UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE DERECHO
ESCUELA ACADÉMICO PROFESIONAL DE DERECHO

TESIS

"BLOQUEO DEL IP DINAMICO DENTRO DEL COMERCIO ELECTRONICO COMO MEDIDA DE PREVENCIÓN DE LOS DELITOS INFORMATICOS DE LA LEY 30096"

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADO

PRESENTADO POR:
YORLI ADRIAN LEÓN OCHOA

Asesor:
DRA. MARLENE ELIZABETH CARDOZO QUINTEROS

Línea de Investigación:
DERECHO PÚBLICO

Pimentel – Perú
2018

BLOQUEO DEL IP DINAMICO DENTRO DEL COMERCIO

ELECTRONICO COMO MEDIDA DE PREVENCIÓN DE LOS DELITOS INFORMATICOS

DE LA LEY 30096

Dra. Cardozo Quinteros, Marlene Elizabeth

Asesor Metodólogo

Mg. Pérez Burga, Fátima del Carmen

Presidente del Jurado de Tesis

Mg. Vílchez Castro, Jorge Napoleón

Secretario del Jurado de Tesis

Abg. Samillán Carrasco, José Luis

Vocal del Jurado de Tesis

Índice

DEDICATORIA

Está investigación tiene como dedicación para el gran amor de mi vida mi madre LEÓN OCHOA, Luz Griselda y a mis abuelos LEÓN SANTACRUZ, Adriano y OCHOA MORALES, Margarita, pilares fundamentales en mi vida y a aquella persona que hoy ya no está más, sigue guiando mi camino desde el cielo mi tío, es a él a quien le debo los valores principios y la inspiración para poder seguir con mis sueños y profesión Eliseo Teobaldo Mejía Ochoa, el hecho de que ellos hayan formado parte de mi vida ha hecho que esta investigación haya sido posible de ejecutar.

AGRADECIMIENTO

Agradezco a Dios que me dio fuerza y fe para creer, que lo que parecía imposible, se puede realizar con éxito. A mi familia por apoyarme en cada momento de mi vida. A mi docente y asesora, la Dra. CARDOZO QUINTEROS, Marlene Elizabeth, quien con su ferviente pasión me guio en esta investigación, a mi amiga FIGUEREO PICHARDO, Perla Lucia y a mis amigos BOGGIANO SOSA, Dennis Maximilian Y BERMUDEZ MARCANO, Arquímedes, de los cuáles recibí un incondicional apoyo amical y estudiantil acorde a los aportes de información para con esta investigación que permitieron formar criterios de amplio desarrollo en la presente tesis.

RESUMEN

Yorli Adrian León Ochoa[1]

La presente investigación da inicio con el análisis de la realidad del comercio electrónico partiendo desde el marco de seguridad jurídica y de la poca eficiencia que se le brinda al desarrollo del comercio electrónico y a los delitos que se cometen en él. Es por ello, pertinente hacer la suscripción de la IP estática para las relaciones jurídicas en el comercio electrónico, está investigación tiene como objetivo principal el bloqueo del protocolo de internet (IP) dinámico, en busca de una seguridad dentro de las transacciones del comercio electrónico, pretendiendo ser una medida de prevención ante los delitos informáticos establecidos en la Ley 30096.

La investigación se justificó en el hecho que fomenta negocios jurídicos suscitados a través de internet, mediante las plataformas web, el cual conlleva a problemas jurídicos no regulados de forma eficiente o tratados con poco enfoque de seguridad para su eficiencia como mercado potencial de ingresos económicos, generar una suscripción del IP para facilitar una geolocalización y promoviendo una mejora en el principio de autentificación de las partes y tomar medidas de prevención ante el fraude electrónico y los delitos en el comercio electrónico.

El tipo y diseño de investigación es descriptivo, pues lo que busca es analizar, observar ciertos fenómenos, la estructura que se tiene, como se correlacionan, haciendo aplicación de las variables dependientes e independientes.

La población que abarco la presente investigación consistió en la realización de encuestas 50 personas que realicen funciones dentro del ámbito jurídico que son: Jueces, especialistas, funcionarios y abogados que permitirían desarrollar el enfoque de las variables.

Palabras clave: **Comercio Electrónico, Bloqueo IP dinámico, para medidas de seguridad, Seguridad en las Transacciones, Soportes Informáticos. Fraude electrónico en la ley 30096.**

[1] *Estudiante de la Escuela Profesional de Derecho, Pregrado, Universidad Señor de Sipán, Pimentel, Perú,* ocleonyo@crece.uss.edu.pe

ABSTRACT

The present investigation began with the analysis of the reality of electronic commerce starting from the legal security framework and the little efficiency that is given to the development of electronic commerce and the crimes that are committed in it. It is therefore pertinent to make the subscription of the static IP for legal relationships in electronic commerce, this research has as its main objective the blocking of the Internet protocol (IP) dynamic, in search of a security within the transactions of electronic commerce, pretending to be a preventive measure against computer crimes established in Law 30096.

The investigation was justified in the fact that it encourages legal business arising through the internet, through web platforms, which leads to legal problems not regulated efficiently or treated with little security focus for its efficiency as a potential market of economic income, generate a subscription of the IP to facilitate a geolocation and promoting an improvement in the principle of authentication of the parties and take preventive measures against electronic fraud and crimes in electronic commerce.

The type and design of research is descriptive, because what it seeks is to analyze, observe certain phenomena, the structure that is had, how they are correlated, making application of dependent and independent variables.

The population covered by the present investigation consisted in the conduct of surveys 50 people who perform functions within the legal scope that are: Judges, specialists, officials and lawyers that would allow to develop the focus of the variables.

Keywords: **E-Commerce Security Issues, Blocking Dynamic IP For security Measures, Security In E-commerce Transactions, Electronic Fraud in the law 30096**

I. INTRODUCCIÓN

La presente tesis es una investigación que tiene por objetivo proponer el bloqueo del IP dinámico dentro de los comercios electrónicos como medida de prevención frente a los delitos informáticos en su clasificación de estafa informática**.** Es así que, mediante el bloqueo del IP dinámico posibilitaría asegurar las transacciones comerciales, y una fuerte disminución de las estafas informáticas, que son las principales medidas que se posibilitarían a través del bloqueo del IP dinámico frente a los delitos informáticos regulados en la ley 30096, forma de prevenir se basa en la seguridad de la plataforma en la que se realiza el comercio electrónico en el c2c, brindando los parámetros de un esquema de soporte informático que pueda ser de utilidad para esta forma de comercio, la cual tiene un fuerte movimiento económico creciente en el país, pero que la presente ley antes acotada aun no puede brindar un seguridad eficiente en el tema de esta nueva tendencia del comercio electrónico es por ello que se hace uso de nociones y uso de fuentes bibliográficas que datan de años de investigación, especialmente a libros obtenidos por mérito al investigador y algunos aportes de la biblioteca de la USS. La bibliografía fue contrastada con la realidad de nuestro país, en cuanto a la problemática que atraviesan el desarrollo de la economía a través del comercio electrónico en su figura de consumidor a consumidor de una manera globalizada por el marco de esta problemática se encuentra en una plataforma virtual desarrollada por el amplio desarrollo de las relaciones comunicación como lo es el Internet.

Esta investigación presenta los siguientes capítulos:

Se presenta el planteamiento de la investigación, el problema, la justificación, los alcances y limitaciones de la misma, también los objetivos, hipótesis y variables de la investigación.

