Universidad Tecnológica ECOTEC

Nombre de la Facultad

Facultad de Derecho y Gobernabilidad

Título del trabajo:

“La Falta de tipificación penal sobre los delitos informáticos en el Ecuador”

Línea de Investigación:

Gestión de las relaciones jurídicas

Modalidad de titulación:

Proyecto de Investigación

Carrera:

Derecho y Gobernabilidad, énfasis en Derechos Humanos y Ciencias Penales

Título a obtener:

Abogado de los Tribunales y Juzgados de la República del Ecuador énfasis Derechos Humanos y Ciencias Penales

Autor (a):

Cristopher Antonio Cires Saona

Tutor (a):

Mgtr. Fabián Orellana Batallas

Guayaquil – Ecuador

2022

DEDICATORIA

Este proyecto de investigación se lo quiero dedicar a mis padres y miembros de mi familia, por haber estado presente en el transcurso de mi carrera universitaria, en cuanto a consejos, apoyo y motivación.

A Dios por haberme dado la bendición de culminar mis estudios en la carrera de Derecho para formarme como próximo Abogado de los Tribunales del Ecuador.

A mis familiares que hoy en día ya no me acompañan físicamente pero en vida aportaron con sus consejos, enseñanzas y que quisieron verme llegar a la meta y lograr lo que tanto anhelaba.

AGRADECIMIENTOS

Agradezco primero a mis padres por apoyarme en todo el proceso de estudio, por estar presentes en las dificultades y dudas que haya tenido durante la carrera universitaria, luego agradecer a los abogados de la Facultad de Derecho y Gobernabilidad por el tiempo de enseñanza, ya que gracias a ellos he adquirido información que me servirá para aplicar en la vida profesional y ser mejor persona.

CERTIFICADO DE REVISIÓN FINAL

Universidad Ecotec

ANEXO N°16

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

Samborondón, 16 de junio de 2022

Magíster
Mario Cuvi Santacruz
Decano de la Facultad
Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: "LA FALTA DE TIPIFICACIÓN PENAL SOBRE LOS DELITOS INFORMÁTICOS EN EL ECUADOR" según su modalidad PROYECTO DE INVESTIGACIÓN, PROPUESTA TECNOLÓGICA O EXAMEN COMPLEXIVO (ESTUDIO DE CASO) **PROYECTO DE INVESTIGACIÓN**; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **CIRES SAONA CRISTOPHER ANTONIO,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,

Mgtr. Fabián Orellana Batallas

Tutor

CERTIFICADO DE COINCIDENCIAS DE PLAGIO

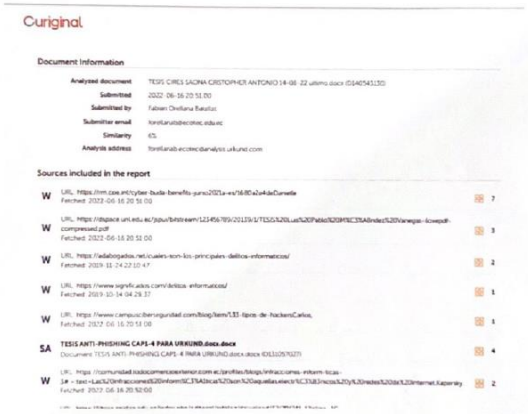
Universidad Ecotec

ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado MGTR. FABIÁN ORELLANA BATALLAS, tutor del trabajo de titulación "LA FALTA DE TIPIFICACIÓN PENAL SOBRE LOS DELITOS INFORMÁTICOS EN EL ECUADOR" elaborado por CRISTOPHER ANTONIO CIRES SAONA, con mi respectiva supervisión como requerimiento parcial para la obtención del título de ABOGADO DE LOS TRIBUNALES DE LA REPUBLICA DEL ECUADOR CON ENFASIS EN DERECHOS HUMANOS Y CIENCIAS PENALES.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias de 6%, mismo que se puede verificar en el siguiente link: https://secure.urkund.com/view/134140526-686759-328752 . Adicional se adjunta print de pantalla de dicho resultado.



Curigina

Document Information

Analysed document: TESIS CIRES SAONA CRISTOPHER ANTONIO 14-08 -22 ultimo.docx (D140541335)
Submitted: 2022-08-16 20:51:00
Submitted by: Fabian Orellana Batallas
Submitter email: forellanab@ecotec.edu.ec
Similarity: 6%
Analysis address: forellanab.ecotec@analysis.urkund.com

Sources included in the report

W URL: https://rm.coe.int/cyber-buda-benefits-punto2021a-es/1680a2a4de Fetched: 2022-08-16 20:51:00 — 7
W URL: https://dspace.uni.edu.ec/jspui/bitstream/123456789/20139/1/TESIS%20Luis%20Pulido%20MESTRIA%20Vanegas-Ecuapdf-compressed.pdf Fetched: 2022-08-16 20:51:00 — 3
W URL: https://adabogados.net/cuales-son-los-principales-delitos-informaticos/ Fetched: 2019-11-24 22:10:47 — 2
W URL: https://www.significados.com/delitos-informaticos/ Fetched: 2019-10-14 04:29:37 — 1
W URL: https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackersCarlos, Fetched: 2022-08-16 20:51:08 — 1
SA TESIS ANTI-PHISHING CAPS-4 PARA URKUND.docx.docx — Document TESIS ANTI-PHISHING CAPS-4 PARA URKUND.docx.docx (D1310570277) — 4
W URL: https://comunidad.radiocomercioexterior.com.ec/profiles/blogs/infracciones-inform-tcas-1#:~text=Las%20infracciones%20informáticas%20tcas%20son%20aquellas,electrónicos%20y%20redes%20de%20Internet.Kaspersky Fetched: 2022-08-16 20:52:00 — 2

FIRMA DEL TUTOR
FABIÁN ORELLANA BATALLAS

RESUMEN

El presente trabajo de investigación comprende un amplio análisis a la normativa legal ecuatoriana en marco a los delitos informáticos. De la misma manera, se incluye un estudio comparativo de diversas leyes que regulan la delincuencia informática en países de habla hispana, con la finalidad de establecer la necesidad de reformar o incorporar nuevas formas de tipificación penal que penalicen y regulen, bajo una normativa común entre países, estas nuevas formas de infracciones informáticas.

Este análisis se realiza desde el estudio de la legislación penal existente y vigente, identificando los diversos tipos de delitos informáticos, penalizaciones y formas de regulación y control. Finalmente se incorpora una propuesta de adhesión al convenio de la ciberdelincuencia de Budapest, el cual provee una legislación penal completa y procedimientos comunes en el ámbito de los delitos informáticos, siendo una referencia mundial en este campo.

Palabras clave:

Delito, informático, convenio, ley, penalización

ABSTRACT

This present investigation work includes a broad analysis of the Ecuadorian legal regulations in the framework of computer crimes. In the same form, a comparative study of different laws that regulate computer crime in Spanish-speaking countries are included, in order to establish the need to reform or incorporate new forms of criminal classification that penalize and regulate, under a common law between countries, these new ways of computer infractions.

This analysis is done by the study of existing and current criminal legislation, identifying the various types of computer crimes, penalties and forms of regulation and control. Finally, a proposal for adherence to the Budapest cybercrime convention is incorporated, which provides complete criminal legislation and common procedures in the field of computer crimes, being a world reference in this field.

Keywords:

Crime, computer, convention, law, penalty

ÍNDICE

ÍNDICE DE CUADROS

Resultados y análisis de las encuestas

ÍNDICE DE GRÁFICOS

Resultados y análisis de las encuestas

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el presente proyecto de investigación, titulado "**La falta de tipificación penal sobre los delitos informáticos en el Ecuador",** se integra una extensa compilación de información bibliográfica, una variedad de análisis tecnológicos y jurídicos sobre los delitos e infracciones informáticas, su regulación en la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, Constitución de la República del Ecuador, Código Orgánico Integral Penal Ecuatoriano y diversas leyes que regulan y sancionan los delitos informáticos en países vecinos. Trabajo que entrego como parte complementaria o final de mis estudios universitarios en la carrera de Derecho y Gobernabilidad, donde he adquirido una amplia gama de conocimientos para realizar este proyecto.

Este tema que abarca a los delitos informáticos no es nuevo, ya tiene muchos años afectando a nuestra sociedad y al mundo entero, vivimos en el mundo de la información, donde los datos e información viajan a través de redes que son utilizadas por expertos informáticos, hackers, piratas de la red, ciberdelincuentes, como desee llamarlos, para obtener de forma astuta e ilícita dicha información y ponerla al alcance de pocos o muchos, sea por placer personal, venganza, dinero o cualquier interés en particular, aprovechando los vacíos legales de nuestras leyes.

Hablamos ahora de otros escenarios más complejos, de guerra de la información, en la que los afectados son los ciudadanos particulares, las pequeñas y medianas empresas e incluso las grandes industrias y entidades gubernamentales, que muchas veces por descuido o engaño, entregamos información o somos víctimas de ataques informáticos, suplantación de identidades, secuestro de información, extorsiones, robos de información, a través de engaños en la web.

Todas estas formas de ataques y delitos informáticos se han incrementado exponencialmente en el mundo. Incluso muchos expertos lo consideran normal, sin embargo debemos generar conciencia como país y colaborar con nuestra sociedad brindando herramientas, seguridad jurídica y

mecanismos de control que permitan proteger a las personas, las redes, los equipos de computación, a los proveedores de servicios de internet, en fin.

En la actualidad, nuestro país cuenta con una Ley que regula el uso de la información y datos, la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, Ley 67 Registro Oficial Suplemento 557 de 17-abr.-2002, sin embargo, dicha ley fue modificada el 10 de febrero del 2014, **derogando**, eliminando o suprimiendo el CAPÍTULO I DE LAS INFRACCIONES INFORMÁTICAS con sus respectivos artículos del 57 al 64 derogados por Disposición Derogatoria Novena de Ley No. 00, publicada en Registro Oficial Suplemento 180 de 10 de Febrero del 2014. Artículos en los cuales se contemplaban y sancionaban a diversos tipos de delitos informáticos como ataques informáticos, suplantación de identidades, secuestro de información, extorsiones, robos de información, etc.

Si bien el título V capítulo I de nuestra Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos formaba parte de una ley obsoleta, no es coherente pensar que una nueva Ley del Código Orgánico Integral Penal Ecuatoriano COIP, incorpore en su contenido, tan solo unos cuantos de estos delitos informáticos, ante lo cual considero pertinente reformar o proponer artículos actualizados que abarquen la mayor cantidad de estas infracciones informáticas o en su defecto proponer que el Ecuador, como país, forme parte del Convenio sobre la Ciberdelincuencia No. 185 ("Convenio de Budapest"), el cual es considerado como la norma internacional más completa hasta la fecha, ya que proporciona un marco integral común y coherente en contra del ciberdelito y la evidencia electrónica.

Este Convenio de Budapest prevé: la criminalización de la conducta, que va desde el acceso ilícito, ataques a la integridad del sistema y de los datos hasta el fraude informático y los delitos relacionados con la pornografía infantil; diversas herramientas de derecho procesal para hacer más efectiva la investigación relacionada con los ciberdelitos y la obtención de evidencias electrónicas; y proveer una cooperación internacional más ágil y eficiente.

Este tratado o convenio está abierto para que cualquier país pueda adherirse. De igual forma, el Convenio de Budapest se complementa con un Protocolo Adicional que penaliza la criminalización de actos de naturaleza racista y xenófoba cometidos en la actualidad y con frecuencia a través de sistemas informáticos.

Este trabajo de investigación ha sido desarrollado en varias etapas, primero el autor ha incorporado un marco de definiciones de diferentes autores, lo cual permite facilitar la comprensión lectora, además de considerar importante para el desarrollo de esta tesis; luego en base a las definiciones poder relacionar el problema planteado y analizar el marco legal que regula las infracciones informáticas, en este caso la Ley del Código Orgánico Integral Penal Ecuatoriano COIP.

A continuación el autor presenta una comparación de diferentes legislaciones que regulan y tipifican las infracciones informáticas, permitiendo identificar y conocer las normas reguladoras de infracciones informáticas de países vecinos al Ecuador, brindando y facilitando la comprensión de la presente investigación.

Posteriormente podrán encontrar la metodología utilizada en este proceso de investigación y los instrumentos utilizados para el efecto, entre ellos las entrevistas a expertos, encuestas, consultas bibliográficas y experiencias compartidas, complementando con los resultados obtenidos de las encuestas, una representación gráfica, análisis porcentual, cuantitativo y cualitativo.

Antes de finalizar el presente trabajo de investigación se da por verificado el cumplimiento de los objetivos propuestos, en cuanto a los resultados obtenidos y se considera imprescindible contar con una actualización a la normativa legal ecuatoriana en lo que respecta a delitos o infracciones informáticas.

Por otro lado, del análisis comparativo realizado con leyes de países vecinos o de habla hispana, se ha evidenciado que la gran mayoría ya es parte o está en proceso de ser miembro del Convenio de Budapest contra la ciberdelincuencia, normativa global y actualizada que regula y sanciona los delitos informáticos.

Por esta razón el autor finaliza con la propuesta de la necesidad de reformar el marco legal sobre las infracciones informáticas o que el Ecuador forme parte del Convenio sobre la Ciberdelincuencia No. 185 ("Convenio de Budapest").

PLANTEAMIENTO DEL PROBLEMA

La problemática actual de nuestro País es la de no contar con una ley coherente y actualizada que identifique, regule y sancione a las personas que utilizando cualquier medio, método o recurso, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información, aplicación digital, aplicación móvil o red electrónica, lo que describiremos más adelante como delito informático.

Contamos con una ley obsoleta de comercio electrónico, firmas electrónicas y mensaje de datos publicada en el 2002, modificada el 10 de febrero del 2014, derogando, eliminando o suprimiendo el CAPÍTULO I DE LAS INFRACCIONES INFORMÁTICAS con sus respectivos artículos del 57 al 64 derogados por Disposición Derogatoria Novena de Ley No. 00, publicada en Registro Oficial Suplemento 180 de 10 de Febrero del 2014 y una Ley del Código Orgánico Integral Penal Ecuatoriano COIP que incorpora, de forma muy superficial, unos pocos de estos delitos informáticos.

Nos encontramos frente a diversas formas modernas de ejecución de delitos informáticos con técnicas de efectividad completamente altas, las cuales ni siquiera están contempladas como delitos mucho menos tipificada su sanción, y por otro lado, no se cuenta con el personal adecuado capaz de entender o reconocer una prueba digital, entiéndase jueces y fiscales, los cuales muchas veces llegan a una escena de un crimen, como parte de la cadena de custodia que se debe llevar a efecto y no tienen el conocimiento penal informático necesario para reconocer a los objetos materia del delito y como se relacionan entre ellos. Ante esto, se considera necesaria una actualización en conocimientos y en técnicas digitales que nos permitan reconocer e identificar este tipo de infracciones.

