 18, así como el domicilio y la correspondencia. Este derecho puede interpretarse como una base para la protección de la privacidad y los datos personales de los ciudadanos.
		En el artículo 66, se establece que "la protección de datos personales será garantizada". Esto implica que el Estado ecuatoriano tiene la obligación de establecer medidas legales y administrativas para proteger la privacidad y seguridad de la información personal de los ciudadanos.	Art 43. Este artículo reconoce el derecho de los ciudadanos a la protección de datos personales y la posibilidad de acceder a la información que se encuentre en poder del Estado.	Art 18. Derecho a la intimidad Inviolabilidad del domicilio. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.
Análisis: El marco constitucional de las legislaciones de Ecuador, Argentina y España, establecen principios generales de derechos a la protección de datos personales, sin embargo, se diferencia en la interpretación, puesto que cada legislación tiene sus propios fundamentos.				

Elaborado por: Autores

TABLA # 7 CUADRO COMPARATIVO – MARCO LEGAL (PRINCIPIOS)

Criterio	Conceptualización	Ecuador	Argentina	España
Marco Legal	Principios que se establecen en las leyes para regular la protección, uso y tratamiento de los datos personales	Consentimiento: La ley establece que el tratamiento de datos personales debe basarse en el consentimiento libre, específico, informado e inequívoco del titular de los datos. Esto significa que las personas deben otorgar su autorización expresa para que sus datos sean recopilados, procesados o utilizados.	Calidad de los datos: La ley establece que los datos personales deben ser exactos, completos, actualizados y relevantes para los fines para los que fueron recopilados. Se deben optar acciones apropiadas para asegurar la exactitud y la integridad de los datos personales.	Principio de legalidad, lealtad y transparencia: El tratamiento de datos personales debe realizarse de manera legal, leal y transparente para el titular de los datos. Esto implica que el tratamiento debe basarse en una base legal específica y que el titular debe ser informado de manera clara y comprensible sobre cómo se utilizarán sus datos.
		Finalidad: Los datos personales solo pueden ser recopilados y tratados para fines determinados, explícitos y legítimos. No se pueden utilizar para propósitos incompatibles con aquellos para los que fueron recogidos inicialmente, a menos que exista consentimiento adicional del titular o una disposición legal que lo permita.	Consentimiento: El principio del consentimiento establece que el tratamiento de datos personales solo puede llevarse a cabo con el consentimiento libre, expreso e informado del titular de los datos. Esto significa que las personas deben ser informadas sobre cómo se utilizarán sus datos y deben dar su consentimiento activo para su procesamiento	Principio de limitación de la finalidad: Los datos personales deben recogerse con fines específicos, explícitos y legítimos, y no deben tratarse de manera incompatible con dichos fines. Esto significa que los datos solo deben utilizarse para los fines para los que fueron recopilados inicialmente.
		Confidencialidad: Se establece la obligación de mantener la confidencialidad de los datos personales, tanto durante su tratamiento como después de finalizado el mismo. Esto implica que los	Información: Al recopilar datos personales, se debe informar a los titulares sobre: la finalidad y destinatarios, la existencia y responsable del	Principio de minimización de datos: Se debe limitar la cantidad de datos personales recogidos a lo estrictamente necesario para cumplir con los fines establecidos. Esto implica que se deben recoger solo los datos que sean