Se aborda el Marco Teórico relacionado a la discusión y aparición de esta problemática y deficiencia en el desarrollo del comercio electrónico en su modalidad C2C y como se logrará un mejor desarrollo con el bloqueo del IP para prevenir los delitos de estafa informática, la definición y conceptos más importantes, evolución histórica del problema y normativas relacionadas, experiencias exitosas, legislación comparada, se trata aspectos universales del tratamiento de este flagelo.

La descripción de la realidad frente a la situación actual de los responsables respecto a la aplicación y a las nociones de seguridad de la Ley N° 30096 y si tienen conocimiento de los planteamientos teóricos, normas y legislación comparada respecto a en que beneficiaria un soporte informático que permita el bloqueo del ip dinámico para las transacciones comerciales.

Realidad problemática

El problema en el que se centra la investigación al que se denominara "El bloqueo de la IP dinámico dentro del comercio electrónico como medida de prevención en los delitos informáticos en la ley 30096". En medida que la situación del comercio electrónico tiene una inseguridad jurídica en las relaciones ***Consumers to consumers***, figura que tiene como desventaja por la presencia de nuevas formas de estafas y otras defraudaciones en los servicios dentro del comercio electrónico.

Es por ello que debería establecerse como medida de seguridad o soporte informático la IP estática, para que sirva como una cualidad de domicilio electrónico para determinadas transacciones comerciales en las cuales se permita la geolocalización de la persona o personas con las que se están realizando diversas formas de comercio electrónico, las cuales permitan un mejor desenvolvimiento en la expansión del bando de ancha que es el internet.

El IP facultaría el grado de responsabilidad con la que tendría que resarcir cualquiera de las partes que incumpla frente a las obligaciones de hacer o no hacer la prestación de un servicio, mediante el código único de identificación del DNI y la tecnología one time pasword para el pago o realización de venta de bitcoins o pagos diferidos con gift card.

La interacción sobre todo en estos sistemas de pagos a través de gift card, tienen un alto nivel de vulnerabilidad, la cual genera riesgos ante la posibilidad del impago respectivo a través de la famosa tarjeta virtual PayPal, al poder hacerse en ella una contraorden que anule el pago que anteriormente se había ejecutado dejando sin fondo y sin pago a quien debe cumplírsele.

Es por ello que para todas estas medidas, el principal factor de seguridad, sería la identificación o la ubicación de las personas que están tratando de iniciar una transacción electrónica; el hacer uso de este sistema de IP estática la cual se consigna para estas transacciones comerciales, sería más fácil su posible ubicación ante un incumplimiento y posible reparación o devolución de la prestación; este sistema siempre implementado al accionar jurídico del Estado, que permita un mejor desenvolvimiento de las relaciones comerciales electrónicas con distintos puntos de "*E-Commerce"* ubicadas en el ciberespacio, la cual no son indiferentes al marco de cumplimiento de todo contrato y sus

posibles formas de garantizar la seguridad económica del consumidor.

Formulación del problema

¿Cuál es el efecto del bloqueo del IP dinámico dentro del comercio electrónico frente a los delitos informáticos en la ley 30096?

Justificación e importancia del estudio

El presente tema tiene como antecedente un mercado potencial ejercido por el avance de la tecnología y el efecto de la globalización, que permite interconectarse con personas de todas partes del planeta y fomentar manifestaciones de voluntades para crear, regular o modificar negocios jurídicos suscitados a través de internet, es en las plataformas de internet donde se desarrolla esta interconexión a través de ordenadores conectadas a la red de internet y sus diversas plataformas, la que conlleva a problemas jurídicos no regulados de forma eficiente o tratados con poco enfoque de seguridad para su eficiencia como mercado potencial de ingresos económicos, es por ello que esta investigación propone insertar el bloqueo del IP dinámico y consignar IP estática para los comercios electrónicos para generar una geolocalización de partes y promoviendo una mejora en el acápite de autentificación de las partes y tomar medidas de prevención ante el fraude electrónico y los delitos en el comercio electrónico.

Es por ello que mediante el bloqueo del IP dinámico posibilitaría asegurar las transacciones comerciales, y una fuerte disminución de las estafas informáticas, que son las principales medidas que se posibilitarían a través del bloqueo del IP dinámico frente a los delitos informáticos regulados en la ley 30096, a lo cual tendría que consignarse la IP estática al momento de hacer una transacción electrónica, esta facilitaría el tema de identificación del deudor de obligación y por consiguiente cumplimiento de la reparación, en caso de incumplimiento frente a las prestaciones a las que se sujetaron cualquiera de las partes, esta forma de transmisión de información de data en el comercio electrónico, puede ser cancelada por una contra orden para evitar la ejecución de un pago respectivo en estas modalidades, ocasionando un daño en una de los sujetos que establecía una negociación comercial electrónica, para este procedimiento.

Se tendría restringido el uso de IP dinámicas o proxys para toda negociación electrónica; ya que ello conllevaría a una mejor facilidad de bloqueo al protocolo TCP/IP, la cual no permitiría al sujeto infractor realizar nuevas formas de negocio electrónico ya que el reporte hecho por la parte afectada, entraría en un registro virtual, el cual contribuiría a que cualquier usuario que desee hacer una transacción electrónica tome en cuenta a que la consignación de la IP tiene un reporte que la hace desconfiable, de esta forma se imposibilitaría la ejecución de que el sujeto realice nuevas operaciones electrónicas y en

caso de querer variar la consignación del IP con su proveedora, esta se manejaría de forma estricta, siendo para esta la verificación del motivo por el cual se desea hacer el cambio de está, mediante el registro susodicho generado a través del reporte, siendo este un sistema de verificación respecto al historial de reportes de bloqueos que se le haya generado al IP con la que se llevó a cabo las transacciones comerciales, esto brindaría un conocimiento o información que generaría un mejor sistema de seguridad a las relaciones del comercio electrónico,. La única forma posible de volver a desbloquear la IP o reestablecerla, es que la persona cumpla con la prestación a la que se sujetó, además, podría ser factible la inhabilitación a través del bloqueo del IP, esto permitiría una mayor seguridad de actividad comercial.

Hipótesis

El Bloqueo de la IP dinámico busca dar seguridad, teniendo como principio la autenticidad y la suscripción de la IP estática para dar autenticación de las partes dentro del dentro del Comercio Electrónico, es así que forjará una medida de prevención ante los delitos informáticos en la Ley 30096.

Objetivo

Proponer el bloqueo del IP dinámico dentro de los comercios electrónicos como medida de prevención frente a los delitos informáticos en la ley 30096.

Objetivos específicos

Para alcanzar el objetivo general establecido en el numeral anterior, se debe lograr los siguientes propósitos específicos:

a) Describir la figura del bloqueo del IP dinámico dentro del comercio electrónico como medida preventiva ante los posibles delitos informáticos de la ley 30096.
b) Identificar los alcances que tendrá el bloqueo del IP como medida de Prevención ante los delitos informáticos de la Ley 30096
c) Plantear el bloqueo del IP dinámico dentro de los soportes informáticos, como suscripción a la IP, la cual será una medida de seguridad que prevenga delitos informáticos de la Ley 30096 a través de la geolocalización.