Por consiguiente, es pertinente primero conocer cómo nuestros países vecinos han avanzado en el tema de los delitos informáticos, cómo los identifican, cómo los sancionan, cómo los regulan, qué tipo de legislación utilizan para su efecto, etc.

Ante esta problemática, se torna muy interesante establecer una propuesta o alternativas que complementen a nuestra obsoleta Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, en su derogado Título V – Capítulo I, referente a las infracciones informáticas, lo cual sin lugar a dudas, será un buen punto de partida como beneficio para nuestra sociedad.

Pregunta problemática de la investigación:

Si tuviésemos una adecuada tipificación penal que regule y sancione coherentemente las infracciones informáticas en nuestro País, ¿disminuirían la cantidad de delitos informáticos incorporados en nuestra sociedad?

OBJETIVOS

OBJETIVO GENERAL

Determinar las consecuencias al no contar con una normativa legal que regule los delitos informáticos en el Ecuador.

OBJETIVOS ESPECÍFICOS

1.- Analizar la normativa legal ecuatoriana referente al tema de delitos informáticos y establecer un esquema comparativo con leyes de países vecinos frente a este tipo de infracción.

2.- Establecer si resulta necesario y eficaz reformar o incorporar nuevas formas de tipificación de los delitos informáticos frente a los avances tecnológicos y las nuevas modalidades de ataques delictivos en este tipo de infracciones.

3.- Proponer alternativas al Código Orgánico Integral Penal Ecuatoriano, con la finalidad que se tipifiquen las nuevas formas y medios de ocasionar daños informáticos en nuestra sociedad.

JUSTIFICACIÓN

Según Matías Koller, experto en ciberseguridad, en el diario perfil.com publicó: “que los delitos informáticos se multiplicaron de manera exponencial durante la pandemia. Se calcula que en el mundo este tipo de modalidad delictiva aumentó entre un 700% y 1000% del 2020 al 2021, a partir de la pandemia y el uso de la tecnología. Hubo empresas que migraron a la digitalización y eso generó que crecieran muchísimo las técnicas de engaño, extorsión y robos de datos, entre otros tipos de delitos” (Matías Koeller, 2022)

Es muy frecuente encontrar este tipo de noticias en los portales de noticias nacionales e internacionales. Los delitos informáticos se han convertido en el pan de cada día. Miles de personas y empresas que intentan migrar a la digitalización o que ya se encuentran dentro de ella, se ven afectadas en su integridad, en su economía, en sus trabajos, hogares e incluso hasta en su intimidad.

Los autores, directos o indirectos, de estos delitos informáticos, utilizan spam y conocimientos informáticos avanzados, utilizando sitios web falsos, software malicioso y otras técnicas altamente efectivas, para engañar a las personas con el fin de obtener cualquier tipo de información, contraseñas o claves personales de forma fraudulenta y así acceder a información confidencial.

Así mismo afectan a nivel de empresas, a la banca, a la industria del entretenimiento, el comercio, la publicidad, las instituciones públicas y del estado De la misma manera afectan a la imagen empresarial, a los secretos comerciales y judiciales, a la violación del secreto de las comunicaciones, interceptación de comunicaciones personales de manera ilegal, utilización y modificación de los datos de carácter personal sin consentimiento, acceso ilegal a datos y sistemas informáticos, difusión de datos, hechos descubiertos o imágenes captadas ilícitamente.

Con la finalidad de advertir la gravedad de estos hechos, cito el siguiente fragmento sobre las cifras económicas que se reportan en los diferentes informes anuales, sean estos de Norteamérica o de la Unión Europea, en los cuales se

habla de un valor en daños económicos entre particulares y empresas que sobrepasa los 550 millones de dólares (según el “National Center for Computer Crime Data”) y de 15 billones de dólares (según la Inter-Pact computer security organization”).

Estas cifras han sido proporcionadas por el Internet Crime Report, el cual se establece como un centro especializado en una variedad de estafas por internet. En este centro especializado se reciben denuncias de delitos causados a través de una red, cada año aumentan sus reclamos que afectan a estas víctimas internacionalmente, entre los años 2015 al 2019 se recibió un reporte de un total de 1,707,618 de reclamos, provocando una pérdida económica de $10.2 millones. (International Crime Report, 2019)

En nuestro país, así mismo se reportan a diario casos de estafas por internet, fraudes, robos, extorsiones, suplantación de identidades, mensajes de publicidad engañosa, mensajes de textos de amigos con cuentas clonadas, en fin, un sinnúmero de nuevas formas de engaños informáticos, lamentablemente no se les da el seguimiento adecuado, ni las denuncias correspondientes.

El tipo de delito reportado con mayor frecuencia en nuestro país es el Phishing o suplantación de identidad. A continuación, incorporo algunos ejemplos, para comprender mejor una de las diversas formas de ataques informáticos.

Caso Banco Bolivariano - 2020

Los bancos o entidades financieras son el blanco perfecto para los delincuentes. Para llevar a efecto este tipo de delito, el atacante crea una página web o aplicación con similares características que la página real de la agencia bancaria con la intención que los usuarios de estas entidades bancarias, no sospechen e ingresen su información personal, como números de cuenta, usuarios, contraseñas, correos, etc. (Caso Banco Bolivariano, 2020)

Entre los casos reportados, se evidencia que el hacker crea un envío masivo de correos “con un boletín informativo” a los usuarios registrados de la

agencia bancaria, solicitando acceder a un link para la actualización de datos de los clientes.

Al realizar el ingreso al link se abre o se carga una página con las características idénticas a la página oficial del banco, mismo logo, agencias, información, etc, lo cual hace presumir al usuario que está dentro de la aplicación bancaria.

Una vez dentro de la aplicación, el usuario desprevenido, ingresa su información personal, la misma que es capturada por el hacker quien la roba y hace uso ilícito de estos datos, generando una apropiación ilícita de datos.

El boletín de actualización de datos que envía el supuesto banco, hace parecer al cliente algo normal, pero tras ello hay una serie de enlaces o links que vale la pena revisar antes de continuar en un sitio web.

Internamente los enlaces se re direccionan de esta manera:

Remitente: communications_msn_cs_esxl@microsoft.windowslive.com

Enlace que mostraba: http://www.bolivariano.com/?codsinc=8746474884899484

Enlace al que direccionaba: http://www.brickyardhill.org/augur/bolivariano/login.html

Caso Banco del Pichincha - 2019:

Otro caso muy similar, reportado en el 2019, fue otra agencia bancaria del medio. De la misma forma, el atacante envía un documento de actualización de datos al cliente, el cual es direccionado, mediante un link, a una página similar a la del banco del pichincha, donde el usuario digita su usuario y clave de ingreso a la aplicación, sin darse cuenta que sus datos están siendo capturados por una aplicación. (Caso Banco de Pichincha, 2019)

El enlace que se visualizaba correspondía a una restauración-personal, lo cual probablemente no generaba sospecha al usuario.

Sin embargo, los otros dos enlaces no correspondían a ninguna aplicación de la agencia bancaria. Por eso siempre existen las recomendaciones que los usuarios deben revisar el sitio al que están siendo redirigidos, en todo sitio web.

Estos fueron los enlaces redirigidos en el caso Banco del Pichincha:

Enlace que mostraba: https://restauracion-personal

Enlace al que direccionaba: http://www.deejays.nu/discobazooka/bilder/gettxt.php

Enlace final: http://www.beblessedphotos.com/oldPhotos/content/pichincha.htm

Web falsa mostraba una pantalla de Banco Pichincha Internexo.

Dos de muchos casos que podríamos citar para este trabajo de investigación, donde prima la astucia, el conocimiento y el ingenio de los hackers o delincuentes de la red.

Otro de los mecanismos encontrados con mucha frecuencia son las publicidades falsas o engañosas a través de redes sociales. De la misma manera los usuarios son víctimas fáciles de las ofertas, de los regalos, de los incentivos y caen cuando ingresan a los links y proveen sus datos personales. En las últimas semanas se han enviado publicidades engañosas de Supermaxi, de cerveza corona, de pasajes al mundial de Catar y muchas más.

En otros casos, el hacker estudia su víctima, a su familia, actividades que hace, tipo de transacciones en la red, horarios de transaccionar, información personal como cuentas de correo electrónico, número de celular, fechas de nacimiento, etc.

Ante estos hechos es importante identificar los beneficios que se podrán alcanzar, al generar propuestas o alternativas a la derogada sección de infracciones informáticas Título V capítulo I de la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, con la finalidad que se contemplen y tipifiquen las nuevas formas y medios de ocasionar daños informáticos en nuestra sociedad y que se establezcan sanciones coherentes frente al verdadero perjuicio de la víctima afectada.

En la actualidad pocos son los países que intentan luchar solos frente a esta gran ola de delincuentes, muchos países están apostando a la cooperación internacional a través de tratados o convenios internacionales.

Esto se debe a que las fronteras entre naciones prácticamente están desapareciendo. Ahora consumimos servicios alojados en otros países (por ejemplo el alquiler de un hosting donde se almacena la página web de un negocio), luego guardamos nuestra información en “la nube” (aquí reposan nuestros documentos, nuestros respaldos de las transacciones efectuadas) o enviamos información que viaja a través de redes internacionales (Correos o mensajes enviados a amigos y familiares de país en país), cuando se trata de un delito informático, incluso de una evidencia digital, la investigación generalmente trasciende el territorio de una nación. No siempre el delito y la evidencia está en un mismo sitio o país. Esto resulta un tanto complejo a nivel legislativo, especialmente si las leyes de los países involucrados no están alineadas.

Para aclarar un poco lo expresado, cito un ejemplo: Supongamos que se comete un fraude informático a través de una página de pagos online Amazon España (amazon.es): la víctima (usted) hace una compra desde Ecuador, a través de un portal alojado en España, pero aquel (el delincuente) que lo engañó, que lo incitó para hacer esa compra o pago se encuentra en Aruba. Tres regiones completamente distantes.

A esto se le puede complicar un poco más, si tanto la víctima como el estafador mantuvieron varias conversaciones por un servicio de chat, el cual pertenece a una empresa norteamericana.

La persona víctima del fraude informático realiza la denuncia por fraude en Ecuador por un delito que está tipificado, pero el delito en sí se cometió desde España y la evidencia está dividida entre Aruba y Estados Unidos. ¿Quién se hace cargo de ese delito entonces? ¿Bajo qué leyes y de qué país se deberá juzgar el delito y tratar la evidencia?

Este tipo de situaciones es **cada vez más común y habitual**, por lo que se vuelve imprescindible la cooperación internacional.

Por tal razón, surge la propuesta para que las autoridades de nuestro país conozcan la magnitud de los perjuicios ocasionados, las nuevas formas o mecanismos de control que están adoptando otros países y puedan realizar las gestiones necesarias para adherir al Ecuador al Convenio Internacional de Budapest, con el objetivo de establecer una política penal común y armonizar la cooperación internacional.

Al día de hoy son varios países que se han adherido al convenio, alrededor de 66 países de todo el mundo, incluyendo Chile, Costa Rica, República Dominicana, Panamá y recientemente Argentina, en lo que refiere a Latinoamérica. Mientras que México, Paraguay, Colombia y Perú están próximos a concretar la adhesión.

Es evidente entonces la importancia de este trabajo de investigación ya que mediante él podremos conocer la realidad jurídica respecto a los delitos informáticos de nuestro país, identificar las diversas modalidades de delitos informáticos y las posibles alternativas de solución para poder frenar con este tipo de amenaza que está tomando cada vez más fuerza en nuestra sociedad.

ALCANCE O TIPO DE INVESTIGACIÓN

El presente trabajo de investigación está basado en el paradigma cualitativo y cuantitativo, es cualitativo ya que se utiliza esencialmente técnicas basadas en el análisis del lenguaje, como es la entrevista a los expertos, y las técnicas de creatividad social. Por otro lado es cuantitativo debido a que se apoya en las técnicas estadísticas, sobre todo la encuesta y el análisis estadístico de los datos.

Por otro lado, la modalidad básica de la investigación bibliográfica documental. La presente investigación es el producto de la recolección y recopilación de información de delitos informáticos de varios textos, publicaciones, sitios web, blogs informáticos, etc.

A su vez nuestra investigación se apoyó con la recolección de la información, mediante entrevistas a expertos, de forma directa en la ciudad de

Guayaquil y a través de encuestas, utilizando las herramientas de google docs, a diversos funcionarios, docentes y profesionales de libre ejercicio de la profesión en el campo del derecho y de las tecnologías.

Por otra parte, el autor se basa en la utilización del método exploratorio, al realizar una investigación sobre las complicaciones y afectaciones causadas por los delitos informáticos, sugiere que debería de existir una reforma a la norma para que se apliquen sanciones adecuadas dependiendo del tipo de delito informático.

MARCO TEÓRICO

CAPÍTULO 1

1.1 Marco Teórico

1.1.1. Definiciones

Los delitos informáticos han generado un gran impacto en la sociedad, no solo por el riesgo de la seguridad de las personas y de las empresas sino también por el riesgo de toda la seguridad nacional.

Con el constante avance y desarrollo acelerado de la tecnología, con la creación de aplicaciones interactivas, de sistemas online, hemos evidenciado casos de uso fraudulento del software sobre información protegida de las personas y las empresas. De aquí la necesidad de fomentar una cultura de autoprotección, donde cada persona o usuario cuide de sus claves y contraseñas, de establecer mecanismos de seguridad para controlar y restringir el acceso a los datos a personas, de exigir a las empresas proveedoras de servicios de internet, mayor control en el acceso a sus sistemas de redes informáticas.

Se conoce que para el cometimiento de este tipo de delitos o infracciones, las personas utilizan los dispositivos electrónicos y sus avanzados conocimientos digitales y tecnológicos para cumplir sus objetivos, entre ellos:

1. Computadores de escritorio y portátiles.
2. Teléfonos inteligentes y dispositivos para identificar llamadas.
3. Tablets, ipads o similares
4. Cámaras de video, capturadores de señal.
5. Sistema de seguridad y sistemas de redes
6. Servidores que almacenan base de datos.
7. Gps y sistema de rastreo.

Dispositivos que aparentan ser inofensivos, pero en el momento que son utilizados de forma ilícita para un delito, infracción o crimen organizado causan daños y perjuicios a las personas.

Con la finalidad de brindar una mejor comprensión al presente trabajo, incluiré varias definiciones a términos informáticos producto de una extensa revisión bibliográfica en relación al tema de investigación.