		datos solo pueden ser divulgados a personas autorizadas y en los casos permitidos por la ley.	archivo, la obligatoriedad de las respuestas, las consecuencias de proporcionar o negar datos, y los derechos sobre los datos.	pertinentes, adecuados y limitados a lo necesario en relación con los fines para los que son tratados.
		Calidad y exactitud de los datos: La ley establece que los datos personales deben ser exactos, completos, actualizados y pertinentes en relación con los fines para los que fueron recopilados. Se deben tomar medidas razonables para garantizar la precisión y la integridad de la información personal	Seguridad de los datos: El responsable debe asegurar la seguridad y confidencialidad de los datos personales, evitando su adulteración, pérdida o uso no autorizado. Está prohibido registrar datos personales en sistemas que no garanticen integridad y seguridad.	Principio de exactitud: Los datos personales deben ser precisos y estar actualizados. Se deben tomar medidas razonables para garantizar que los datos inexactos se rectifiquen o se eliminen sin demora.
		seguridad: Se requiere que los responsables del tratamiento de datos implementen medidas técnicas, organizativas y legales adecuadas para garantizar la seguridad de los datos personales y prevenir su alteración, pérdida, acceso no autorizado o cualquier otra forma de tratamiento indebido	Confidencialidad: Los datos personales deben ser tratados con confidencialidad y no pueden ser divulgados o transferidos a terceros sin el consentimiento del titular, salvo en los casos permitidos por la ley.	Principio de limitación de la conservación: Los datos personales deben conservarse durante el tiempo necesario para cumplir con los fines para los que fueron recogidos. Esto implica que los datos deben ser eliminados o anonimizados una vez que ya no sean necesarios para dichos fines.
		responsabilidad: Los responsables del tratamiento de datos son responsables de cumplir con los principios y disposiciones de la ley. Deben demostrar que están en conformidad con la normativa de protección de datos y ser capaces de rendir	Cesión: Los datos personales solo pueden ser cedidos con el consentimiento del titular, salvo excepciones establecidas por ley. El cesionario debe cumplir las	Principio de integridad y confidencialidad: Los datos personales deben tratarse de manera segura, protegiéndolos contra el acceso no autorizado o su divulgación. Se deben implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos.

		cuentas por su cumplimiento.	mismas obligaciones legales que el cedente y se debe preservar la identidad de los titulares en ciertos casos.	
			Responsabilidad: Los responsables del tratamiento de datos son responsables de cumplir con los principios y disposiciones de la ley. Deben adoptar políticas y procedimientos internos para garantizar el cumplimiento de la normativa de protección de datos.	Responsabilidad y rendición de cuentas: Los responsables del tratamiento de datos son responsables de cumplir con los principios de protección de datos. Deben ser capaces de demostrar el cumplimiento de estos principios y estar preparados para rendir cuentas ante las autoridades de protección de datos.
Análisis: En lo referente al marco legal, los principios que proporciona la protección de datos, se pueden evidencia que Ecuador y argentina, tienen similitud, tanto en el consentimiento, seguridad, y responsabilidad, mientras que España su estructura de estos principios es más amplia por los reglamento y leyes que han implementado a lo largo de los años.				

Elaborado por: Autores

TABLA # 8 CUADRO COMPARATIVO CONVENIOS INTERNACIONALES

Criterio	Conceptualización	Ecuador	Argentina	España
Convenios internacionales vinculados a la protección de los datos personales	El convenio de Budapest es un tratado internacional que se centra en la creación de parámetros y medidas que se deben seguir cuando se es víctima de un ciberdelito.	No forma parte del convenio de Budapest	forma parte del convenio de Budapest desde 2017	forma parte del convenio de Budapest desde 2010
Análisis: Respecto a los convenios internacionales vinculados a la protección de los datos personales, Budapest es uno de los convenios internacionales de la ciberseguridad, que Argentina y España forman parte. En cambio, Ecuador es uno de los países que aún se encuentra en fase de evaluación para adherirse a este convenio, debido a que implicaría un cambio radical para el derecho informático.				