II. MARCO REFERENCIAL

2.1. Antecedentes de la investigación

2.1.1. Evolución Histórica- Desarrollo del Internet y del Comercio Electrónico.

Tener como base fundamental de noción que el Internet es una conjunción de redes que guardan interconexión, las cuales funcionan como una red única, es por ello que los primeros momentos que dieron origen a esta conmoción de lo que es el internet.

Cañedo (2004) "Una aproximación para la Historia del Internet", está se habría generado desde un lanzamiento al espacio generado del primer satélite soviético, el Sputnik, en octubre de 1957 por lo cual puede tenerse como un punto de partida cronológica segura, para el comienzo de la historia de Internet. La transición en órbita terrestre de aquella pequeña esfera de metal galvanizó a los Estados Unidos. La que pretendía el envío al espacio de un cohete y su variación en un satélite artificial de la Tierra, se encontraba fuera del alcance de parámetros establecidos que tenían como base a los de una ejecución de procedimiento de lanzamiento de bomba nuclear a un objetivo, siendo superior el cohete hacia el espacio. Aquella revolución, produjo distintos resultados, que fueron desde la subvención para elaborar formas efectivas de capacitación de los científicos hasta la innovación de una nueva agencia de defensa, la Advanced Research Project Agency (ARPA).

En 1961, el entorpecimiento a tres torres de microondas en Utah renovó, aunque a una jerarquía menor, la conmoción que produjo el Sputnik unos años antes. La preocupación sobre la fiabilidad de los mecanismos militares de "comando y control", así como el susto a nuevas perpetraciones de ataques subversivos, los cuales hubiesen podido dejar al país sin medios de comunicación, impulsaron la búsqueda de plataformas más invulnerables. El final de aquella interminable búsqueda fue el diseño de un prototipo de comunicación capaz de sobrevivir a una guerra nuclear.

Es exactamente en el año de 1962 que surge el proyecto de Internet, a raíz de los afanes de los Estados Unidos por la elaboración de una red de militar,

con la expectativa de soportar las comunicaciones de esta esfera bajo los presupuestos de un ataque nuclear procedente de la Unión Soviética y otros países del campo socialista.

Entre 1962 y 1964, Paul Baran de la Rand Corporation, estructuraron un repertorio de informes en los que recomendaron la innovación de una plataforma de comunicación, con cierta tipología análoga a las redes de una araña, con la finalidad de bloquear la distinción de objetivos para cualquier perpetración de ataque. Dado este proyecto, se constituyó el protocolo de Internet. Se creía en la posibilidad de que esta fuera la única forma de tecnología capaz de sobrevivir a un ataque nuclear.

En 1962, ARPA creó la Information Processing Techniques Office (IPTO). La fundación de dicha institución faculto que la agencia de defensa mantuviera un vínculo con el naciente campo de la computación. La cual tuvo una contribución notable en la generación del trabajo a tiempo fraccionado, la informática interactiva y las redes. En consecuencia, si era posible que varias personas se interconecten masivamente a un mismo ordenador a través de distintos terminales, no es complejo cavilar en la existencia de una segunda computadora que actúe como si fuera un punto temporal de la primera y viceversa.

Desde una óptica capitalista, la invención de está redes ha ocasionado una expansión de ámbito comunicativo y un índice mayoritario de explotación de recursos con un costo bajo.

El espacio-tiempo de compartimiento permitía el uso más eficaz de las maquinas en relación con el costo de su capacidad computacional, es por ello que ampliar la red lo más que sea posible sobre un determinado territorio demográfico tenía un criterio exquisito para los intereses económicos en los que se encontraban en la base de la agenda de trabajo de la IPTO.

En 1966, es en esas fechas que esta entidad financiaba 17 sitios que publicitaban un inaudito rango de hardware y software. La diferencia de

caracteres era la regla; para poder continuar por esa senda era la excesiva pérdida de recursos. Estos presupuestos facilitaron la identificación de la red como una posibilidad de solución al problema de costos excesivos. El objetivo primigenio de ARPANET era la de brindar una conectividad remota a ordenadores distantes para compartir variedades de ficheros remotos como las experiencias de información obtenidas a través de investigaciones en materia de computación.

Siendo 1967, en el transcurso de una asamblea de la Association for computing Machinery (ACM) en Tennessee, se desglosaron actividades muchas de las ideas obtenidas a partir de las cuales se conformó la matriz de la primera red ARPA, en la cual, los oradores de Gran Bretaña; Scantlebury R. y D.W Davies; propusieron sus concepciones sobre la conmutación de paquetes, una definición nueva para la época en la que se desarrolló.

La Historia de la Creación del *New Host-to-host Protocol*

Con la creación de Network Working Group (NWG), formado por Larry Roberts en 1967 se tomaron partes en los primeros tipos de conexiones compuestos por dicho grupo, siendo la Universidad de California, Stanford, la Universidad de Utah, Ucla, sí como Rand Corporation.

Siguiendo un cronograma de desarrollo basaron especificaciones para la construcción de la red, siendo en 1968 que Larry Roberts publicito el proyecto que consistía en dicha construcción de red al director de ARPA, el cual este proyecto, fue financiado con 2,2 millones de dólares. Siendo la firma consultora BBN (Bolt, Beranek y Newman) obtuvo el contrato para la realización del proyecto.

El proceso que tenía la BBN era trazar un equipo que debía facultar diversos hosts interconectándose a través de una red de ordenadores intermediarios con la denominación de “Procesador de Mensajes de Interfaz (IMP)”, equitativamente al trabajo en el IMP, se había hecho de conocimiento, el informe en 1822 de la BBN, el cual se hizo famoso por

hacer noción de “Procesado de Mensajes de Interfaz”, la precisión para desarrollar la interconexión de un host y un IMP, es así que en mayo de 1969 Peter Saludos hace noción a lo que en ese entonces era la Biblia de las redes. Dicho informe se subyugo a varias revisiones hasta 1978. En octubre de 1980, se le integro un aditamento que describía la norma x.25 del Comité *Consultatif Internationale de Telegraphie et Telephonie* (CCITT).

Durante el año de 1969, la transición del diseño de los programas iba ligada al trabajo en el hardware. El modelo primigenio tuvo una denominación de cliente-servidor, un modelo familiar por la omnipresencia de terminales que desempeñaban las computadoras a tiempo compartido.

Ello conllevo a innovación del *Network Control Program (NCP),* el primer programa de control de redes que después se llamaría Network Control Protocol. La expresión “Protocolo”, se varia del costumbrismo diplomático, aparentemente surgió de una metáfora, que se empleó en un dialogo entre Vint Cerf, Jon Postel y Stephen Crocker, con la determinación de una fecha insulsa. En la RFC (Request for Commets) número 33 de Crocker y Cerf con fecha 12 de febrero de 1970, se dio utilidad al término “*New Host-to-Host Protocol”.*

Los protocolos de comunicación son un agregado de reglas que permiten que diferentes computadoras con variados sistemas operativos los cuales tienen una comunicación y un compartimiento de recursos. En su grado más significantes son: IP (Internet Protocol), TCP (Transmission Control Protocol); FTP (File Transfer Protocol), TelNet (Network Terminal Protocol), y SMTP (Simple Mail Transmission Protocol).

La instalación del primer procesador se llevó a cabo en setiembre de 1969, el cual era un mensaje de interfaz, denominado ARPANET, en la Universidad de California (UCLA), en los Angeles. Contaba con cuatro nodos enlazados mediante líneas telefónicas. La conexión amateur entre un host y un IMP se llevó acabo el 2 de septiembre de 1969 en la UCLA.