1.1.2 Delito Informático.-

“El delito informático es cualquier uso ilegal, delictivo, inmoral o no autorizado de dispositivos electrónicos e Internet, con el objetivo de invadir, destruir o dañar la propiedad de partidos u organizaciones”. (Revista Seguridad 360, 2021)

Según el libro ¿Vida privada o muerte a la privacidad?: protección de datos personales en la relación empresa-cliente en Ecuador define los delitos informáticos, considerados como un género, han sido definidos como aquellas conductas indebidas realizadas por el sujeto activo que lesionan el bien jurídico tutelado, afectando la integridad de los equipos y la intimidad de sus propietarios (Enrique, 1996)

Por otro lado en la página oficial de la policía nacional del Ecuador sobre los delitos informáticos establecidos en el COIP y cómo prevenirlos define “los delitos informáticos son actividades ilícitas, que se cometen a través de medios y dispositivos tecnológicos y de comunicación, cuyo objetivo es causar algún daño, provocar pérdidas o impedir el uso de sistemas informáticos. En los últimos tiempos la pornografía infantil, fraudes informáticos e incluso actividades terroristas, han sido considerados como nuevos delitos informáticos”. (Richard Ramirez, 2017)

En otra página de significados define a los “delitos informáticos que son todas aquellas acciones ilegales, delictivas, antiéticas o no autorizadas que hacen uso de dispositivos electrónicos e internet, a fin de vulnerar, menoscabar o dañar los bienes, patrimoniales o no, de terceras personas o entidades. Conocidos también con el nombre de delitos cibernéticos o electrónicos, abarcan un amplio espectro de acciones ilegales de diferente naturaleza. Todos tienen en común las tecnologías de la información, sea estas el medio o el objetivo en sí mismo”. (Significados.com, 2022)

En palabras del autor los define como actos cometidos a través de dispositivos electrónicos, mediante el uso de plataformas digitales, redes sociales u otras aplicaciones con el fin de causar daños.

1.1.3. Comercio Electrónico.-

“Comercio electrónico es el modelo de negocios basado en las transacciones de productos y servicios en los medios electrónicos, ya sea en las redes sociales o en los sitios web.” (Edgar Higuerey, 2021)

Otra definición de la página economipedia.com define al “comercio electrónico (conocido popularmente como ecommerce), es la compraventa y distribución de bienes y servicios a través de internet u otras redes informáticas.” (Janire Carazo Alcalde, 2016)

Por otro lado “El e-commerce, o comercio electrónico, es un sistema de compra y venta de productos o servicios que se realiza exclusivamente a través de Internet. Se refiere a las transacciones entre compradores y vendedores mediante una plataforma online que gestiona los cobros y los pagos de manera completamente electrónica.” (Eserp Busisness & Law School, s.f.)

1.1.4. Ciberdelincuente.-

Según los expertos de la universidad Internacional de Valencia definen “al ciberdelincuente, también conocido como hacker, es una persona cuyo conocimiento informático le permite realizar acciones delictivas en Internet”. (Equipo de Expertos en Ciencia y Tecnologia, 2022)

“La ciberdelincuencia es una actividad delictiva que tiene como objetivo principal un ordenador, una red asociada a este o un dispositivo conectado. No obstante, aunque la creencia más arraigada en la sociedad es que es llevada a cabo por individuos o ciberdelincuentes, la ciberdelincuencia también puede ser practicada por organizaciones. Incluso los Estados utilizan herramientas para acometer ciberataques a otras naciones”. (Red Seguridad, 2022)

En otras palabras, el autor los identifica como la persona quien realiza la infracción o daño utilizando sus conocimientos informáticos para su ejecución.

1.1.5. Hacker.-

Según la Real Academia Española (RAE) “un Hacker o Pirata Informático es una persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora.” (Campus Internacional Ciberseguridad, 2022)

Persona especializada en altos conocimientos y estrategias en tecnología, que además de sus técnicas de programación y software de computadoras puede entrar a una red, alterar una base de datos, y apropiarse de perfiles digitales para alterar información.

1.1.6. Hosting.-

“Un hosting es un servicio de alojamiento en línea que te permite publicar un sitio o aplicación web en Internet. Cuando obtienes un hosting, básicamente alquilas un espacio en un servidor que almacena todos los archivos y datos de tu sitio web para que funcione correctamente. En este artículo aprenderás todos los detalles sobre qué es un hosting.” (Gustavo B., 2022)

Para el autor un hosting es como el alquiler un espacio en la red donde las empresas pagan un valor mensual o anual para que sus archivos almacenados en un lugar seguro y confiable y con la disponibilidad 24/7.

1.1.7. Infracción Informática.-

“Las infracciones informáticas son aquellas acciones de carácter administrativo antijurídicas y culpables que se dan por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de internet.” (Josselyn Asimbaya Guanochanga, 2020)

En otras palabras, es todo acto mal intencionado cometido por los hackers o intrusos en una red con el fin de alterar, modificar, eliminar cualquier información que se encuentre dentro de una red.

1.1.8. Firma Electrónica.-

“Art. 20.- Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.” (Ley de Comercio Electronico, 2002)

Dicha firma sirve para certificar y darle validez a la persona titular de un documento.

1.1.9. Ingeniería Social.-

“La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados.” (Kapersky, s.f.)

“La definición de ingeniería social abarca varios tipos de manipulación psicológica. En ocasiones, la ingeniería social puede tener resultados positivos, como fomentar comportamientos saludables. En términos de seguridad de la información, sin embargo, la ingeniería social a menudo se utiliza únicamente para beneficio del atacante. En estos casos, **la ingeniería social implica manipulación para obtener información confidencial**, como datos personales o financieros. Por tanto, la ingeniería social también puede definirse como un tipo de ciberdelito.” (Danielle Bodnar, 2021)

Los hackers se aprovechan de la falta de conocimiento por parte de los usuarios, ya que los avances tecnológicos se actualizan día a día, por eso numerosos usuarios son atacados por este medio.

Un ejemplo en este caso puede ser que una persona finja ser un empleado de un banco o de alguna entidad financiera con el fin de enviar una solicitud de renovación de datos por un formulario falso, lo cual esta hace que el usuario que desconoce ingrese sus datos y así permitiéndole al hacker atacar y utilizar su información.

1.1.10. National Center for Computer Crime Data.-

"El Centro Nacional de Datos sobre Delitos Informáticos es un instituto de investigación que estudia e informa sobre los medios para facilitar la prevención, detección, investigación y enjuiciamiento de los delitos informáticos." (Schweitzer, 1987)

1.1.11. Inter-Pact computer security organization.-

"Interactive es un proveedor de servicios de ciberseguridad gestionados. Su objetivo es mejorar la seguridad y la resiliencia de los clientes a través de inteligencia basada en datos, basada en una asociación de confianza. Mejorar la resiliencia de su negocio a través de inteligencia de seguridad basada en datos, basada en una asociación de confianza." (Interactive Security, s.f.)

1.2. Tipos de delitos informáticos

1.2.1 Phishing.-

En un estudio el Abg. Carlos Alcívar Trejo del libro el phishing como nueva modalidad de fraude en la era digital define al phishing en su Capítulo III pagina 40 como "una técnica que se utiliza para duplicar una página web o manipular el diseño de correo electrónico logrando que cualquier enlace que generen los phishers parezca legítimo y así hacen creer al usuario que se encuentran en una página oficial y que el correo que reciben proviene de una identidad segura y lo utilizan generalmente en páginas de instituciones bancarias para poder tener el login y la contraseña del cliente de la institución y así poder realizar diversos delitos." (Carlos, s.f.)

Por otro lado la entidad bancaria Banco del Pichincha define "El phishing es un ataque informático de ingeniería social que usa medios de comunicación digitales, como el correo electrónico, para engañar y estafar a las personas. A través de técnicas de manipulación emocional genera confianza en las personas para poder robar su información y dinero." (Banco de Pichincha, 2020)

“El objetivo del phishing es engañar a las personas para obtener datos confidenciales, como contraseñas e información bancaria. Este cibercrimen se comete a través de correos falsos, mensajes o llamadas telefónicas. El estafador utiliza una identidad falsa para obtener los datos que necesita y cometer delitos como el robo de dinero en cuentas bancarias.” (Banco de Pichincha, 2020)

El autor menciona que en los últimos años personas, entidades financieras, negocios, se han visto afectados por este método de suplantación de identidad, lo cual ha causado y originado una red fraudulenta que debe sancionarse conforme a su grado de infracción.

1.2.2. Spear Phishing.-

“El spear phishing es una estafa de correo electrónico o comunicaciones dirigida a personas, organizaciones o empresas específicas. Aunque su objetivo a menudo es robar datos para fines maliciosos, los cibercriminales también pueden tratar de instalar malware en la computadora de la víctima.” (Kapersky, s.f.)

En la página oficial de Incibe sobre aprender elementos de la ciberseguridad menciona que “el spear phishing consiste en una modalidad phishing dirigida contra un objetivo específico, en el que los atacantes intentan, mediante un correo electrónico, conseguir información confidencial de la víctima.” (Incibe, 2021)

1.2.3. Virus Informático.-

Según especialista de software malicioso de Norton menciona “que un virus informático, como un virus de gripe, está diseñado para propagarse de un host a otro y tiene la habilidad de replicarse. De forma similar, al igual que los virus no pueden reproducirse sin una célula que los albergue, los virus informáticos no pueden reproducirse ni propagarse sin programar, por ejemplo, un archivo o un documento.” (Norton Life Lock, s.f.)

Por otro lado, el autor Gonzalo Torres define “Los virus, una de las amenazas informáticas más antiguas, son un desagradable tipo de malware que secuestra los recursos del equipo para replicarse, propagarse y sembrar el caos. Siga leyendo y aprenda cómo funcionan los virus y cómo puede proteger su equipo ante ellos, aplicando tanto el sentido común como una herramienta dedicada de ciberseguridad.” (Gonzalo Torres, 2022).

El autor explica que los virus pueden ingresar en cualquier sistema por algún archivo infectado, transferido desde un dispositivo móvil, desde una cuenta de correo, descargado de la web, o cualquier otro medio de transferencia de información, con la finalidad de contaminar y multiplicarse en todo un sistema informático.

1.2.4. Malware.-

Iván Belcic, empleado de Avast, define “Malware es un término general para referirse a cualquier tipo de “**mal**icious soft**ware”** (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento. Hay muchos tipos de malware y cada uno busca sus objetivos de un modo diferente. Sin embargo, todas las variantes comparten dos rasgos definitorios: son subrepticios y trabajan activamente en contra de los intereses de la persona atacada.” (Ivan Belcic, 2022)

De acuerdo a esta definición, podemos definir al malware como otro tipo de ataque informático o cibernético que usa los virus, spam y otros para aprovechar las debilidades de un sistema y de esa manera inactivar los controles informáticos del dispositivo.

1.2.5. Ciberterrorismo.-

“El Ciberterrorismo consiste en el uso de medios tecnológicos por parte de grupos terroristas para cometer una intrusión, un fallo o un ataque en los sistemas informáticos o las redes de telecomunicaciones de instituciones políticas, económicas o sociales.” (Universidad Europea, 2022)

Este tipo de delito informático busca desestabilizar a un país o gobierno, utilizando métodos de sabotaje introduciendo virus, suplantando identidad, realizando ataques informáticos y requieren de menor financiamiento que un ataque terrorista común.

1.2.6. El espionaje informático.-

"El espionaje informático también utiliza programas del tipo spyware, que se instalan en nuestros dispositivos sin consentimiento y monitorean los movimientos de los usuarios conectados a Internet para obtener un perfil comercial completo de cada uno de ellos, estos programas se apoderan de la información personal de cada usuario y es transferida a la sede de una empresa de espionaje con la finalidad de ser comercializadas." (Quanti, 2022)

Estos spywares ingresan a nuestros dispositivos cuando la persona descarga algún elemento o programa que incluye un archivo malicioso ejecutable que rastrean los datos que se encuentran almacenados en la computadora.

1.2.7. Piggybacking.-

El proveedor de ciberseguridad Sababa Security nos define "El Piggybacking representa aquella situación en la cual alguien accede a un área reservada con el permiso, en la mayor parte de los casos obtenido mediante engaño, de una persona autorizada." (Sababa Security, 2021)

Se trata de figuras que participan en los delitos suplantando a la persona, utilizando su nombre para cometer delitos informáticos mediante el engaño para obtener la información.

1.2.8. Ransomware.-

En definición del portal We Live Security sobre seguridad informática menciona que "El Ransomware es un tipo de malware que luego de comprometer

un equipo secuestra la información y exige el pago de un rescate para recuperar los datos y evitar otros daños colaterales.” (We Live Security, 2021)

Este tipo de malware busca extorsionar a su víctima, pretendiendo que esta le entregue un pago para la recuperación de sus datos.

1.2.9. Smishing.-

El Instituto Nacional de Ciberseguridad (INCIBE) define el smishing como una técnica que consiste en el envío de un SMS por parte de un ciberdelincuentes a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. Con el objetivo de robar información privada o realizarle un cargo económico. Generalmente el mensaje invita a llamar a un número de tarificación especial o acceder a un enlace de una web falsa bajo un pretexto. (Incibe, s.f.)

Ejemplo de esta técnica puede ser que una persona con perfil incógnito envíe por vía sms un link ofreciendo alguna oferta laboral o anuncio falso haciendo creer al usuario que la información es real para luego acceder y una vez ingresado al link o habiendo agregado sus datos, le permite al ciberdelincuente tener acceso a toda su información que tenga agregada en archivos, cuentas bancarias, contactos, y perfiles en redes sociales.

1.3 MARCO JURÍDICO

En el Ecuador existen varias normativas legales en relación al tema de la presente investigación sobre los delitos informáticos, entre ellos:

1) Constitución de la República del Ecuador, Registro Oficial 449 de 20 de octubre del 2008.
2) Ley de Derechos Humanos
3) Ley de Comercio Electrónico, Firmas y Mensajes de Datos, Registro Oficial Suplemento 557 de 17 de abril del 2002.

4) Código Orgánico Integral Penal, Registro Oficial Suplemento 180 de 10 de febrero del 2014.
5) Código de Procedimiento Penal, Registro Oficial Suplemento 360 de 13 de enero del 2000.