Elaborado por: Autores

TABLA # 9 CUADRO COMPARATIVO – ANTECEDENTES DEL TIPO PENAL

Criterio	Conceptualización	Ecuador	Argentina	España
Antecedentes	Conocer los antecedentes de cuando los países fueron implementando artículos penales que regulen la conducta en el ámbito de los delitos informáticos.	Los delitos informáticos comenzaron a regularse formalmente con la promulgación del Código Orgánico Integral Penal (COIP), que entró en vigencia el 10 de agosto de 2014. El COIP incluyó una sección específica sobre delitos informáticos, estableciendo las bases legales para sancionar conductas como el acceso no autorizado a sistemas informáticos, la interferencia en el funcionamiento de los sistemas, el espionaje informático, entre otros.	Los delitos informáticos comenzaron a ser regulados explícitamente en el Código Penal a partir del año 2008. Este cambio se implementó mediante la Ley N.º 26.388, que fue promulgada el 4 de junio de 2008. Entre estos se encuentran el fraude informático.	Los delitos informáticos comenzaron a regularse formalmente en el Código Penal a partir del año 1995 con la aprobación de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal. Esta ley incorporó por primera vez en el Código Penal español una serie de artículos específicamente dirigidos a sancionar conductas delictivas relacionadas con el uso de tecnologías de la información y comunicación.
Análisis: En cuanto a los antecedentes del tipo penal referente a los delitos informáticos, las legislaciones de Ecuador, Argentina y España disponen de normas y regulaciones que pueden contrarrestar el delito de phishing. No obstantes, estas legislaciones se diferencian por los años de promulgación, sanciones e interpretación.				

Elaborado por: Autores

TABLA # 10 CUADRO COMPARATIVO ELEMENTO OBJETIVO DEL TIPO PENAL

	Criterio	Conceptualización	Ecuador	Argentina	España
Elementos objetivos del tipo penal	Denominación del tipo penal	Como se encuentra tipificado el delito en sus respectivos códigos penales en las diferentes legislaciones.	Estafa - Apropiación fraudulenta- Interceptación ilegal de datos- Acceso no consentido	Estafa – Acceso ilegitimo a sistemas informáticos – Falsificación informática	Acceso ilícito a sistemas informáticos- Estafa
	Verbo rector / núcleo	Acción que realiza una persona o un sujeto, es decir la base en que se centra y se describe una conducta.	Altere/ Modifique/ Acceda	Engaño /Acceda/ Introducir	Acceda/ Engaño
	Bien jurídico protegido	El Bien jurídico protegido es aquel que se busca proteger mediante las normas penales y que se encuentran reconocido en cada	Datos personales	Datos personales	Datos personales

		una de las constituciones.			
	Sujeto Activo	Persona que comete el acto delictivo y que su acción con llevaría a una sanción impuesta en la norma.	Delincuente informático	Delincuente informático	Delincuente informático
	Sujeto Pasivo	El sujeto pasivo es aquel a que se está vulnerando su derecho o aquella que ha sido víctima de una conducta antijuridica, estas pueden ser personas naturales es decir los ciudadanos o personas jurídicas, empresas privadas o entidades publicas	Persona común o jurídica	Persona común o jurídica	Persona común o jurídica
	Sanción	Pena que se impone por el incumpliendo de una norma o la vulneración de un derecho a otra.	Pena privativa de libertad de uno a tres años/pena privativa de libertad de uno a tres años / pena privativa de libertad de tres a cinco años	Un mes a seis años/ quince días a seis años/ prisión de un mes a dos años	Prisión de seis meses a tres años / Si la cuantía de lo defraudado no excediere de 400 euros, se impondrá la pena de multa de uno a tres meses.
Análisis: Acerca de los elementos objetivos del tipo penal relacionados al delito de phishing, Ecuador, Argentina y España, identifican a este delito como una estafa, o acceso ilegitimo del sistema informático, dado que, sus objetivos es engañar, alterar, modificar y acceder a datos personales de personas naturales o jurídicas, no obstante, las sanciones de cada país son diferente, a causa de los problemas informáticos que ocurren en esas legislaciones.					

Elaborado por: Autores

TABLA # 11 CUADRO COMPARATIVO DE ELEMENTO SUBJETIVO DEL TIPO PENAL

Criterio	Conceptualización	Ecuador	Argentina	España
Elemento subjetivo del tipo penal	Conocer el grado de participación del sujeto activo en el cometimiento del delito, si lo hace mediante el dolo o culpabilidad.	Dolo	Dolo	Dolo

Análisis: En lo que concierne al elemento Objetivo del Tipo penal sobre el delito informático phishing, en las legislaciones de Ecuador, Argentina y España es el Dolo, puesto que la persona que cometen este delito, lo hacen de manera voluntaria con el objetivo de engañar a alguien, conociendo de su ilicitud

Elaborado por: Autores

4.2. Verificación de la idea a defender

Luego de haber analizado los medios bibliográficos, Leyes, doctrina, y normativas de Ecuador, Argentina y España acerca del delito informático phishing, se logró identificar la veracidad de la idea a defender, por lo que se afirmó, que las normativas de las legislaciones de Argentina y España tienen más efectividad en la protección de datos personales de sus ciudadanos, debido a que cuenta con artículos eficientes, convenios internacionales, canales informáticos que ayudan contrarrestar este tipo delito, en cambio, Ecuador, cuentan con normativas eficientes para los delitos informáticos, pero la falta de especificidad no se ajusta al delito de phishing lo que lo convierte en un problema al momento de interpretar la norma.