Mantener este sistema de interconexión, es de criterio razonable tener en cuenta que este programa de investigación en conmutación de paquetes de ARPANET, suponía tener como base un capital que financie tal elevado costo, porque los ordenadores de fines de los 60 e inicios de los 70, con la particularidad las maquinas más avanzadas tendría un presupuesto elevado. En vez de poseer una adquisición para cada una de las instituciones que desarrollaban investigaciones para ARPA, tenía la posibilidad de llevar a cabo una instalación de una o dos de estas máquinas a nivel nacional y compartirlas, se daba el caso del uso de software, que corrían solo en potentes máquinas, base de datos e información global, mediante una red.

2.1.2. Tesis nacionales.

Arata (2002*) "Las Nuevas Tecnologías de la Información y la Problemática Jurídica del Comercio Electrónico"* El enfoque plasmado en su tesis rebasa en una proyección de regulación legislativa al comercio electrónico por medio de una dirección que tenga como un marco en la región, la cual debe comprender diversas etapas de la contratación electrónica, donde se integren los elementos fundamentales a raíz de la forma y al fondo de contratar por medio del uso de soportes informáticos, detallando un dominio de aplicación, es por ello que las nuevas conceptualizaciones y preceptos jurídicos que integran el comercio electrónico deben regular actos de comercio virtuales trascendentes, tienen que tener un proyecto global para ser una legislación más coherente, que tenga un mayor precepto y concatenación con la legislación regional comparada a fin de que esta se pueda ejecutar en lo posible con los países de Europa y Asia, que poseen tecnologías de punta para el comercio electrónico en el mundo.

Armas (2002) *"Sistema de Contratación por Medios Electrónicos: Manifestación de voluntad y perfeccionamiento contractual"*. El desarrollo tecnológico ha impactado de tal forma que el derecho, ha creído conveniente indicar que este suceso plantea una alteración en los

presupuestos de hecho, por ello refiere a la aplicación análoga del código civil, para adecuar los contratos a través de medios electrónicos, es así que se busca adecuar la realidad normativa aun espacio de aplicación al cual no se puede llegar de manera física, sino virtual, entendiéndose como al proceso de eliminación de la etapa cartular, a la transformación digital, lo cual fue que motivo al investigador plantearse el desarrollo de esta investigación citada, respecto a la nueva forma de contratación del soporte material atómico-masa a contratación por medios electrónicos, digitales o documento electrónico e igualmente cambios de la firma manuscrita a la firma digital como soporte informático de prevención ante las nuevas formas de contratación por medios electrónicos.

Méndez (2014) "*Análisis, Diseño e Implementación de una plataforma web basada en un esquema C2C para la Gestión de Entrega de Servicios Generales"* El estudio realizado por el ingeniero en informática basa su investigación en la creación de una plataforma que tenga como vínculo entre las partes que configuran el comercio electrónico que son: el proveedor; el cual mediante ese soporte informático permitirá que puedan ser localizados y contactados por sus clientes, es por ello que al ejecutarse como un nexo primigenio de comunicación, con sus clientes, que al disponer del servicio de sus proveedores, está tendrá un desarrollo eficaz, es por ello que funcionalidad el servicio de suministrar insumos requeridos por los proveedores a las tiendas, tenga como objetivo el uso de este soporte informático creado, es por esto que para lograr todo esto, ha llevado a cabo en su proyecto, la necesidad de crear un modelo de negocio de forma novedosa, el cual se enfocara en los requerimientos de cada una de las partes.

2.1.3. Tesis extranjeras.

Vorapranee (2003) "Enchancing the Security of Electronic commerce transactions" Esta investigación evalúa la seguridad del proceso de transacciones en el comercio electrónico, detalla desde la terminología en la que se basa cada sistema de seguridad proporcionada dentro de un soporte informático, además de la descripción de los requisitos de seguridad para pagos con tarjeta a través de internet, y los posibles protocolos para el

procesamiento de transacciones electrónicas, a la actualidad el protocolo Secure Socket layer(SSL) junto con su protocolo estandarizado o genérico TLS (Transport Layer Security) son los medios más utilizados para brindar soportes a las transacciones electrónicas realizadas a través de Internet. Por lo tanto, el análisis y las discusiones que se han integrado en esta investigación basan su teoría en el supuesto de que estos protocolos proporcionan un nivel "Base" de seguridad, contra el cual deben proporcionarse nuevas medidas de seguridad poniéndose a escalas de medición en su nivel de seguridad, los protocolos SSL Y TLS se analizan de acuerdo a lo bien que satisfacen los requisitos de seguridad que se han de describir, a su vez la proporción del transporte en el que se generan las transacciones de seguridad electrónicas tienen capas de seguridad y algunos de los requisitos de seguridad están en aplicación del nivel, no es sorpresa que no aborden todas las cuestión de requisitos de seguridad, por lo tanto en esta investigación la propuesta el resultado a la investigación es dar a conocer cuatro protocolos que se pueden utilizar para construir sobre las características de seguridad proporcionadas por SSL/TLS, para lo cual su objetivo principal es diseñar sistemas que mejores la seguridad del procesamiento electrónico, de esta forma se imponen gastos mínimos a las partes involucradas. En el primer protocolo se proponen utilizar una tarjeta EMV para mejorar la seguridad de transacciones en línea, el segundo protocolo; implica el uso del abonado de la Autenticación en GSM, para proporcionarse una autenticación del usuario a través de internet. En tercer lugar, el investigador propuso el uso del servicio de confidencialidad de datos GSM para proteger, así como garantizar la autenticación del usuario; independientemente del régimen de protección empleado para las transacciones. Por ende, existen tantas amenazas a todos los ordenadores (PCs). Utilizados para realizar transacciones de comercio electrónico, pero estos protocolos examen las amenazas residuales y motivan el diseño el cuarto protocolo, que específicamente está hecho para hacer frente a las amenazas de cookies.

Niranjanamurthy y Dharmendra (2013) “The study of E-Commerce Security Issues and Solutions” El soporte en el comercio electrónico, una parte dentro del marco de seguridad de la información y se aplica específicamente a los componentes que afectan al comercio electrónico, que incluyen seguridad informática, seguridad de datos y otros ámbitos.

Este marco de seguridad de la información tiene sus propios matices particulares y es uno de los más visibles cuando se trata de los componentes de seguridad que afectan al usuario final a través de su interacción de pago diario con otros usuarios o con las empresas. La seguridad del comercio electrónico es la protección de los activos dentro del comercio electrónico contra cualquier acceso, uso, alteración o destrucción no autorizados de los mismos. Estas dimensiones de la seguridad en el comercio electrónico: integridad, no repudio, autenticidad, confidencialidad, privacidad, disponibilidad. E-Commerce, ofrece al sector bancario una gran oportunidad, pero también crea un conjunto nuevo de riesgos y vulnerabilidades como amenazas de seguridad. Por lo tanto, la seguridad de la información es un requisito esencial de gestión y técnica para efectivo desempeño de las actividades de transacción de pago a través de internet.

Sin embargo, su definición es un proceso complejo debido al constante desarrollo tecnológico de negocio y requiere una combinación coordinada de algoritmos y soluciones técnicas. Es por ello que en esta investigación se discute con visión general de la seguridad del comercio electrónico, desde cómo entender los pasos de compras en línea por Orden, Propósito de la seguridad en el comercio electrónico, diferentes problemas de la seguridad en el comercio electrónico y pautas de compras en línea de forma segura.