INFRACCIONES INFORMATICAS	REPRESION	MULTAS
Delitos contra la información protegida (CPP Art. 202)	6 meses a 1 año	$500 a $1000
1. Violentando claves o sistemas accede u obtiene información	1 a 3 años	$1.000 - $1500
2. Seguridad nacional o secretos comerciales o industriales	3 a 6 años	$2.000 - $10.000
3. Divulgación o utilización fraudulenta	6 a 9 años	$2.000 - $10.000
4. Divulgación o utilización fraudulenta por custodios	2 meses a 2 años	$1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	3 a 6 años	---
Falsificación electrónica (CPP Art. 353)	3 a 6 años	---
Daños informáticos (CPP Art. 415)		
1. Daño dolosamente	6 meses a 3 años	$60 - $150
2. Servicio público o vinculado con la defensa nacional	3 a 5 años	$200 - $600
3. No delito mayor	8 meses a 4 años	$200 - $600
Apropiación ilícita (CPP Art. 553)		
1. Uso fraudulento	6 meses a 5 años	$500 - $1000
2. Uso de medios (claves, tarjetas magnéticas, otros instrumentos	1 a 5 años	$1.000 - $2.000
Estafa (CPP Art. 563)	5 años	$500 - 1.000

Tabla No. 1
Fuente: Tesis “REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA” Pag. 54
https://dspace.unl.edu.ec/jspui/bitstream/123456789/20139/1/TESIS%20Luis%20Pablo%20M%c3%a8ndez%20Vanegas-ilovepdf-compressed.pdf

Mediante el proceso de investigación encontramos información sobre los delitos que se encontraban tipificados antes de la derogación y reforma, mismo que se adjuntan para demostrar el tipo de sanción y multa económica que se aplicaba al delincuente informático.

1.4 LEGISLACIÓN COMPARADA

A continuación, el autor incorpora un cuadro con la cantidad de delitos informáticos reconocidos por país o región.

Delitos informáticos tipificados por país

Puesto	País	Cantidad
1.º	República Dominicana	31
2.º	Paraguay	22
3.º	Costa Rica	21
4.º	México	20
5.º	Venezuela	20
6.º	Ecuador	19
7.º	Chile	14
8.º	España	13
9.º	Argentina	13
10	Nicaragua	13
11	Perú	12
12	El Salvador	12
13	Puerto Rico	11
14	Cuba	11
15	Panamá	10
16	Colombia	9
17	Guatemala	9
18	Honduras	8
19	Bolivia	6
20	Uruguay	4
Promedio ponderado general		13,9

Tabla No. 2
Fuente: https://www.redalyc.org/

1.5. ANÁLISIS ESPECÍFICO POR PAÍS

1.5.1 Ecuador - Ley 67 del 2002

Nuestro país cuenta con la Ley 67 del 2002, "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos", cuyo objeto es regular los mensajes de datos, la firma electrónica y la prestación de servicios electrónicos a través de redes de información. Sin embargo, el 28 de enero del 2014, la Asamblea Nacional de la República del Ecuador publicó el Código Orgánico Integral Penal COIP, y deroga el Título V – Capítulo I, referente a las infracciones informáticas, de esta Ley 67.

La pornografía infantil es el delito informático con mayor pena de prisión en Ecuador, aquel que se lleve a efecto mediante el uso de fotografías, filmaciones, grabaciones, transmisión o edición de materiales visuales de desnudos o semidesnudos reales o simulados.

- Art. 103 Pornografía infantil, de 13 a 16 años de prisión.
- Art. 178 Violación del derecho a la intimidad, de 1 a 3 años de prisión.
- Art. 229 Revelación ilegal de información de bases de datos, de 1 a 3 años de prisión.
- Art. 476 Interceptación de comunicaciones, de 3 a 5 años de prisión.
- Art. 232 Ataque a la integridad de sistemas informáticos, de 3 a 5 años de prisión.
- Art. 233 Delitos contra la información pública reservada legalmente, de 3 a 5 años de prisión.
- Art. 234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones, de 3 a 5 años de prisión.
- Pharming y Phishing, pena de 3 a 5 años de prisión.
- Fraude informático, pena de 3 a 5 años de prisión.

1.5.2 Bolivia – Ley No. 1768

Este país cuenta con el título X de los "Delitos contra la libertad" y el título XII sobre los "Delitos contra la propiedad", del libro segundo del Código Penal de Bolivia.

La manipulación informática en beneficio particular o de un tercero, mediante transferencia de datos informáticos, es el delito informático con mayor pena de prisión en Bolivia.

En la actualidad, Bolivia se encuentra desarrollando el proyecto de ley de telecomunicaciones, con la finalidad de modificar los artículos del Código Penal relacionados a la delincuencia informática y de esa manera robustecer y aumentar las penas contra la manipulación informática; la alteración, acceso y uso indebido de datos informáticos y proteger la propiedad intelectual. De la misma manera incorporar artículos respecto a la falsificación y suplantación de identidad; el sabotaje informático y la interrupción del normal funcionamiento de sistemas de información o telecomunicaciones.

1.5.3. Perú - Ley 30096 del 22 de octubre de 2007

Nuestro país vecino del sur, publicó la Ley 30096, el 22 de octubre del 2007, también llamada la ley de delitos informáticos, la cual tiene por finalidad de prevenir y sancionar toda conducta ilícita cometida mediante el uso de las tecnologías de la información o comunicación y que puedan llegar a afectar los sistemas, datos informáticos y otros bienes jurídicos penalmente importantes.

Esta ley, consta de siete capítulos y su finalidad es la de luchar contra la ciberdelincuencia. Entre los siete capítulos tenemos:

1. Finalidad y objeto de la Ley
2. Delitos contra datos y sistemas informáticos
3. Delitos informáticos contra indemnidad y libertad sexuales
4. Delitos informáticos contra la intimidad y el secreto de las comunicaciones
5. Delitos informáticos contra el patrimonio

6. Delitos informáticos contra la fe pública
7. Disposiciones comunes.

Pese a contar con la Ley 30096, el 10 de marzo del 2014, el Congreso de la República del Perú emite la Ley 30171, donde se incluyen los delitos informáticos con mayor pena de prisión.

- Interceptación indebida de datos informáticos.
- Fraude a través de las tecnologías de la información o comunicación,

1.5.4. México - reforma publicada el 6 de junio de 2007

Mediante una reforma publicada el 6 de junio del 2007 se modifica el Código Penal Federal de México, con la finalidad de penalizar las conductas relacionadas con la corrupción de menores e incapaces, la pornografía infantil y prostitución sexual de menores, así mismo se incorporan los delitos en materia de derechos de autor, revelación de secretos y acceso ilícito a sistemas y equipos de informática.

Transmitir, elaborar, reproducir, vender o publicitar material que contenga grabaciones de actos de exhibicionismo corporal, lascivos o sexuales en que participen menores de 18 años, es considerado el delito informático con mayor pena de prisión en México.

El 31 de enero del 2007 México ha sido invitado a adherirse al Convenio de Budapest, adhesión que se encuentra en estado pendiente.

1.5.5. Chile - Ley 19223, del 7 de junio de 1993

Mediante la Ley 19223, del 7 de junio del 1993, el Congreso Nacional de Chile incorpora las figuras penales relativas a la informática con la tipificación de tan solo cuatro artículos que sancionan los delitos informáticos.

Por otro lado, mediante la Ley 18168 del 10 de octubre del 1982, el mismo congreso aprueba la ley general de telecomunicaciones, en la cual se tipifican varias conductas relacionadas con el uso indebido de las telecomunicaciones.

Así mismo, Chile cuenta con un complemento que sanciona el uso indebido de tarjetas de crédito o débito y limita la responsabilidad de los propietarios de tarjetas de crédito por operaciones realizadas con tarjetas extraviadas, robadas o hurtadas.

La difusión pública o privada de cualquier comunicación obtenida de forma fraudulenta a lo establecido en Ley General de Telecomunicaciones, se considera el delito informático con mayor pena de prisión en Chile.

Al igual que México, el Consejo de Europa emitió la invitación a Chile para formar parte del Convenio sobre la Ciberdelincuencia.

1.5.6. Argentina - Ley 26388, del 4 de junio de 2008

Con el objetivo de incorporar y sustituir del código Penal de Argentina varios artículos regulatorios sobre los delitos informáticos se modifica la Ley 26388, del 4 de junio del 2008.

Defraudar con nombre supuesto, calidad simulada, títulos falsos, influencia, abuso de confianza o aparentando bienes, negociaciones valiéndose de trucos o engaños, mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de sistemas informáticos, se considera el delito informático con mayor pena de prisión.

En marzo del 2010, Argentina fue invitada a adherirse al Convenio sobre la Ciberdelincuencia.

1.5.7. Panamá - Ley 14 de 2007

"Delitos contra la seguridad jurídica de los medios electrónicos", es el nombre que identifica a la ley que regula los delitos informáticos en Panamá, Ley 14 del 2007, tipifica principalmente los delitos informáticos en su título VIII.

Los delitos informáticos con mayor pena de prisión en este país son los siguientes:

- Fabricar, elaborar, producir, ofrecer, comercializar, exhibir, publicar, publicitar, difundir o distribuir a través de Internet o de cualquier medio masivo de comunicación o información, material pornográfico.
- Utilizar Internet, para el entrenamiento en la construcción de artefactos explosivos o el reclutamiento de personas, para la ejecución de actos con fines terroristas.

El 5 de marzo de 2014 se ratifica la adhesión de Panamá al Convenio sobre la Ciberdelincuencia y se convierte en el segundo país latinoamericano, después de República Dominicana, en ratificar el convenio citado.

1.5.8. República Dominicana - Ley 53 del 2007

El Congreso Nacional de la República Dominicana incorpora la Ley 53 del 2007, sobre "crímenes y delitos de alta tecnología", cuya finalidad es la de proteger los sistemas de tecnologías de la información y comunicación de forma integral.

Los delitos informáticos con mayor pena de prisión en esta nación son los siguientes:

- El sabotaje, espionaje o suministro de informaciones, a través de un sistema informático, electrónico, telemático o de telecomunicaciones.
- Ejercer actos de terrorismo, con el uso de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones.

La República Dominicana es el primer país latinoamericano en ratificar el Convenio sobre la Ciberdelincuencia, siendo un modelo para Sur y Centroamérica.

1.5.9. Colombia - Ley 1273, del 5 de enero de 2009

El Código Penal Colombiano fue modificado el 5 de enero del 2009, mediante la Ley 1273, con la finalidad de crear un nuevo bien jurídico tutelado denominado "De la protección de la información y de los datos", además de

preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

El hurto por medios informáticos y similares, es el delito informático con mayor pena de prisión.

El hurto informático consiste en superar medidas de seguridad informáticas para apoderarse de una cosa mueble ajena, con el fin de obtener provecho para sí o para otro, mediante la manipulación de un sistema informático, una red de sistema electrónico o mediante la suplantación de identidad ante sistemas de autenticación y de autorización.

El 11 de septiembre de 2013, Colombia ha sido invitada a adherirse al Convenio sobre la Ciberdelincuencia, con la posibilidad de ser parte de su protocolo adicional, relativo a la penalización de actos de índole racista y xenófoba, cometidos por medio de sistemas informáticos.

1.5.10. Análisis Comparativo

Luego de este análisis, es justo reconocer que República Dominicana se caracteriza por ser una de las naciones con mayor severidad penal en lo relacionado con la delincuencia informática, ya que cuenta con el mayor número de delitos informáticos tipificados y las más altas penas de prisión.

Sin embargo, existen otros países como Uruguay y Bolivia donde los delitos informáticos no implican la privación de la libertad, lo que podría encadenar que sea un estímulo para los delincuentes en el desarrollo de la delincuencia informática.

Por otra parte, podemos apreciar que varios países de habla hispana ya han sido invitados a conformar el convenio de Budapest, con la finalidad de fortalecer su legislación sobre los delitos informáticos.

Así mismo, existen países que castigan con pocos meses de prisión las conductas penales relacionadas con la delincuencia informática, otros cuentan con una cantidad aceptable de delitos informáticos tipificados y un buen número de penas máximas en meses de prisión.

En general, la mayoría de los países comparados en esta investigación, de una u otra manera, se encuentran preocupados por las conductas como acceso o interceptación ilícita a redes y sistemas informáticos, ataques a la integridad de los datos y de los sistemas y falsificación o fraude informático.

METODOLOGÍA DEL PROCESO DE INVESTIGACIÓN

CAPÍTULO II

2.1. ENFOQUE DE LA INVESTIGACIÓN

Este proyecto investigativo ha sido construido con un enfoque de investigación cualitativa, la misma que abarca situaciones en ambientes reales, analizando diversas realidades subjetivas de las personas y de las pequeñas y medianas empresas, las mismas que a consecuencia del tema de investigación, se han visto afectadas en su economía, credibilidad, imagen, productividad y hasta en la intimidad.

La investigación cualitativa implica recopilar y analizar datos no numéricos para comprender conceptos, opiniones o experiencias, así como datos sobre experiencias vividas, emociones o comportamientos, con los significados que las personas les atribuyen. Por esta razón, los resultados se expresan en palabras.

Es de vital importancia profundizar en el tema de investigación y las graves consecuencias a falta de una adecuada tipificación penal sobre los delitos informáticos en el Ecuador, por ser un hecho que afecta directa o indirectamente a gran parte de nuestra población.

2.2. TIPO DE INVESTIGACIÓN

Respecto al tipo de investigación utilizado en el presente trabajo, es exploratorio y explicativo al encontramos frente a un tema levemente estudiado en nuestro medio y que actualmente es necesario reformarlo o adaptarlo a las necesidades como país.

La investigación exploratoria es un tipo de investigación utilizada para estudiar un problema que no está claramente definido, por lo que se lleva a cabo para comprenderlo mejor y la investigación explicativa es aquella que tiene relación causal; no sólo persigue describir o acercarse a un problema, sino que intenta encontrar las causas del mismo.

Para ello, el autor ha identificado las causas que provocan la presencia de este tipo de delito, por qué se presentan y bajo qué condiciones, para posterior analizar las afectaciones y los puntos negativos de la temática, la cual podemos revisar en el Código Orgánico Integral Penal y la Ley de comercio

electrónico y firmas digitales, siendo para ello indispensable una variación en la disposición legal de la norma con la finalidad de mejorar la seguridad de las personas y de las empresas.

2.3. UNIVERSO Y MUESTRA DE LA INVESTIGACIÓN

Los instrumentos seleccionados para la recolección de datos del presente trabajo de investigación fueron las encuestas y entrevistas a expertos. Para la ejecución de las encuestas se definió una muestra aleatoria entre una población de 200 profesionales universitarios de las áreas del derecho procesal y penal; y, de expertos informáticos e ingenieros en IT de las diversas universidades de Guayaquil, entre ellas la Universidad Católica, Universidad de Especialidades Espíritu Santo y Universidad Estatal de Guayaquil.