Dentro de las legislaciones de Ecuador, Argentina y España, el delito informático phishing se asemeja a la estafa, dado que este delito se produce mediante ingeniería social con el objetivo de engañar a su víctima a través de medios electrónicos, y a la apropiación de datos personales, ya que se fundamenta en la apropiación ilícita de datos sin la autorización del afectado.

En Ecuador este delito se compara a los Art. 186, Art. 190, Art. 230, Art.234 del COIP, que trata de la estafa, apropiación fraudulenta, intercesión de datos y al acceso no consentido de un sistema informático, asimismo en Argentina este delito también se contrasta en su código penal en los Art. 172, Art 173 numeral 15 y 16 que alude al acceso ilegitimo, falsificación, y estafas informáticas, del mismo modo, España, en sus Art. 248 y Art 249 del código penal, que se refiere, a las estafa y a los fraudes informáticos.

En el ámbito constitucional de Ecuador, Argentina y España, el delito informático phishing, aborda específicamente la protección de datos personales estableciendo medidas legales para proteger los datos que son de carácter personal de los ciudadanos.

Posteriormente, en la ley de protección de datos de Ecuador, Argentina, España se desarrollan principios similares, los cuales ayudan a regular los delitos informáticos, sin embargo, España, al tener un reglamento de protección de datos, hace que sus principios sean más eficientes.

Respecto a las legislaciones internacionales, se constata que Argentina y España pertenecen al convenio de Budapest, que establece medidas sólidas y aptas para poder contrarrestar la ciberdelincuencia. Por otro lado, el Ecuador al no estar suscrito a este convenio, se limita a la cooperación internacional que aborda la protección de datos y la ciberdelincuencia.

Para finalizar, es importante resaltar que el delito informático phishing, en la legislación de Ecuador, se puede contrarrestar, sin embargo, la falta de análisis, es el problema al momento de aplicar una sanción, ya que se divide en secciones de tipo penal que ocasiona problemas a los jueces al calificar este tipo de conducta, en cambio Argentina y España al tener pocas normativas de esta clase de delitos, son más estructuradas y detalladas, lo que ayuda abarcar varios aspectos al imponer una sanción.

CONCLUSIONES

Después de finalizar el presente trabajo de investigación sobre el Phishing Como Delito Informático En El Ámbito De Las Legislaciones De Ecuador, Argentina Y España, 2023, se concluye lo siguiente:

- El avance del internet ha ocasionado ventaja en la vida cotidiana del ser humano tanto en la flexibilidad de la comunicación, educación, trabajo e investigación, y a la vez desventaja por la inseguridad que se presenta al momento de navegar, puesto que los datos personales que se exponen en el internet, varias veces son utilizados por personas fraudulenta, para cometer ataque informático por medio de redes sociales, correos electrónicos o mensajes de texto.

- El phishing es un delito informático que se asemeja a la estafa, a la apropiación de datos personales, y es uno de los delitos más común en la actualidad, debido a que los hackers (personas con conociendo informático), utilizan este método con la finalidad de conseguir información confidencial por medio de enlaces de páginas o sitios web similares a la página original. Es necesario resaltar que el phishing no solo perjudica a personas naturales, sino también a persona jurídicas.

- Las legislaciones de Ecuador, Argentina y España, denominan al delito de phishing como una estafa, lo que genera una similitud en su concepto, pero no en su normativa, puesto que Argentina y España cuenta con leyes más generalizadas, portales web diseñadas para contrarrestar los delitos informáticos, y pertenecen al convenio de Budapest, lo que les ayuda a mantener una percepción clara de los delitos informáticos, mientras que el Ecuador, pese a tener leyes eficientes, resulta innecesario, ya que existen varios tipos penales que se asemejan a esta conducta, pero su especificidad no son tan claros para abarcar el problema del phishing.