Dilané y Mantas (2005) “Incidencia de los Acuerdos y los Tratados Internacionales en la Aplicación de la Ley 126-02 de Comercio Electrónico en la República Dominicana” Los investigadores proponen con urgencia que el Estado propicie la tipificación de los delitos electrónicos, tal como lo contempla el proyecto del Código Penal Dominicano, a los fines de llenar el vacío que al respecto contiene la ley sobre comercio electrónico y firmas digitales a lo que el proyecto del Gobierno digital que el Poder Ejecutivo

pone en marcha para la construcción de la Sociedad de la Información Dominicana, no sólo debe garantizar los cuatro libertades del mercado interno (Libre circulación de personas, capitales, bienes y servicios), sino que también deber contemplar la política de competencia, una política comercial común para todos los sectores y la construcción de la Asociación Nacional de Comercio Electrónico. Este trabajo pretende varios objetivos, los cuales derivan de cierta contribución de la realidad contractual del comercio electrónico y establecer los alcances de la Ley 126-02 sobre Comercio Electrónico, Documentos y Firmas Digitales.

La determinación de como la legislación dominicana, ha sido impactada por los acuerdos o convenios internacionales que dieron como resultado la constitución de la Organización Mundial del comercio (OMC) y de su estandarización de las fórmulas contractuales del comercio digital impuesta por las exigencias de la sociedad.

La existencia de las leyes 126-02 sobre Comercio Electrónico, por tanto, la información constituye una mercancía que merece atención legislativa del Congreso y reguladora por parte del Poder Ejecutivo, a los fines de proporcionar seguridad jurídica a los proveedores y consumidores en marco de las nuevas prácticas del comercio digital. Con la aceleración del proceso de la globalización determina para la investigación, un apurado crecimiento exponencial de la interconexión digital de las naciones, el derecho y el comercio ha asimilado nuevos conceptos por lo que los limites geopolíticos y las fronteras comerciales fueron borradas a causa de esta, por tanto, se debe reforzar el sistema de seguridad para el comercio electrónico.

Celenia y Yaneris, (2012) “Incidencias de las leyes fiscales en el Comercio Electrónico de la República Dominicana (2008-2010)” Es así que la investigación gira en torno a la evolución que ha tenido el comercio electrónico en República Dominicana, y que por ende trata de establecer los parámetros que sirven para regular el comercio electrónico, es por ello que se busca determinar las incidencias fiscales del comercio electrónico para

las empresas en república dominicana, a través de una investigación que mida las lees del comercio electrónico en el fisco de la República Dominicana, que a su vez analice y fundamente la estructura del comercio electrónico, es así que desarrollar el papel que jugaran las Instituciones del estado es un elemento esencial para detectar los tipos de gravámenes y fiscales que se aplican dentro del comercio electrónico, es por eso que la determinación de si las empresas dominicanas realizan sus aportes de acuerdo a las leyes que regulan el comercio electrónico es una contribución a las estadísticas planteadas en la presente investigación.

Fernández, Pujols, Mata y Pérez (1999) "Seguridad en Redes de Internet Caso de Estudio El Comercio Electrónico" El esboce de los elementos que enmarcan la investigación citada no es más que hacer contar que para realizar el Comercio Electrónico por Internet, las empresas deben tomar muy en cuenta lo que es la seguridad, privacidad fiabilidad. Las transacciones electrónicas son: capacidad para impedir transacciones de datos no autorizados, una forma de impedir que el contenido de los mensajes sea alterado después de enviado, capacidad para determinar si una transacción se ha realizado desde una fuente autentica o desde alguien o algo que se ha hecho pasar por dicha fuente. Una manera de impedir a un emisor que se esté haciendo pasar por otro. Es por ello que la seguridad dentro de estas nuevas formas de ver al mercado como reedición de la mismas por el desarrollo tecnológico es que se debe mantener un sistema que permita el flujo de estas actividades económicas teniéndose en cuenta los parámetros de la seguridad dentro del comercio electrónico, si no se mantiene una continuidad respecto a esta forma de interacción entre usuarios, se verán afectadas también por todos estos cambios igualmente, los miembros individuales de la sociedad estarán del mismo modo presentes con nuevos medios de compra de bienes de acceso a la información y a servicios. Lo más importante para un comercio electrónico eficaz es tener un algoritmo de seguridad que cumpla con lo requerido, ya que si no se tiene una seguridad pertinente no se tendrá un Comercio Electrónico exitoso.

Barrera (2014). “Determinar los delitos de estafa informática según la Ley 67 de Comercio Electrónico en la Legislación Ecuatoriana” En la actualidad con la creación de la denominada “autopista dela información”, el internet, las posibilidades de comunicación e investigación se han acrecentado, se tiene acceso aún ilimitado número de fuentes de consulta y entretenimiento. No existe una legislación adecuada que pueda contener el avance de esta clase de ilícitos, primero por una inadecuada y obsoleta normativa y, posteriormente por un procedimiento penal que si bien se ha modernizado, aún inadmiten los medios de prueba tecnológicos que se precisa en esta clase de delitos que no conocen fronteras, ya que el delito informático no se ajusta solo al país, pudiendo detectarse, como se analizará en el transcurso de la investigación, como se viola las seguridades de las cuentas bancarias desde el extranjero. Debido a que existe una legislación adecuada en el Ecuador se siguen cometiendo a nivel particular e institucional de los delitos informáticos aprovechándose de que las instituciones informáticas no dan seguridad personal e institucional para el buen uso de estas. Es así que, en un inventario amplio, las actividades principales de las organizaciones criminales, en suma, abarcan la provisión de bienes y servicios ilegales, ya sea la producción y el tráfico de drogas. Armas, niños, órganos, inmigrantes ilegales, materiales nucleares, el juego, la usura, la falsificación, el asesinato a sueldo o la prostitución; la comercialización de bienes lícitos obtenidos por medio de hurto, el robo o el fraude, en especial vehículos de lujo, animales u obras de arte, el robo de identidad, clonación de tarjetas de crédito; la ayuda a empresas legítimas en materias ilegales, como la vulneración de las normativas medio ambientales o laborales; o la utilización de redes legales para actividades ilícitas, como la gestión de empresas de transporte para el tráfico de drogas o las inversiones inmobiliarias para el bloqueo de dinero. Entre aquellas organizaciones que pueden considerarse como típicamente propias del crimen organizado, practicando algunas de estas actividades, se encuentran, dentro de un listado más o menos extenso, las organizaciones dedicadas casi exclusivamente al tráfico de drogas a gran escala, ya sean propias de los

países europeos o se generen en países latinoamericanos, del sudeste asiático, la Mafia italiana es su proceso de expansión mundial que ya se inició hace décadas, las Yakuza japonesas, las Triadas chinas y, en última instancia, ese magma que constituye el crimen organizados en Rusia y en otros países del Este Europeo, y ahora existe otro grupo que ha entrado en la escena del crimen organizado transnacional son los llamados Crackers, los verdaderos piratas informáticos, que a través del cometimiento de infracciones informáticas, han causado la perdida de varios millones de dólares, a empresas, personas y también a algunos estados. Es por ello, que se tiene como objetivos la determinación de los delitos por estafa electrónica según la Ley Nº 67 de Comercio Electrónico en la legislación ecuatoriana; además de, plantear la responsabilidad civil objetiva de las instituciones bancarias y financieras que carezcan de protección adecuada contra la estafa informática; por lo tanto. Se busca efectuar una investigación para poder ver la frecuencia en la que se dan los fraudes, crímenes y como se realizan; teniendo a su vez en cuenta la creación de un anteproyecto que pueda beneficiar la seguridad del usuario y que a su vez pueda determinar con exactitud, en que consiste el delito de esta informática y las similitudes y diferencias contempladas en la legislación penal, poniendo énfasis en los aspectos tecnológicos de los que se valen los autores de este ilícito. Para así, poder analizar las eventuales ventajas y desventajas del ordenamiento jurídico nacional referente al delito de esta informática y confrontarla con normas existentes en el derecho comparado, sustentándolo, asimismo, en la doctrina que sustenta los autores sobre la materia.