Estos instrumentos permiten obtener un gran aporte y relevantes conocimientos sobre el tema de investigación. Por otro lado, la entrevista a expertos, en cada una de sus áreas, permitió conocer detalladamente ciertos casos comunes que se dan en la práctica profesional.

Para el cálculo de la muestra se utilizó una aplicación en internet localizada en el sitio https://es.wikihow.com/calcular-el-tama%C3%B1o-de-una-muestra la cual nos dio como resultado una muestra de 100 personas.

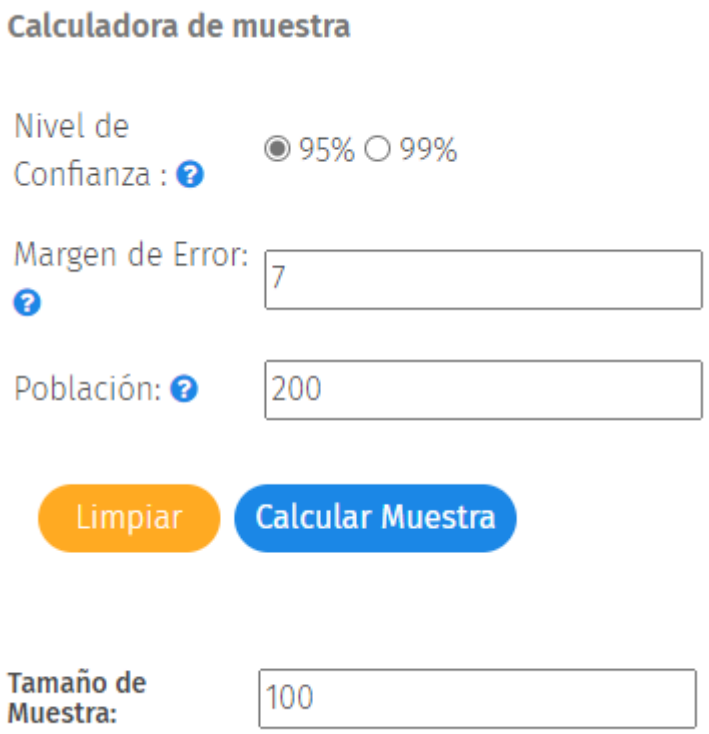


Imagen No. 1
Elaborado por: Cristopher Cires Saona
Fuente:https://es.wikihow.com/calcular-el-tama%C3%B1o-de-una-muestra

Hipótesis: Si existiese una adecuada tipificación penal, con reformas actualizadas y que guarden relación con el perjuicio ocasionado a las víctimas, se podría disminuir o mitigar las graves consecuencias sobre los ataques o delitos informáticos en el Ecuador.

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA INVESTIGACIÓN

CAPÍTULO III

3.1. Metodología

La falta de tipificación penal sobre los delitos informáticos en el Ecuador.

El presente trabajo de investigación corresponde básicamente a un estudio exploratorio y bibliográfico, es decir, consiste en la observación directa de los objetos en cuanto a su estructura, comportamiento y circunstancia en que se dan ciertos hechos, cuyo propósito es describir, interpretar, entender su naturaleza y factores constituyentes.

Un estudio exploratorio sirve para preparar el terreno, y generalmente anteceden a los otros tipos de estudios. Los estudios exploratorios se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes.

Por otro lado, la investigación documental o bibliográfica es aquella que procura obtener, seleccionar, compilar, organizar, interpretar y analizar información sobre un objeto de estudio a partir de fuentes documentales, tales como libros, documentos de archivo, hemerografía, registros audiovisuales, entre otros.

Los datos de interés serán reales, recogidos de manera directa; o sea se trata de una investigación a partir de datos primarios u originales recogidos de la población de la investigación, que para el efecto se han seleccionado a diversos profesionales, docentes y expertos en las áreas del derecho penal y de tecnologías de la información y comunicación de las distintas universidades de Guayaquil.

Este trabajo de tesis se encuentra fundamentado en el estudio bibliográfico y documental del tema, este tipo de investigación tiene su peculiaridad en el manejo de libros, leyes, códigos, documentos y artículos publicitarios de fuentes reconocidas y válidas, que permitan conocer, comparar y derivar los diferentes enfoques y criterios, recogiendo las recomendaciones de los diversos autores e instituciones analizadas, con el propósito de incrementar el conocimiento y elaborar nuevas propuestas, en el proyecto de investigación.

3.2. Aplicación del Instrumento-encuesta

- Encuestas a la muestra seleccionada utilizando formularios de google docs, enviadas a los correos electrónicos de los diversos profesionales de las Universidades de Guayaquil.
- Tabulación de los resultados utilizando Excel como hoja de cálculo
- Análisis de los resultados y representación en gráficos estadísticos.

3.3. Aplicación del Instrumento-entrevista

1. Preparación del cuestionario de preguntas para la entrevista.
2. Entrevistas dirigidas a dos especialistas Dr. Leopoldo Larrea Simball, experto derecho penal y el Master Christian Cires Larrea, experto en tecnología y seguridades.
3. Análisis y conclusiones de las entrevistas realizadas.

La entrevista: En este instrumento utilizamos términos cordiales, adecuados y de mucho respeto para nuestros entrevistados, las preguntas con las cuales se trabajaron cumplían con un orden para poder lograr el objetivo deseado.

Grabaciones: Para este tipo de trabajo fue importante contar con evidencias que nos permitan formalizar la información obtenida. Estas evidencias por medio de imágenes, sonidos, datos, pronunciación o demás, registradas en video-cámaras, celulares, un grabador portátil facilitan tener pruebas de lo investigado para después poder reproducirlo.

3.4 Procesamiento y análisis

Luego de receptar las encuestas de cada uno de los profesionales que fueron objeto de estudio, se procedió a clasificar y analizar la información recabada mediante el software de análisis estadístico Excel y posteriormente se

representó en gráficos estadísticos los resultados obtenidos de nuestro estudio y se determinó la verificación de las hipótesis.

3.5 ENTREVISTAS

Entrevista realizada a Abogado penalista.

Dr. Leopoldo Larrea Simball – Abogado en derecho penal y procesal.

1. **¿Quiénes son estas personas que cometen delitos o infracciones informáticas?**

Son delincuentes, generalmente no identificados por falta de seguimiento, control y porque no son denunciados. Más del 80% de los casos de delitos informáticos no son denunciados en nuestro país.

2. **¿Muchos piensan que el cometer un delito por Internet hace "imposible" localizar al criminal o delincuente?**

No es imposible. Si es complicado por la falta de evidencia que se obtiene en cada uno de los casos, pero es ahí cuando debe entrar en juego el conocimiento de los abogados, peritos y especialistas, porque todo deja rastro por pequeño que sea.

3. **Tengo la impresión de que los delincuentes informáticos son más preparados e incluso van por delante de cualquier experto en seguridad informática. ¿Eso es así?**

Muchas veces no. Somos nosotros mismos los que no mantenemos el cuidado de nuestra información. Es como cuando sales de casa, no dejas la puerta abierta, la ventana sin seguro o tu billetera en el balcón al acceso de todos. Así como mantienes seguridades en tu casa, así deben ser contempladas las seguridades al momento de ingresar a una red por privada que esta sea.

4. **¿Considera que se deben endurecer las sanciones a los piratas informáticos?**

Insisto en lo comentado anteriormente, no solo se trata de cambiar nuestra legislación, sino que se debe cambiar la mentalidad de las personas que piensan que pueden ingresar a cualquier red y compartir información, a contestar cualquier mensaje o correo desconocido con datos personales, a publicar

información íntima de la familia por las redes, en fin. Nada vamos a lograr endureciendo las penas sin cambiar de actitud.

5. **¿Según su opinión, la justicia ecuatoriana está preparada para enfrentar delitos informáticos?**

Considero que necesitamos prepararnos ante tantos avances tecnológicos. En esta preparación debemos incluir a todas las personas que administran justicia en nuestro país.

Entrevista realizada a profesional en Tecnologías.

Master Christian Cires Larrea – Ingeniero de Sistemas y experto en IT

1) **¿Quiénes son estas personas que cometen delitos o infracciones informáticas?**

Generalmente son jóvenes estudiantes de informática que parecen tener unos conocimientos muy superiores a quienes velan por la seguridad de las redes, que andan en búsqueda de vulnerabilidades de las personas o empresas para obtener información.

2) **¿Estas vulnerabilidades que usted habla son responsabilidad de la persona, del encargado del departamento de informática o del proveedor de los servicios de internet?**

Realmente el hacker es quien ingresa como intruso a una red, pero el ingresa porque la persona o empresa no tiene las seguridades para detectar al intruso o no tiene las seguridades para bloquear los accesos desde fuera de una organización. Sin embargo, el proveedor de internet también tiene parte de responsabilidad.

3) **Tengo la impresión de que los delincuentes informáticos son más preparados e incluso van por delante de cualquier experto en seguridad informática. ¿Eso es así?**

Bueno, relativamente es así. Este tipo de personas son obsesionados por violar las seguridades u obtener lo que desean, muchos de ellos simplemente lo

hacen por placer de demostrar que nada los detiene. A esto se suma los nuevos métodos o mecanismos de estafa que inventan cada día y los cuales se tarda mucho en detectarlos y posterior mucho tiempo en solucionarlos.

4) **¿Considera que se deben endurecer las sanciones a los piratas informáticos?**

Definitivamente. En nuestro país las sanciones son muy débiles versus el daño o perjurio que estas ocasionan. Por ejemplo hay sanciones que van desde 2 meses de prisión y multa de $600 a personas que comercialicen o dañen base de datos de empresas. Cuando el valor económico de una base de datos de una empresa tiene un valor, muchas veces, incalculable.

5) **Según su opinión, ¿la justicia ecuatoriana está preparada para enfrentar delitos informáticos?**

Este tema de los delitos informáticos no es nuevo, sin embargo considero que se debe actualizar la legislación para enfrentar los delitos informáticos. Por otro lado, preparar o capacitar tanto fiscales como jueces en el manejo de la evidencia digital, que es uno de los elementos fundamentales para este tipo de infracción. Tengo entendido existen convenios internacionales de cooperación contra los delitos informáticos, considero que Ecuador podría ir por esa línea para buscar el respaldo de países que tienen mayor experiencia en este tipo de infracción.

Resultados y análisis de las encuestas

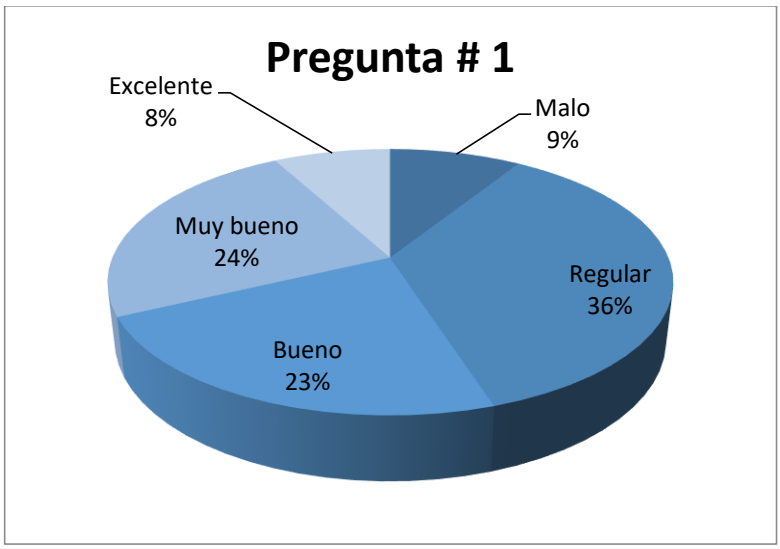
1.) ¿Cuál es su nivel de conocimiento respecto a las diversas técnicas o formas de los delitos o ataques informáticos detectados con mayor frecuencia en nuestra ciudad?

CUADRO No. 1

Encuestados	Cantidad	Porcentajes
Malo	9	9%
Regular	36	36%
Bueno	23	23%
Muy bueno	24	24%
Excelente	8	8%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 1



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

Como podemos observar, aproximadamente la mitad de nuestra población presenta un desconocimiento sobre la diversidad y formas de delitos informáticos detectados en nuestra ciudad. Solo un 8% considera mantener un alto nivel de conocimiento sobre esta modalidad de amenaza.

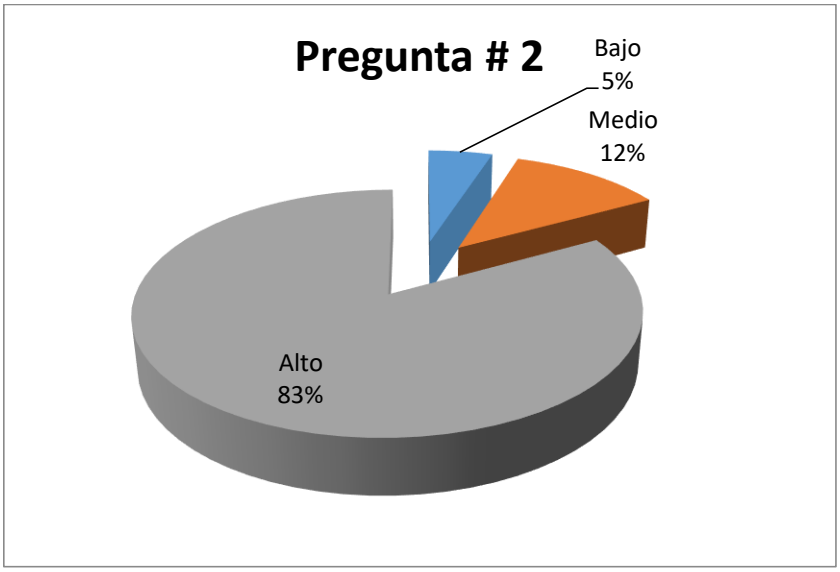
2.) Según su experiencia. En qué grado de afectación, considera usted, que están siendo amenazadas las personas y las pequeñas y medianas empresas por los delitos o ataques informáticos, como, por ejemplo, suplantación de identidades, rodo o secuestro de datos e información o extorsiones.

CUADRO No. 2

Encuestados	Cantidad	Porcentajes
Bajo	5	5%
Medio	12	12%
Alto	83	83%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 2



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

Como podemos observar, nuestros encuestados consideran que existe un alto riesgo de ataques informáticos para las personas y las PYMES, presumiblemente por ser el grupo que presenta más vulnerabilidades en sus redes. A esto se podría añadir el mismo hecho que no cuentan con los recursos necesarios para protegerse ante esta nueva modalidad de amenaza.