- La eficacia de las normas, la creación de instituciones u organismos para contrarrestar los delitos informáticos es muy importante, dado que permite salvaguardar los derechos de los usuarios que cada día están inmerso en el mundo informático, y así mismo, proteger los datos personales que se encuentran expuesto en las redes sociales, sitios web, aplicaciones, que son vulnerable a ataques informáticos.

RECOMENDACIONES

- Se recomienda a las personas tener cuidado al momento de navegar a través del internet sobre todo en las redes sociales correos electrónicos o mensajes de texto, ya que en estos medios radica un peligro al momento de que hacemos uso de estos en nuestras tareas cotidianas.

- El phishing es una conducta que busca mediante enlaces obtener información personal, siendo su principal medio las redes sociales, por lo que se recomienda a las personas no acceder a enlaces de los cuales no se tenga una certeza de que estos sean seguros, por lo general estos enlaces te redirigen a una página similar a la original en donde te pedirán que registres tus datos para ingresar a la misma, uno de los varios método que existen para poder combatir el robo de datos a través de internet es tener activada al verificación en dos pasos, ya que esta te permite iniciar sesión o no en dispositivos desconocidos, ya que para poder hacerlo tendrás que conceder dicho permiso, es decir que te mantiene informado de tus inicios de sesión que no hayas realizado y bloquearlos en caso de tu no hayas iniciado sesión.

- Por otro lado, se recomienda a la legislación de Ecuador ser más específica en su normativa respecto a lo que es la conducta de phishing, ya puede causar un conflicto en cuanto a que tipo penal debe ser aplicado, de igual forma se evidencia la importancia de estar suscrito a un convenio internacional que trate estos aspectos tal como lo hacen la legislación de España y Argentina.

- Respecto al marco legal e institucional en las legislaciones de España y Argentina, se evidencia en las normas abarcan de una mejor manera la conducta de phishing debido a que esta conducta se subsume dentro de su marco legal, de igual forma ambas legislaciones tienen más instituciones especializadas en lo que son los delitos informáticos, en consideración a lo antes mencionado, se recomienda a Ecuador que su marco legal sea más específico en lo que concierne a la conducta del phishing, además de que tampoco cuentan con instituciones especializadas en lo que concierne a la investigación y la persecución de delitos informáticos.

BIBLIOGRAFÍA

Acosta, M. G., Benavides, M. M., & Garcia, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Dialet*, 351-368.

Armengo, C. M. (2015). *METODOLOGÍAS: ENSEÑANZA E INVESTIGACIÓN JURÍDICAS.* Obtenido de https://archivos.juridicas.unam.mx/www/bjv/libros/8/3983/46.pdf

Barahona, F. (23 de Febrero de 2023). *Protegerse*. Obtenido de Protegerse: https://blogs.protegerse.com/2023/02/23/informe-eset-espana-sigue-en-el-ranking-de-paises-que-mas-detectan-ciberamenazas-en-todo-el-mundo/

Cabanellas, G. (2006). *Dicionario Juridico Elemental.* Buenos Aires: Heliasta S.R.L.

Cáceres, C. F. (2017). *EL PHISHING COMO COMPORTAMIENTO PENALMENTE RELEVANTE.* Valparaíso: Pontificia Universidad Católica de Valparaíso.

Callejas, J. F., Afifi, A., & Lozinskiy, N. (2021). *La ciberseguridad en las organizaciones del sistema de las Naciones Unidas.* Ginebra: Naciones Unidas. Obtenido de https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf

Carlos Eduardo Méndez Álvarez. (1995). *METODOLOGIA*. Santafé de Bogota: Kimpres Ltda. - Santafé de Bogotá. D.C.