García (2004). “Seguridad en el Comercio Electrónico” El citado Denomina al desarrollo de una Sociedad de la Información, donde se ofrecen servicios telemáticos y de valor agregado, que gracias a las redes de transmisión de información, permite conectar dos puntos, sin importar la distancia entre estos, en tiempo récord, sin embargo, este servicio afronta un gran inconveniente de inseguridad razón por la cual, se proporciona al lector una visión técnica, jurídica y práctica, sobre los aspectos más relevantes del comercio electrónico y la seguridad. Este último elemento, es el pilar de la eficacia en el desarrollo del intercambio de información a través de redes de

valor agregado como el internet, lograr entornos seguros genera confianza en el sistema y ambientes propicios para el intercambio de información. De este modo, como primera medida, se introduce al lector al comercio electrónico, dejando al descubierto la falta de confianza en el sistema, tato nacional como internacionalmente. Así, se dispone la senda en busca de la seguridad del comercio electrónico, Pues para ello la investigación busca dejar en claro, que al asegurar el perímetro y utilizar mecanismos de seguridad adecuados: cortafuegos, antivirus, certificados digitales, etc., reduce costos y prevención de ataques. Para lo cual busca que se ejecute a través de personal idóneo, para lo cual tiene la alternativa de contratar un proveedor externo en servicios de seguridad establecidas en medidas preventivas, para lo cual resultaría importante realizar monitoreos y simulacros de ataques con el fin de probar la eficacia de los sistemas que es para dar una explicación pertinente al desarrollo del bloqueo de la IP dinámica dentro del Comercio Electrónico, hay que tener en cuenta el transcurso histórico de la creación del Internet, por lo que es necesario identificar el inicio de la relación innata entre el internet y la creación de protocolos de internet hasta el momento de las plataformas web donde se desarrolla los comercios electrónicos; además de que es lo que se propone, esta investigación de proponer el desarrollo de una plataforma basada en un sistema similar al de los videojuegos MMORPG O RPG, con su sistema de VPN y el Sistema de Registro de Usuarios, identificados con un *ID y password*, anexado a su sistema de ingreso de login y su ubicación de IP y sus posibles sanciones, respecto a funciones ilícitas ejecutadas dentro de sus políticas privadas de juego y su bloqueo respectivo de IP y las restricciones a las regiones a través de las VPN y uso de IP’s dinámicas, es en razón a esto que se propone a desarrollar un sistema análogo al de este para ejecutar una plataforma más segura en tiempo real para el comercio electrónico.

2.1.4. Bases teóricas científicas.

2.1.4.1. Variable independiente: Bloqueo del IP dinámico dentro del comercio electrónico.

Romero (2003). "*Seguridad en redes y Protocolos Asociados"* en su artículo científico, señala que en el transcurso del desarrollo y proceso del Internet estuvo sujeta a cambios y a medidas de seguridad que pudieran permitir salvaguardar las transferencias de datas que se hacían a través de la interconexión masiva de los paquetes de redes surgiendo dentro de ellas la famosa *Access Control List (ACL)* se entiende como la lista de sentencias que tienen un control de acceso que aplican a una determinada interfaz del router, haciendo uso de un indicador el cual hace una partición entre que tipos de paquetes de datos serán admitidos y cuáles deben ser denegados, teniendo esto como referencia a los puntos de origen y destino, con la consignación del protocolo de capa superior y la numeración del puerto, haciendo un listado de acceso de IP estandarizado que deniega paquetes de data provenientes de un determinado host como por ejemplo "El host 192.5.5.2 hacia otro host en la red con la identificación de 210.93.105.0 el cual admita el tráfico desde todas las demás redes; asimismo, las ACLs extendidas brindan una mayor variabilidad de opciones de control que las ACLs estándares, pudiendo especificarse facultativamente la numeración del puerto del protocolo TCP o UDP para el que se aplica una serie de sentencias figuradas en 20 y 21 datos y programa File Transfer Protocol, 23 de Telnet, 25 SMTP, 53 DNS, 69 TFTP, haciendo un proceso más sofisticado de bloqueo de todo el tráfico desde la red haciendo que la generación de un servidor con determinada dirección origen solo se conecte con su dirección destino, provocando una menor cantidad de tráfico en la red.

Es por ello, que las ACL pueden controlar una variedad de protocolos en un router cisco. A través, del uso de las ACLs restringe el tráfico de red, optimizando su rendimiento, proporcionando un flujo de control que debe pasar por el router, generando un nivel primario de seguridad de acceso a red en función de diferentes parámetros, siendo el dirigente el que por libre

albedrío decida qué tipo de tráfico se envía o sufre un baneo en los interfaces del router.

Barrio (2013) *"VPLS: Alternativa de interconexión a través del backbone IP/MPLS de ETECSA".* La Habana, Cuba: Ediciones Futuro La empresa de telecomunicaciones ETECSA en cuba, tiene a su merced la operación de exclusividad en la infraestructura de telecomunicaciones de este país, por ende, los demás proveedores, buscan otro método de desarrollo para dar ejecución a dicha infraestructura como soporte para la interconexión de nodos que integran sus redes. Dado cuenta que el desarrollo de las tecnologías de las telecomunicaciones, ETECSA ha apostado por la implementación de un *backbone Internet Protocolo ver MultiProtocol Label Switching:* Protocolo de Internet sobre Conmutación Multiprotocolo basada en Etiquetas en su red, por ello se tiene la expectativa que impregne todos los servicios que a su momento son sostenidos por el *backbone Asynchronous Transfer Mode/ Frame Relay,* hallándose con obstaculizaciones producto de que la red IP/MPLS abarca solo lo que es el *Virtual Private Network-VPN* como forma de servicios*:* teniendo dentro de sus parámetros un nivel tres de red del modelo OSI; lo cual es inadmisible para los distintos proveedores. Es por ello que se crea una propuesta análoga a este sistema con la implementación de una entidad *Virtual Private LAN Service- Servicio de LAN Privada Virtual;* como medio alterno para migrar las *Virtual Private Network* de nivel 2 el cual tiene compatibilidad con el sistema *backbone ATM/Frame Relay,* hacia la plataforma del *backbone Internet Protocolo MultiProtocol Label Switching*, un sistema genérico similar que avala la autonomía por parte de los proveedores que son clientes de ETECSA en la operación y enrutamiento de su red.

Mientras más encaje los parámetros de la primera variable haciendo noción al bloqueo de IP dinámica como un proceso sistemático por lo que se toma en cuenta a la seguridad por niveles, como parámetros que permitan fijar la suscitación de esta medida de prevención dentro de los comercios electrónicos.