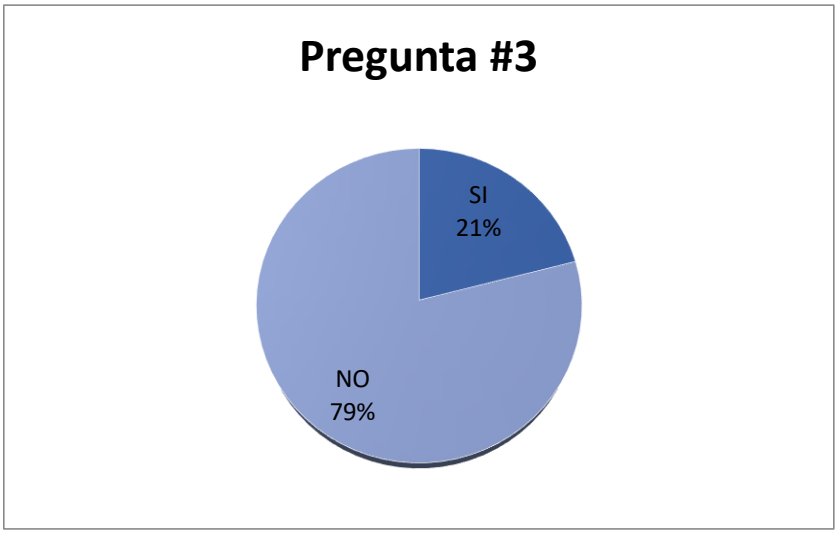
3.) ¿Considera usted que los delitos informáticos en nuestra ciudad reciben el seguimiento, que estos se merecen, por parte de las autoridades?

CUADRO No. 3

Encuestados	Cantidad	Porcentajes
SI	21	21%
NO	79	79%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 3



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

De los profesionales en libre ejercicio de la profesión encuestados, un alto porcentaje considera que no se está otorgando un adecuado seguimiento a los casos de delitos informáticos denunciados por las personas o empresas afectadas. Podríamos concluir que 8 de cada 10 profesionales tiene una mala percepción de los sistemas de administración de justicia del Ecuador, conclusión que probablemente hemos escuchado con frecuencia en los medios de comunicación.

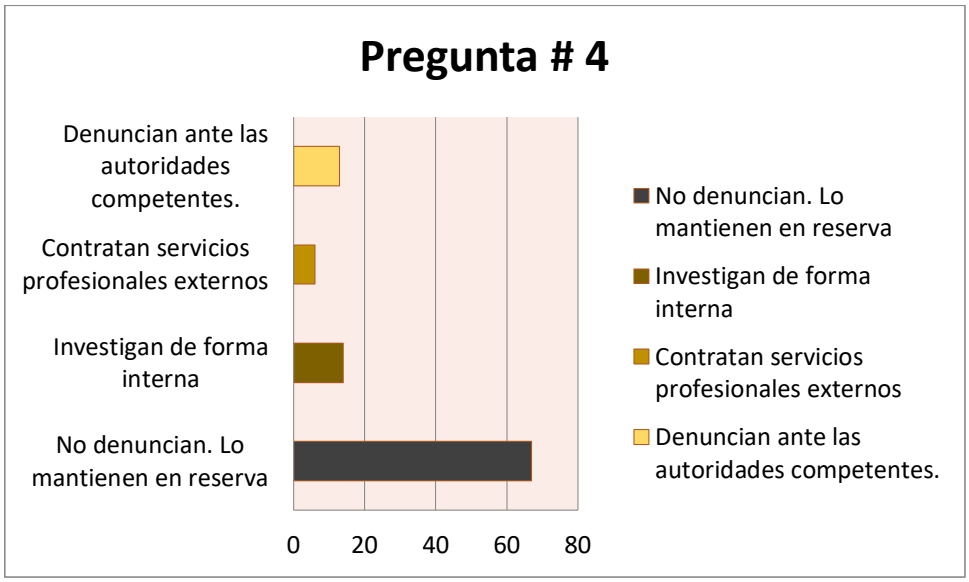
4.) ¿Según su experiencia laboral, cómo actúan las pequeñas y medianas empresas ante la presencia o ejecución de un delito informático?

CUADRO No. 4

Encuestados	Cantidad	Porcentajes
No denuncian. Lo mantienen en reserva	67	67%
Investigan de forma interna	14	14%
Contratan servicios profesionales externos	6	6%
Denuncian ante las autoridades competentes.	13	13%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 4



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

Los resultados de esta pregunta deja en evidencia que las PYMES prefieren mantener en reserva los ataques informáticos a los que han sido expuestos, la mayoría no los denuncia, probablemente con la finalidad de no perder credibilidad frente a la sociedad o por desconfianza en el sistema judicial de nuestra ciudad.

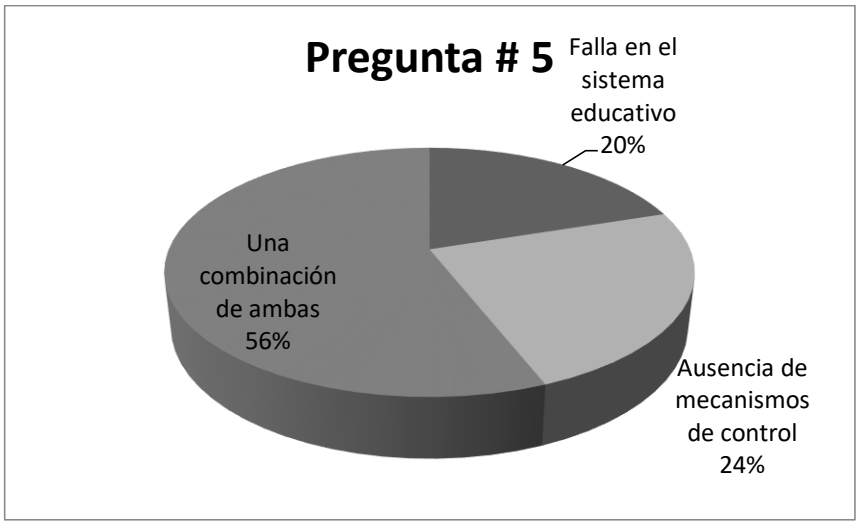
5.) Considera usted que la proliferación o incremento de casos sobre delitos informáticos se debe a una falla en el sistema educativo actual, a la falta de mecanismos de control o una incidencia de ambas.

CUADRO No. 5

Encuestados	Cantidad	Porcentajes
Falla en el sistema educativo	20	20%
Ausencia de mecanismos de control	24	24%
Una combinación de ambas	56	56%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 5



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

Definitivamente nuestros encuestados concuerdan que el incremento de casos respecto a los delitos informáticos en nuestra ciudad se debe a las incidencias de no contar con un sistema educativo que forme a los jóvenes de manera integral y así mismo el no contar con los mecanismos adecuados para que el sistema judicial pueda ejercer control sobre este tipo de amenaza.

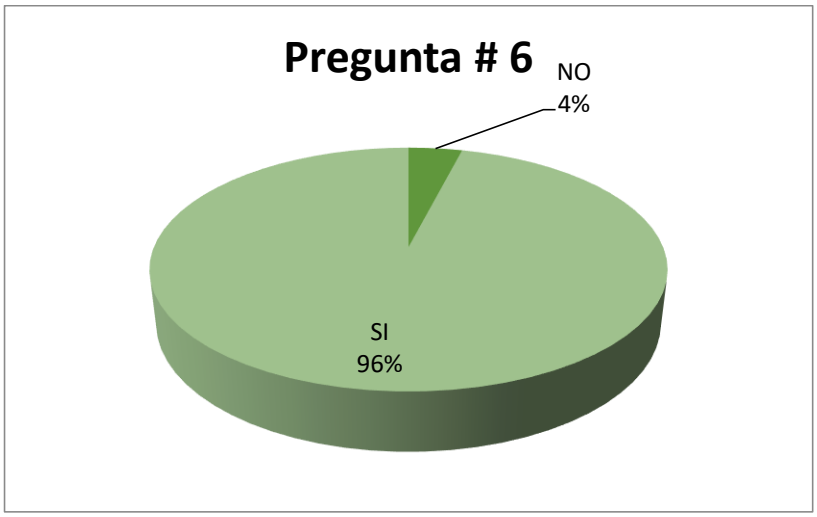
6.) Considera usted, que la pandemia y el crecimiento de la modalidad de trabajo virtual expuso a las personas y a las empresas a ser víctimas de delitos cibernéticos.

CUADRO No. 6

Encuestados	Cantidad	Porcentajes
NO SI	4 96	4% 96%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 6



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

La pandemia no solo cambió la vida de las personas, sino también el enfoque que las empresas daban a sus proveedores y clientes. Ahora la gran mayoría apostó al cambio y funcionan a través de una red y con ello el riesgo inmerso de los ataques informáticos. Por dicha razón nuestros encuestados califican de alto riesgo el ser víctimas de estos delitos.

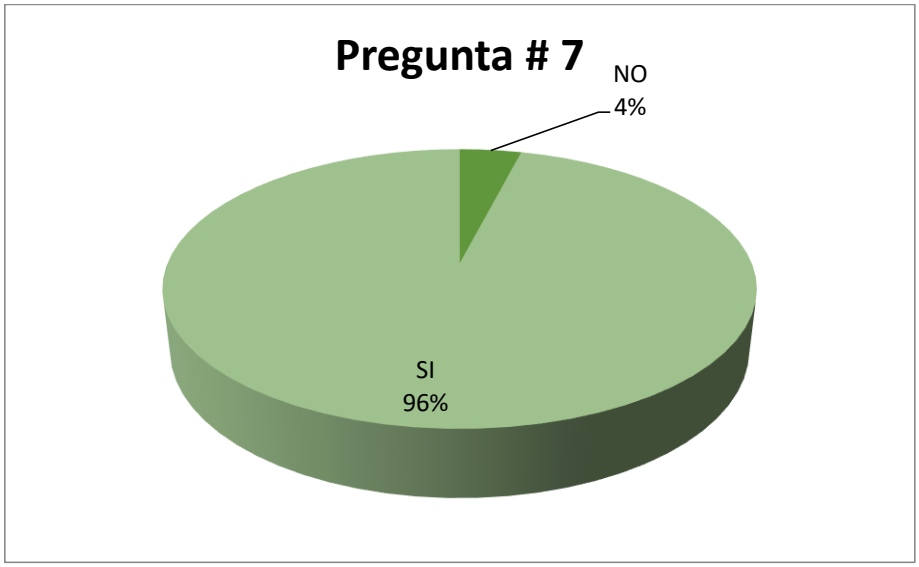
7.) Estos piratas informáticos, hackers o intrusos de la red, utilizan las mismas técnicas tradicionales que usaban antes o han implementado nuevas y mejoradas técnicas con una efectividad tremendamente alta.

CUADRO No. 7

Encuestados	Cantidad	Porcentajes
Técnicas Tradicionales	14	14%
Nuevas formas de ataque	86	86%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 7



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

Uno de cada 10 encuestados afirma que los atacantes o involucrados en los delitos informáticos usan las mismas técnicas tradicionales de años atrás. Sin embargo, 9 de cada 10 afirman que desarrollan nuevas técnicas y cada vez más efectivas con la finalidad de no dejar rastro o evidencia que les permita detectar.

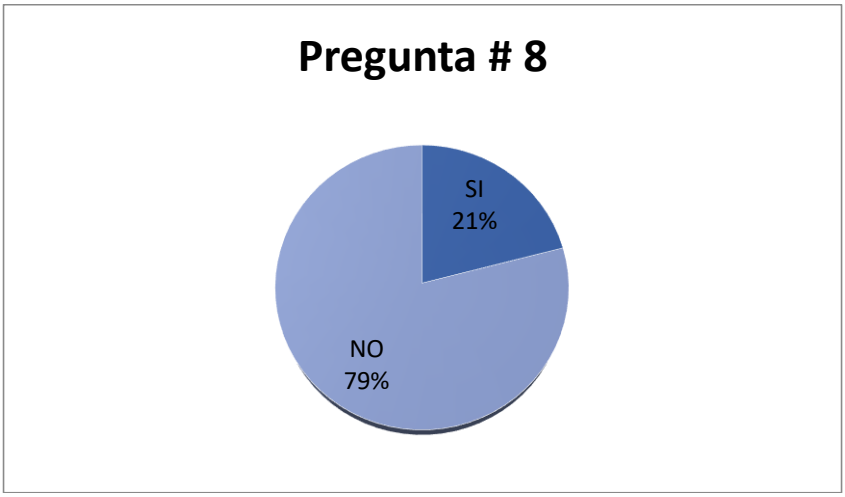
8.) En nuestra ciudad mucho se habla de la transformación digital, de la nueva era de la comunicación y de las tecnologías. ¿Cree usted que es pertinente abordar estos temas de la Ciudad sin tener en cuenta la seguridad y los aspectos legales que esto conlleva?

CUADRO No. 8

Encuestados	Cantidad	Porcentajes
Es indispensable relacionarlas	87	87%
No es necesario relacionarlas	13	13%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 8



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

Para nuestros profesionales, es muy indispensable que exista una armonía entre los cambios tecnológicos, la normativa que los regule y la seguridad que se deba desarrollar o implementar para su utilización.

No puede existir una transformación digital sin el apoyo de un mecanismo de control y seguridad.

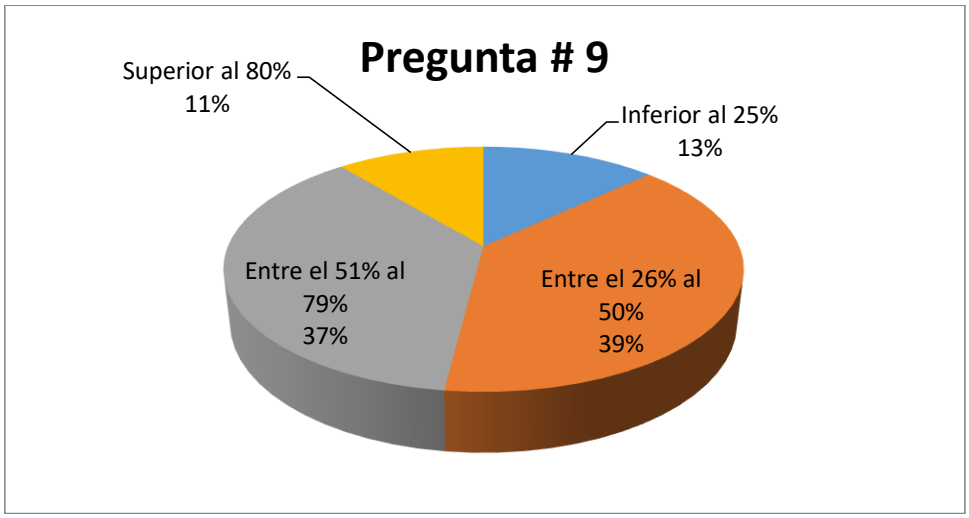
9.) ¿En qué rango de porcentajes usted conoce la ley que regula las infracciones informáticas en el Ecuador, para el efecto, la Ley de Comercio electrónico, firmas digitales y mensaje de datos del Ecuador?