Ciberseguridad, D. N. (2021). *Phishing una guía y un glosario para conocer sus modalidades y prevenirlas.* Argentinaunida. Obtenido de https://www.argentina.gob.ar/sites/default/files/2021/10/informe_phishing_1.pdf

Codigo Organico Integral Penal. (2014). *CÓDIGO ORGÁNICO INTEGRAL PENAL, COIP.* QUITO: LEXIS. Obtenido de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

CODIGO PENAL. (2008). *Ley Nº 26.388.* Buenos Aires: REGISTRADO BAJO EL Nº 26.388.

Codigo Penal. (2023). *Codigo Penal.* Madrid: cpage.mpr.gob.es. Obtenido de https://www.boe.es/biblioteca_juridica/abrir_pdf.php?id=PUB-DP-2023-118

Código Penal de la Nación Argentina. (1984). *CODIGO PENAL DE LA NACIÓN ARGENTINA*. Buenos Aires: InfoLEG. Obtenido de

https://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

Constitución De La República Del Ecuador. (2008). *CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR*. Quito: Lexis. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

CONSTITUCIÓN ESPAÑOLA. (1978). *CONSTITUCIÓN ESPAÑOLA*. MADRID: publicacionesoficiales.boe.es.

Contreras, F. (2001). Internet: la red en España. *Revista Latina de Comunicación Social*.

ESET. (2023). *SECURITY REPORT*. Obtenido de https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

ESET Security Report. (2023). Security Report Latam. *ESET*, 8-20. Obtenido de https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

Flores Salgado, L. (2015). *Derecho Informático.* Mexico: Grupo editorial patria.

Frances, L. G. (2015). *Fraude informático y estafa.* Madrid: Ministerio de justicia.

Francés, M. L. (1991). *Fraude informático y estafa.* Madrid: Ministerio de justicia de España.

GALLO, C. C., & TOMALA, B. R. (2015). *GUÍA METODOLÓGICA DE PROYECTOS DE INVESTIGACIÓN SOCIAL.* SANTA ELENA : UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA.

La Nación / Costa Rica / GDA. (17 de septiembre de 2023). *El Economista*. Obtenido de El Economista: https://www.eleconomista.net/tecnologia/Costa-Rica-es-el-segundo-pais-mas-afectado-por-phishing-en-Latinoamerica-20230917-0005.html

Lima, M. D. (1984). *Delitos Electrónicos.* Mexico: Ediciones Porrua.

LOSA, L. C. (1987). *EL DELITO INFORMÁTICO.* MADRID: L. Camacho.

MATUTE, J. C. (2013). EL DELITO INFORMÁTICO DE PHISHING. *UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES UNIANDES*, 1-130.

Merwe, A. v., Loock, M., & Dabrowski, M. (03 de Enero de 2005). Characteristics and responsibilities involved in a Phishing attack; WISICT '05: Proceedings of the 4th

international symposium on Information and communication technologiesJanuary 2005Pages 249–254. *ACM; DL: Digital Library*, 1. Obtenido de https://dl.acm.org/doi/10.5555/1071752.1071800

Mite, L. M. (08 de Septiembre de 2017). *Ecuador accede a internet desde hace 25 años*. Obtenido de eltelegrafo: https://www.eltelegrafo.com.ec/noticias/tecnologia/1/ecuador-accede-a-internet-desde-hace-25-anos

Pérez Luño, A. E. (1996). *Manual de Informatica y derecho.* Barcelona: Ariel S.A.

RETAMAR, N. (14 de Diciembre de 2022). *Argentina en Internet: se cumplieron 35 años de la creación del código país .ar*. Obtenido de Agencia de noticias científicas: https://agencia.unq.edu.ar/?p=9623

Rodríguez Gámez, O., Hernández Perdomo, R., Torno Hidalgo, L., Rodríguez Romero,, R., & Rodríguez Romero, R. (2005). Telefonía móvil celular: origen, evolución, perspectivas. *Ciencias Holguín, XI*, 1-8.

Terreros, F. V. (2014). Delitos Informáticos. *IUS ET VERITAS*, 1-21.

Villegas Cubas, J. E. (2021). Modelo de machine learning en la detección de sitios web phishing. *(Tesis de Doctorado).* Universidad Señor de Sipán, Chiclayo.