Corletti (2011) “Seguridad por niveles” Es por ello, que para llegar a este punto se hace la noción a la presentación de modelo de capas que son formas de como los protocolos ayudan a gestionar las comunicaciones, siendo que para cubrir cada capa está sustentada por el modelo OSI o Sistema de interconexión abierta, siendo en concreto que para tener un interfaz entre dos equipos que tienen Terminales de Datos-ETD, se ejecuta la función de más de un protocolo, que son determinados por una ***PILA de protocolos*** conformados por X.25, TCP/IP, IPX/SPX, ISDN, etc. Esta congregación es cotidianamente encontrada en los siete niveles del modelo OSI, que se derivan de tres grupos. Siendo su esquema de trabajo del modelo OSI el siguiente: Aplicación, Presentación, Sesión, Transporte, Red, Enlace, Físico y en su versión generalizada solo Aplicación, Transporte y Red.

Siendo así que OSI, es el estándar a nivel mundial más reconocido, por excelencia, la cual consta con sistema que no puede dar una demora de red y una incompatibilidad de productos que sean de uso final para el consumidor por ello es que se estandariza en este sistema o modelo OSI, es por ello que para la actual investigación basara en la capa nivel dos denominada “ENLACE” siendo su función el establecimiento de la conexión con el nodo inmediatamente adyacente y la proporción de los medios para asegurar la confiabilidad a la ristra de bits que recibió, efectuando un control básico de flujo de información, siendo de redundancia la División de datos en varias conexiones físicas y las IEEE que hace la subdivisión de dos capas MAC (Medium Access Control) Y LLC (Logica Link Control), este medio no está contemplado por OSI.

Además, de también de tener en cuenta el nivel 3 del modelo OSI que está orientada en lo que se denomina “RED”, para dar curso en al encaminamiento y retrasmisión, definiendo las rutas a seguir, la conmutación de paquetes, multiplexación de conexiones de red, establecimiento de circuitos virtuales y por último el direccionamiento de red.

El camuflar la SSID en la configuración del router un proceder idóneo la práctica de seguridad que tenga un ámbito empresarial u hogareño, la denominación de la red de Wifi queda sin ser detectada a la vista de los atacantes. Estas se pueden conectar a la red solamente las personas que conozcan el nombre de la red, esto puede tener un gasto pecuniario excesivo para redes con masificación de personas conectadas a la red, por lo que los parámetros fijados en relación esta no suelen ser muy beneficiosas distinto es para redes con interconectividad pequeña para ellas son demasiado beneficiosas, además, de que otras formas de brindar seguridad que se ha analizado en el presente artículo, es la configuración del router para que designe parámetros de aceptación de conexiones confiables de dispositivos, con la anticipación de adecuar un registro con una respectiva MAC desde la administración propia. Los límites que existen en esta medida de seguridad es la permanencia en el registro que debe darse en el dispositivo del usuario por la autorización de la conexión que este debe ejecutar.

Siguiendo este margen de errores es otra adecuada opción para redes que aún están en desarrollo no exponencial. El sistema del filtro de las MAC que viene siendo usado para proteger los WIFI según el análisis efectuado por los investigadores presentan una vulnerabilidad considerable por lo que no es abastecedor para las necesidades de seguridad que se han propuesto, ya que hay instrumentalización de variar la dirección de MAC del equipo atacante para imitar el de un cliente legítimo. Es así como las contraseñas a utilizarse tienen que tener un margen factible de ser recordada pero difíciles de adivinar. Monsalve, Aponte y Chaparro (2014) en su investigación *Análisis de seguridad de una muestra de redes WLAN en la Ciudad de Tunja Boyacá*

2.1.4.2. Variable dependiente: Medida de prevención ante los delitos informáticos de la ley 30096.

Por esta suscitación de secuencias de conexiones a la red, es que los parámetros de adecuación para que se den ambientes propicios para el desarrollo de una efectiva plataforma privada, que tenga márgenes de

usuarios con un ID y Password en similitud y semejanza a las MMORPG o RPG en donde se usa interconexión masiva de usuarios a la red se adecuan para un ámbito propicio de desarrollo de comercio electrónico la emulación de esas plataformas conllevarían a una ejecución idónea de esta actividad económica sujetos a los protocolos pertinentes y al uso de las VPN, y medidas de seguridad ejecutadas en plataformas de MMORPG, que son propiciadas en plataformas hechas para videojuegos.

Siendo que el cloud computing, da servicios de computación a través de internet, esta plataforma abastece de herramientas de software, plataformas e infraestructura como servicios, siendo esta un esquema que permite un acceso determinado a recursos computacionales difundidos en su plataforma como el de redes, servidores, almacenamiento, aplicaciones y servicios, siendo una forma de negociación de herramientas computacionales que tienen un mercado privado que se rige a través de una demanda con exclusividad de hacer un trabajo solo ha pedido. Siendo una plataforma dinámica, abastece, diseña, y reestructura servidores como sea necesario. Mamani (2012) "*Protocolos de Comunicación Utilizados en Cloud Computing"*

Está dinámica hace un arquetipo de proyección modelo a lo que se tiene en la presente investigación, respecto al servidor MMORPG que se quiere poner a servicio de una comunidad que hace uso del comercio electrónico en su figura de C2C, B2C Y B2B, la cual absorbería de forma amplia, en una plataforma privada, con parámetros virtuales de comercio electrónico a tiempo real.

Las medidas de seguridad respecto a la información que se transfiere a través de la red, estás vienen siendo afectadas por un marco de seguridad de información las cuales tienen como sistema de seguridad informática, las cuales tienen un sistema de medición de data y otros ámbitos más extensos. La seguridad de comercio electrónico tiene sus propias interacciones con la empresa, la construcción de activos de comercio electrónico contra entradas ilícitas, suplantación o cambiar la asistencia dimensional del comercio electrónico de seguridad integral referente a legitimidad, confidencialidad,

privacidad, accesibilidad en el comercio electrónico, el cual se ofrece por medio de la industria bancaria con grandes posibilidades, pero que genera un conjunto de riesgos incipientes y la sensibilidad de tales amenazas de seguridad. La seguridad de la información, por lo tanto, es un presupuesto fundamental para la gestión y surgimiento técnico para cualquier diligencia pertinente al momento de hacer transacciones de pagos eficientes e ineficaces en el mundo virtual. La discusión de los puntos de seguridad en el comercio electrónico y la comprensión del proceso que se ejecuta en línea para realizar un pedido y también para garantizar los lineamientos de compras en línea, con un nivel de seguridad elevado. El meollo del asunto es tener siempre presente que la seguridad en la transacción es la cuestión que se tiene como punto principal será en los campos del B2C o C2C ejecutados a través de web´s; esta investigación tiene como objetivo proponer una estrategia de respuesta entre la ingeniería y el sistema, a fin de subrogar el entorno o el espacio en el que se desarrolla esta actividad electrónica, producto de que las aplicaciones web, tienen por integrada los ajustes de terceros, lo cual permite ingresos de nuevas amenazas y generación de nuevos desafíos de seguridad, por ser primigenios en la materia debido a la involución de una aplicación que tenga por efectos coordinar una mancomunidad interna con los de refugio de partes y el cliente web a través de la red. Siendo así que los dueños de plataformas web de comercio electrónico tienen la cartera de agrandar su amplio mercado de clientes y la magnetización de usuarios hace que sus plataformas tengan una exquisitez de demanda, por lo que el simple hecho de visitar el sitio ya está generando una repercusión económica, pero la otra parte configurada por el usuario de cese debe calificar un sitio web de comercio electrónico y lo que deben hacer para poder ejecutar la comunidad biótica en línea. El objetivo es que se aproveche los consejos seguros para ejecutar transacciones seguras. Adamu (2015) *"Concern for e-Commerce Security"*

La seguridad es un factor principal de continuas preocupaciones, que restringe la libertad de los clientes y las organizaciones que se aprestan al comercio electrónico, teniendo como objetivo de este trabajo es localizar la percepción de seguridad en el comercio electrónico desde la óptica del B2B

Y C2C ejecutados desde plataformas web, tanto en los clientes y las perspectivas organizacionales. Los factores que trasgreden se destacan por los conflictos entre las medidas de los clientes con respecto a la seguridad. Siendo que el punto de vista de las organizaciones es la investigación existente que no ha destacado, esta cuestión en gran escala.