CUADRO No. 9

Encuestados	Cantidad	Porcentajes
Inferior al 25%	13	13%
Entre el 26% al 50%	39	39%
Entre el 51% al 79%	37	37%
Superior al 80%	11	11%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 9



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

Estos resultados confirma que aproximadamente la mitad de nuestros encuestados necesitan conocer acerca de las regulaciones de control sobre los delitos informáticos, para ellos deben prepararse, entrenarse y capacitarse, en nuevas estrategias, conceptos y tecnologías para detectar o identificar a todas estas nuevas formas de delitos que están afectando gravemente a nuestra sociedad.

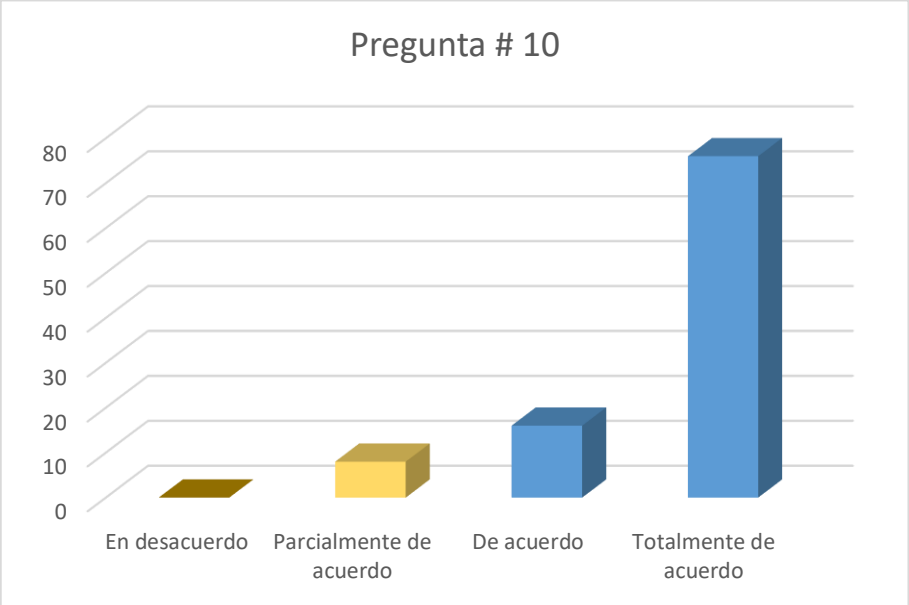
10.) Si existiera la posibilidad de que el Ecuador se adhiera como miembro de algún convenio de cooperación internacional, que provea una normativa legal común entre países, que regule y combata la ciberdelincuencia, ¿usted estaría de acuerdo que el Ecuador participe?

CUADRO No. 10

Encuestados	Cantidad	Porcentajes
En desacuerdo	0	0%
Parcialmente de acuerdo	8	8%
De acuerdo	16	16%
Totalmente de acuerdo	76	76%
	100	100%

Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

GRÁFICO No. 10



Fuente: Profesionales en libre ejercicio de la profesión
Elaboración: Cristopher Cires Saona

ANÁLISIS

Un alto porcentaje de nuestros encuestados considera muy necesaria la implementación de nuevos mecanismos de control, de ser el caso aprobarían que nuestro país participe de forma activa en algún convenio de cooperación internacional que luche contra la ciberdelincuencia.

PROPUESTA

CAPÍTULO 4

Propuesta de Investigación

Antes de finalizar este trabajo de investigación y detallar las conclusiones y recomendaciones, producto del análisis bibliográfico, de los resultados de las encuestas y entrevistas a expertos, el autor considera oportuno sugerir, a través de una propuesta, en este trabajo de titulación, una interesante alternativa para que el Ecuador forme parte, de manera voluntaria, como miembro del convenio de ciberdelincuencia de Budapest, el mismo que regula de forma integral los delitos informáticos.

Esta propuesta surge al evidenciar la necesidad de contar con una normativa integral que regule y penalice este tipo de actividad ilícita. Como es de conocimiento, ante toda necesidad es muy importante encontrar la forma de cubrirla, satisfacerla, de darle un plus o un factor diferenciador, algo que permita cambiar el método actual con el que hemos trabajado, es por ello que se cita al convenio No. 185.

El convenio de Budapest, es un acuerdo transnacional que permite combatir el crimen organizado internacional, específicamente en el campo de los delitos informáticos, su objetivo primordial es establecer una legislación penal y procedimientos comunes entre sus países miembros.

De esta forma, establecer una política penal común aplicable a toda la comunidad internacional y que brinde protección frente a la cibercriminalidad. Además de este propósito, también busca la creación de nuevos mecanismos de cooperación transnacional frente a los delitos cibernéticos

A la fecha los países que se han incorporado a este convenio de cooperación internacional son: Canadá ,Argentina, Australia, Colombia, Cabo Verde, Costa Rica, Chile, Estados Unidos de América, Ghana, Israel, Japón, Filipinas, Mauricio, Panamá, Marruecos, Paraguay, Perú, República Dominicana, Sri Lanka, Senegal, Tonga, Irlanda y Sudáfrica. Por otra parte ya han sido invitados a formar parte del convenio 9 países, entre ellos, Brasil, Burkina Faso,

Guatemala, Nigeria, México, Nueva Zelanda, Níger, y Túnez y 66 Estados entre ellos países europeos,

Será de mucho beneficio para nuestro país, formar parte de este Convenio sobre la Ciberdelincuencia, así como lo es para países vecinos como Colombia, Argentina, Chile y Perú.

Contenido del Convenio de Budapest

El convenio No. 185 también conocido como el Convenio de Budapest contiene una ley de 46 artículos divididos en 4 capítulos, conteniendo el capítulo 1 las referencias a terminologías informáticas y su descripción, en el capítulo 2 se cuenta con las medidas que se deberán adoptar a nivel nacional, el capítulo 3 sobre la cooperación internacional y finaliza con sus cláusulas finales en su capítulo 4.

Clasificación de los delitos en el convenio No. 185

Ante la proliferación de amenazas cibernéticas y la especificidad de nuevos delitos informáticos, este convenio internacional clasifica a los delitos de la siguiente manera:

- Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos;
- Delitos informáticos;
- Delitos relacionados con el contenido (como, por ejemplo, delitos relacionados con la pornografía infantil); y
- Delitos relacionados con infracciones a la propiedad intelectual

Además, el Convenio de Budapest establece que deben ser sancionadas, así mismo, las figuras de tentativa y complicidad en los delitos antes referidos. Inclusive dispone que las sanciones deben ser efectivas, proporcionadas y disuasorias, incluyendo las penas privativas de libertad.

De manera complementaria, este convenio No. 185, incluye un protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la penalización de

actos de índole racista y xenófoba cometidos por medio de sistemas informáticos.

Este protocolo tiene por objeto la lucha contra el racismo, la discriminación racial, la xenofobia y la intolerancia, en el ámbito de los sistemas informáticos -y en particular, a través de Internet-, penalizando jurídicamente los actos racistas y xenófobos.

El objetivo de este protocolo es la asistencia mutua en la legislación penal, en cuanto a la lucha contra el racismo y la xenofobia en la web, así como mejorar la cooperación internacional en esta área.

¿Cómo Ecuador puede formar parte del convenio de Budapest?

Para integrar o adherir a un país es necesario cumplir varios requerimientos solicitados por el consejo de estado del Convenio de Budapest.

Art. 37 El procedimiento de adhesión implica:

1. El ministro de Relaciones Exteriores u otro representante autorizado, del país interesado, deberá enviar una carta dirigida al secretario general del Consejo de Europa en la que manifieste el interés en adherirse al Convenio de Budapest.

2. Una vez que exista un consenso entre los actuales países o Estados que forman parte del Convenio, se invitará al Estado a adherirse.

3. Las autoridades del país interesado, deberán formalizar sus procedimientos internos similares a la ratificación de cualquier tratado internacional, para posteriormente depositar el instrumento de adhesión ante el Consejo de Europa.

CONCLUSIONES

Dentro del escenario de los delitos informáticos, es notorio que en el Ecuador tenemos un problema, por un lado nuestros jueces y fiscales presentan un desconocimiento del tema o no tienen clara la idea sobre la materia penal informática y por otro lado, no se cuenta con una normativa integral que tipifique a estas infracciones de una manera adecuada, ordenada y donde de manera general pueda ser entendida, no solo por fiscales, jueces y abogados, sino por la ciudadanía en general. De aquí nacen las conclusiones de este trabajo de investigación:

1. De los objetivos propuestos para nuestro estudio, se desprende que efectivamente la normativa legal ecuatoriana necesita una actualización en lo que respecta a delitos o infracciones informáticas. Si consideramos los resultados comparativos con las leyes de países vecinos o de habla hispana, podremos evidenciar que la gran mayoría ya es parte o está en proceso de formar parte del Convenio de Budapest contra la ciberdelincuencia, normativa global y actualizada que regula y sanciona los delitos informáticos.

2. De la misma manera, al igual que los países vecinos de habla hispana, existen decenas de países del mundo que se han adherido a este convenio internacional de Budapest, con la finalidad de contar con un marco legal común y actualizado que permita regular las diversas formas y nuevas modalidades de ataques informáticos.

3. Por otro lado, se ha evidenciado que existe un buen porcentaje de desconocimiento respecto a la diversidad de técnicas y formas de delitos informáticos por parte de empresarios, administradores de justicia, y personas en general, lo que ocasiona que existan altos riesgos de vulnerabilidad en cada una de las víctimas.

4. No existen mecanismos ni de control, ni de seguridad, confiables y seguros que brinden la tranquilidad a las personas al momento de transaccionar o transitar dentro de una red informática.

5. El país entero se encuentra sumergido en una tendencia de **"no denunciar un delito"**, sea por miedo, represalia por parte del atacante, por falta de mecanismos de seguridad en el entorno, o por la desconfianza existente en la mayoría de las autoridades que controlan la justicia. Así mismo, se ha evidenciado un seguimiento no adecuado a los diversos casos de ataques de delitos informáticos.

6. Ante esta tendencia de amenazas o ataques informáticos, es obvio que nos encontramos frente a profesionales o expertos en tecnologías carentes de una buena cultura, ética y moral, esperando únicamente incrementar su ego al aprovecharse de las vulnerabilidades de sus víctimas.

7. Por otro lado, se evidencia un alto riesgo de vulnerabilidad en las grandes redes proveedoras de internet, las mismas que deben proporcionar firewalls, filtros, bloqueos, antivirus, antimalware y advertencias ante cualquier amenaza respecto a la seguridad de nuestros datos que navegan por la red.

8. En los últimos dos años se ha evidenciado un incremento de ataques informáticos y alteraciones en las redes de datos y comunicación producto o consecuencia de la pandemia COVID-19 y al crecimiento inesperado y abrupto de la modalidad de trabajo virtual, sin las medidas básicas de control y seguridad.

9. Al igual que en muchas áreas del conocimiento, siempre se está evolucionando en descubrimientos, cambios y tendencias. Así como en la medicina se desarrollan nuevas enfermedades, se crean nuevas vacunas y medicamentos, en tecnología también se implementan nuevas y mejoradas técnicas de ataque informático con alto grado de efectividad, las cuales deben ser combatidas con nuevas herramientas y procedimientos de detección, para lo cual es necesario mantener actualizados a jueces, fiscales, abogados y todo profesional que colabore con la administración de la justicia.

10. Por otra parte, en nuestro medio no existe armonía y coherencia entre la gravedad del perjurio de un delito informático versus la sanción o pena impuesta en la derogada Ley de Comercio Electrónico, Firmas y Mensaje de datos, ahora incorporada en la COIP.

11. Pese a haber sido derogados todos los artículos del título V capítulo I de la Ley de Comercio Electrónico, Firmas electrónicas y Mensaje de datos e incorporados a la COIP, se mantiene una normativa, en cuanto a seguridad informática, muy obsoleta que requiere de una actualización o reforma urgente.

12. Finalmente, luego de una comparativa general con leyes que regulan los delitos informáticos, podemos concluir que nos encontramos muy por debajo en cuanto a normativa y regulación en este tipo de amenazas, a diferencia de países vecinos, como Chile, Argentina, Colombia, México, Perú, entre otros, que han dado un paso más y se han adherido al convenio de cooperación internacional de Budapest, el cual provee una amplia y eficaz normativa internacional que regula los ciberdelitos.

RECOMENDACIONES

Antes de detallar las recomendaciones del siguiente trabajo de investigación, me permito incluir un comentario a criterio personal.

En nuestro país se debe empezar por crear o fomentar una cultura tecnológica, en la cual las generaciones anteriores se vean guiadas, protegidas o educadas por las nuevas generaciones, en temas sobre los mecanismos de protección y de esta forma evitar que sean víctimas de fraudes, extorsiones o cualquier tipo de delito informático.

Y por otro lado, se debe priorizar asignando, de forma adecuada, a los entes administradores de justicia, de manera que cuenten con la capacidad técnica e intelectual necesaria en lo referente a seguridad informática, derecho informático, inteligencia tecnológica y análisis de información.

A continuación detallo las recomendaciones consecuencia de este trabajo de investigación:

1. Tomar como punto de referencia las fortalezas y debilidades de los países vecinos con mayor experiencia en los casos de detección y control de amenazas en delitos informáticos.

2. Incorporar nuevas regulaciones a la legislación ecuatoriana en el ámbito de los delitos informáticos con la finalidad de estar preparados y hacer frente a las nuevas formas infracciones informáticas.

3. Fomentar talleres o cursos de actualización constante a todos los organismos de control y administradores de justicia con la finalidad de reconocer y sancionar de manera correcta cada uno de estos delitos.

4. Capacitar y brindar oportunidades a los negocios particulares y a las pequeñas y medianas empresas para que adopten mecanismos de seguridad informática y prepararlos en estrategias de respaldo y protección de datos.

5. Se sugiere endurecer las penas privativas de libertad y las sanciones correspondientes para aquellas personas que de forma directa o indirecta

participan en los diversos delitos informáticos como suplantación de identidad, robo o manipulación de información, alteración de redes, extorsión, etc.

6. Brindar seguridad a los ciudadanos y a los representantes de las empresas al momento de denunciar acciones delictivas, muchas de las cuales por temor, descrédito o desconfianza en las autoridades administradoras de justicia no son reportadas a tiempo ni de la forma correcta.

7. Reincorporar en las mallas curriculares, sean estas de escuelas, colegio y universidad materias como la ética y la moral, cualidades necesarias que debe desarrollar toda persona en su preparación profesional.

8. Mejorar los tiempos de respuestas y proveer aplicaciones que permitan dar seguimiento a todos los procesos legales que se encuentren activos en los centros de administración de justicia.

9. Exigir que toda compañía proveedora de internet y de seguridad de la información garantice la seguridad total de nuestros datos y de todas las transacciones que se efectúen dentro de una red.

10. Proporcionar talleres, conferencias, charlas, para aquellas personas y empresas que post pandemia, sin estar preparados y sin contar con los recursos físicos y económicos, se arriesgaron a proporcionar diversas soluciones o servicios a la comunidad.

11. Proveer de seguridades informáticas en los espacios públicos y abiertos de nuestra ciudad donde se brinda acceso abierto a las redes.

12. Proponer a las autoridades correspondientes del Ecuador que soliciten la oportunidad de adherirse al convenio de Budapest, el mismo que provee de una amplia normativa legal internacional sobre delitos informáticos, de tal manera que se puedan juzgar a los involucrados con una normativa general y global, con coherencia real y justa entre los daños económicos ocasionados, la violación de intimidad y las sanciones correspondientes.

REFRENCIAS Y BIBLIOGRAFIA

Bibliografía

Banco de Pichincha. (09 de diciembre de 2020). *Banco de Pichincha*. Obtenido de Banco de Pichincha: https://www.pichincha.com/portal/blog/post/que-es-phishing

Campus Internacional Ciberseguridad. (03 de junio de 2022). *campusciberseguridad.com*. Obtenido de Campus Internacional Ciberseguridad: https://www.campusciberseguridad.com/blog/item/133-tipos-de-hackers

Carlos, A. T. (s.f.). *Libros Ecotec*. Obtenido de Libros Ecotec: https://libros.ecotec.edu.ec/index.php/editorial/catalog/download/32/29/241-1?inline=1

Código Orgánico Integral Penal. (17 de febrero de 2021). *Código Orgánico Integral Penal*. Obtenido de Código Orgánico Integral Penal: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Código Penal Sucre. (marzo de 1997). Congreso Nacional de Bolivia. (1997) Ley 1768. *Congreso Nacional de Bolivia. (1997) Ley 1768*. Bolivia: Código Penal Sucre.

Congreso de la República de Colombia. (enero de 2009). Ley 1273. *Protección de la información y de los datos*. Bogotá, Colombia.

Congreso de la República del Perú. (22 de octubre de 2007). Ley 30096. *Ley de Delitos Informáticos*. Perú.

Congreso Nacional de Chile. (marzo de 2005). Ley 20009. *Complemento a la Ley de Delitos Informáticos de Chile*. Chile: Ley 20009 Chile.

Congreso Nacional de la República Dominicana. (2007). Ley número 53. *Crímenes y Delitos de Alta Tecnología*. Santo Domingo, República Dominicana.

Convenio de Budapest sobre la Ciberdelincuencia. (04 de junio de 2021). *Convenio de Budapest*. Obtenido de Convenio de Budapest: https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de

Danielle Bodnar. (29 de octubre de 2021). *Avast*. Obtenido de Avast: https://www.avast.com/es-es/c-social-engineering

Edgar Higuerey. (1 de junio de 2021). *Rock Content*. Obtenido de Rock Content: https://rockcontent.com/es/blog/comercio-electronico/

El Universo. (04 de agosto de 2021). *El Universo*. Obtenido de El Universo: https://www.eluniverso.com/noticias/seguridad/los-delitos-informaticos-con-pena-de-prision-en-ecuador-nota/

Equipo de Expertos en Ciencia y Tecnologia. (10 de enero de 2022). *Universidad Viu*. Obtenido de Universidad Viu: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/ciberdelincuente-una-nueva-alerta-para-nuestra-seguridad

Eserp Busisness & Law School. (s.f.). *Eserp*. Obtenido de Eserp: https://es.eserp.com/articulos/e-commerce-o-comercio-electronico/

Gobierno de México. (junio de 2007). Modificación al Código Penal Federal de México. *Modificación al Código Penal Federal de México*. México: Código Penal Federal de México.

Gobierno de Panamá. (2010). Ley 14. *Ley 14*. Ciudad de Panamá, Panamá: Código Penal de Panamá.

Gonzalo Torres. (29 de marzo de 2022). *Avg*. Obtenido de Avg: https://www.avg.com/es/signal/what-is-a-computer-virus

Gustavo B. (24 de mayo de 2022). *Hostinger* . Obtenido de Hostinger : https://www.hostinger.es/tutoriales/que-es-un-hosting

Incibe. (8 de junio de 2021). *Incibe*. Obtenido de Incibe: https://www.incibe.es/aprendeciberseguridad/spear-phishing

Incibe. (s.f.). *Incibe.com*. Obtenido de Incibe: https://www.incibe.es/aprendeciberseguridad/smishing

Interactive Security. (s.f.). *Interactive*. Obtenido de Interactive: https://www.interactive.com.au/services/cyber-security/

Ivan Belcic. (15 de marzo de 2022). *Avast*. Obtenido de Avast: https://www.avast.com/es-es/c-malware

Janire Carazo Alcalde. (15 de diciembre de 2016). *Economipedia*. Obtenido de Economipedia: https://economipedia.com/definiciones/comercio-electronico-ecommerce.html

Josselyn Asimbaya Guanochanga. (26 de julio de 2020). *Comunidad todo comercio exterior*. Obtenido de Comunidad todo comercio exterior: https://comunidad.todocomercioexterior.com.ec/profiles/blogs/infracciones-inform-ticas-3#:~:text=Las%20infracciones%20inform%C3%A1ticas%20son%20aquellas,electr%C3%B3nicos%20y%20redes%20de%20internet.

Kapersky. (s.f.). *Kapersky*. Obtenido de Kapersky: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

Kapersky. (s.f.). *Kapersky*. Obtenido de Kapersky: https://latam.kaspersky.com/resource-center/definitions/spear-phishing

Ley 1273. (05 de enero de 2009). *Ley 1273*. Obtenido de Ley 1273: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Ley 30096. (20 de diciembre de 2018). *Ley 30096*. Obtenido de Ley 30096: https://cdn.www.gob.pe/uploads/document/file/1671764/Ley%20N%C2%B0%203009 6%20-%20Ley%20de%20Delitos%20Informa%CC%81ticos-.%20%28vigente%29.pdf.pdf

Ley de Comercio Electronico. (17 de abril de 2002). *Ley de Comercio Electronico, Firmas y Mensajes de Datos*. Obtenido de Ley de Comercio Electronico, Firmas y Mensajes de Datos: https://www.telecomunicaciones.gob.ec/wp-

content/uploads/downloads/2012/11/Ley-de-Comercio-Electronico-Firmas-y-Mensajes-de-Datos.pdf

Norton Life Lock. (s.f.). *Norton*. Obtenido de Norton: https://lam.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

Quanti. (21 de enero de 2022). *Quanti*. Obtenido de Quanti: https://quanti.com.mx/articulos/espionaje-informatico-robo-identidad-e-informacion/

Red Seguridad. (17 de enero de 2022). *Red Seguridad*. Obtenido de Red Seguridad: https://www.redseguridad.com/actualidad/cibercrimen/que-es-la-ciberdelincuencia-y-como-se-puede-prevenir_20220117.html

Revista Seguridad 360. (23 de diciembre de 2021). *Revista Seguridad 360*. Obtenido de Revista Seguridad 360: https://revistaseguridad360.com/destacados/tipos-de-delitos-informaticos/

Richard Ramirez. (27 de diciembre de 2017). *Policia Nacional del Ecuador*. Obtenido de Policia Nacional del Ecuador: https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

Sababa Security. (28 de diciembre de 2021). *Sababa Security*. Obtenido de Sababa Security: https://www.sababasecurity.com/es/tailgating-y-piggybacking/

Schweitzer, J. A. (01 de agosto de 1987). *dl.acm.org*. Obtenido de ACM DL Digital Library: https://dl.acm.org/doi/abs/10.1145/36342.1059523#:~:text=The%20National%20Center%20for%20Computer,and%20prosecution%20of%20computer%20crime.

Senado y Cámara de Diputados de la Nación de Argentina. (4 de junio de 2008). Ley 26388. *Ley 26388*. Buenos Aires, Argentina: Código Penal de la Nación Argentina.

Significados.com. (11 de junio de 2022). *Significados.com*. Obtenido de Significados.com: https://www.significados.com/delitos-informaticos/

Universidad Europea. (06 de mayo de 2022). *Universidad Europea*. Obtenido de Universidad Europea: https://universidadeuropea.com/blog/ciberterrorismo/

We Live Security. (21 de mayo de 2021). *We Live Security*. Obtenido de We Live Security: https://www.welivesecurity.com/la-es/2021/05/21/que-es-ransomware/

Libro “El Delito Informático” autor: Leyre HERNÁNDEZ DÍAZ. Editorial EGUZKILORE. Diciembre 2009

Libro “Análisis Espacial de los Delitos y Aplicación de la Normativa Jurídica Ecuatoriana”.Autor: Carlos Alcívar Trejo, Mgs. Juan Tarquino Calderón Cisneros, Mgs. Año 2016.

Libro “¿Vida privada o muerte a la privacidad?: protección de datos personales en la relación empresa-cliente en Ecuador”. Septiembre 2019

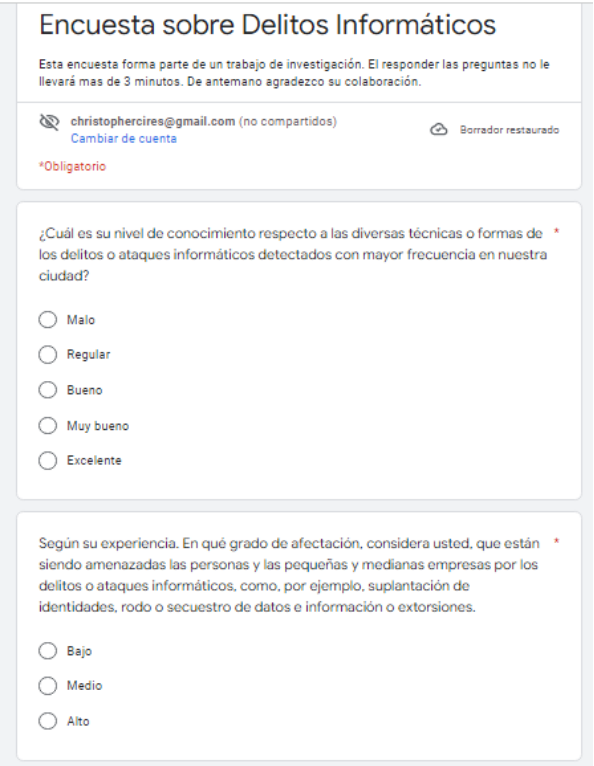
Libro “Los ciberdelitos en el ordenamiento español”. Autor: Alfonso Galan Muñoz.

Libro “Delitos informáticos”. Autor: Laura Davara Fernández. Año: 2017

Libro “Los accesos ilícitos a sistemas informáticos”. Autor: Leyre Hernandez Año; 2019

ANEXOS

Anexo 1. Encuesta sobre Delitos Informáticos



Encuesta sobre Delitos Informáticos

Esta encuesta forma parte de un trabajo de investigación. El responder las preguntas no le llevará mas de 3 minutos. De antemano agradezco su colaboración.

christophercires@gmail.com (no compartidos)
Cambiar de cuenta

Borrador restaurado

*Obligatorio

¿Cuál es su nivel de conocimiento respecto a las diversas técnicas o formas de los delitos o ataques informáticos detectados con mayor frecuencia en nuestra ciudad? *

- Malo
- Regular
- Bueno
- Muy bueno
- Excelente

Según su experiencia. En qué grado de afectación, considera usted, que están siendo amenazadas las personas y las pequeñas y medianas empresas por los delitos o ataques informáticos, como, por ejemplo, suplantación de identidades, rodo o secuestro de datos e información o extorsiones. *

- Bajo
- Medio
- Alto

¿Considera usted que los delitos informáticos en nuestra ciudad reciben el seguimiento, que estos se merecen, por parte de las autoridades? *

- ◯ Si
- ◯ No

¿Según su experiencia laboral, cómo actúan las pequeñas y medianas empresas ante la presencia o ejecución de un delito informático? *

- ◯ No denuncian. Lo mantienen en reserva
- ◯ Investigan de forma interna
- ◯ Contratan servicios profesionales externos
- ◯ Denuncian ante las autoridades competentes.

Considera usted que la proliferación o incremento de casos sobre delitos informáticos se debe a una falla en el sistema educativo actual, a la falta de mecanismos de control o una incidencia de ambas. *

- ◉ Falla en el sistema educativo
- ◯ Ausencia de mecanismos de control
- ◯ Una combinación de ambas

Considera usted, que la pandemia y el crecimiento de la modalidad de trabajo virtual expuso a las personas y a las empresas a ser víctimas de delitos cibernéticos. *

- ◯ Si
- ◯ No

Estos piratas informáticos, hackers o intrusos de la red, utilizan las mismas técnicas tradicionales que usaban antes o han implementado nuevas y mejoradas técnicas con una efectividad tremendamente alta.

- ◯ Técnicas tradicionales
- ◯ Nuevas formas de ataque

En nuestra ciudad mucho se habla de la transformación digital, de la nueva era de la comunicación y de las tecnologías. ¿Cree usted que es pertinente abordar estos temas de la Ciudad sin tener en cuenta la seguridad y los aspectos legales que esto conlleva?

- ◯ Es indispensable relacionarlas
- ◯ No es necesario relacionarlas

¿En qué rango de porcentajes usted conoce la ley que regula las infracciones informáticas en el Ecuador, para el efecto, la Ley de Comercio electrónico, firmas digitales y mensaje de datos del Ecuador?

- ◯ Inferior al 25%
- ◯ Entre el 26% al 50%
- ◯ Entre el 51% al 79%
- ◯ Superior al 80%

Si existiera la posibilidad de que el Ecuador se adhiera como miembro de algún convenio de cooperación internacional, que provea una normativa legal común entre países, que regule y combata la ciberdelincuencia, ¿usted estaría de acuerdo que el Ecuador participe?

- ◯ Estoy de acuerdo
- ◯ En desacuerdo

Enviar Borrar formulario