Una de las razones más impactantes dentro del criterio del cliente es que sientan que la página web o destino web sea seguro y sea de creíble calificación, sistema por el cual los indicadores reflejan un sistema de aprobación y desaprobación por parte de los compradores y vendedores y los mejores compradores y vendedores.

Algunas opiniones de las organizaciones en los puntos de vista personal técnico y gestión en cuanto a clientes consideran esencial, la opinión del cliente, pero no es razón suficiente para demostrar la confiabilidad entre este sistema de seguridad en el sistema de comercio electrónico, lo que significa que la empresa debe explicar la seguridad del sitio web, a sus clientes, no solo de presentar un logotipo o utilizar una frase que permita indicar genialidad en tema de seguridad, deben explicar el parámetro de indicador del enlace cuando hace sugerencia al icono del candado el cual sugiere que la página a la que se está intentando ingresar es perjudicial por el sistema bloqueo o de seguridad que tiene el candado sirve para utilizar el cifrado de datos y que protocolos cumplen parámetros en dicha navegación.

Por lo que en la recepción de la idea que hizo un participante de la organización fue que las precauciones de los clientes de nivel servicio deben ser aceptados por el cliente y no deben ser subestimados al momento de la realización de estas transacciones ya que son los primeros que permiten la sujeción a este amplio tema, por lo que recae en la responsabilidad de educar a sus clientes en temas relacionados a consejos de seguridad. Mohaned y Cristhine (2008). *“Security Perception in E-commerce: Conflict between Customer and Organizational Perspectives”*

Las dimensiones de seguridad del comercio electrónico que ofrece la industria bancaria son una gran oportunidad, pero también crean un conjunto de nuevos riesgos y vulneraciones como amenazas a la seguridad. Que dentro de ellas están previstas la seguridad de la información, por lo que hay pautas para asegurar los sistemas y las redes disponibles para el personal de los sistemas de comercio electrónico, es por ello que se considera extensamente la compra y venta de productos a través de internet, pero cualquier transacción que se complete únicamente a través de medidas electrónicas puede ser considerada comercio electrónico, día a día el comercio electrónico está funcionando un esquema de planificación buena, en la categoría de venta de productos al por menor en línea y los pueblos que utilizan está tecnología, la lucha constante es protección contra la divulgación no autorizada de datos y los estafadores buscando sacar un beneficio de los compradores en línea propensos a cometer errores de principiante. Los errores comunes que dejan a la gente vulnerable incluyen el hacer compras en la website, que no son seguros, dando demasiada información personal y dejando las computadoras abiertas a los virus. Raghav (2014) *"Network Security Issues in e Commerce"*

La pre-disponibilidad del consumidor a la calidad de información del sitio web donde se ejecuta el desarrollo del comercio electrónico, en parámetros provisionalmente apropiados, el desarrollo de esta genera desconfianza que tiene que abordar un tema de generación de seguridades que permitan el crecimiento de la reputación del sitio web, promoviendo las campañas de reputación por parte de la compañía para que esta tenga fuertes efectos en la seguridad con la que se desarrolla el comercio electrónico en internet y en ese determinado sitio web. Los problemas principales que abordan de forma crítica es sustancialmente lo susodicho el tema de confianza en el desarrollo del comercio electrónico, por ello es primordial el tema de seguridad y privacidad; esta secuencia armoniosa tiene como requisito esencial en cuestión de control sobre los datos personales y la seguridad pertinente hacia el no acceso a estos datos. Para cualquier actividad de transacción de pago eficientemente y efectiva a través de internet, es por ello que el refuerzo del tema de la confianza y el comportamiento de compra son

estudiados en integridad, privacidad, no repudio, autenticidad, confidencialidad y disponibilidad. Palak y Akshat (2016) *"E-Commerce-Study of Pryvacy, Trust and Security from consumer's Perspective"*

Es de criterio basar los datos relevantes de las compras-ventas efectuadas por internet a través de plataformas web o medios electrónicos, que han sido desarrollados en las últimas décadas han sido vulneradas por delincuentes informáticos, este nuevo ambiente propicio para el desarrollo de la actividad económica si bien reduce costos ha tenido vulneraciones a su desarrollo por lo que han sido materia de análisis y posteriormente dado a generar una normatividad con respecto a los incumplimientos contractuales y los delito de estafa, se procede a explicar la tipología delictual pre establecida en el ordenamiento de montevideo respecto a las falsificaciones de documentos electrónicos comunes, el phishing o simulación de identidad online, entre otros sistemas delictuales a los que están abocados los black hacking. Pecoy (2011) "*Delito en el Comercio Electrónico*"

E-commerce está comprando y vendiendo bienes y servicios a través de Internet. El comercio electrónico es una parte del negocio electrónico que se especifica en. El comercio electrónico es una estructura que incluye no sólo aquellas transacciones que se centran en la compra y venta de bienes y servicios para generar ingresos, sino también aquellas transacciones que apoyan la generación de ingresos. Estas actividades incluyen generar demanda de bienes y servicios, ofrecer soporte de ventas y servicio al cliente, o facilitar las comunicaciones, entre los socios comerciales. Uno de los factores críticos de éxito del comercio electrónico es su seguridad. Sin la garantía de seguridad, el comercio electrónico puede no funcionar normalmente. Y es un problema de complejidad, porque el comercio electrónico de seguridad se refiere a la confianza entre vendedores y compradores, tarjeta de crédito y extremadamente.

Información personal confidencial. Por lo tanto, la seguridad del comercio electrónico depende de una compleja interrelación entre plataformas de aplicaciones, sistemas de gestión de bases de datos, software e infraestructura de red y así sucesivamente. Cualquier debilidad puede

poner en peligro la seguridad del comercio electrónico Revathi, Shanthi y Saranya (2015) *"A Study on E- Commerce Security Issues"*

Se proporciona un método para el comercio electrónico usando un testigo de seguridad y un aparato del mismo. El método de comercio electrónico que utiliza un token de seguridad comprende una entidad de aprobación de transacciones que genera un testigo de seguridad basado en lenguaje de marcado de aserción de seguridad (SAML), que utiliza la información de crédito de un comprador que solicita emitir un token de seguridad y transmite el token de seguridad al comprador. El comprador escribe una firma electrónica en una orden y transmite la orden junto con la ficha de seguridad a un vendedor; el vendedor tiene que verificar la orden acotada y el token de seguridad y luego entrega los bienes de acuerdo con la orden del comprador; la entidad de aprobación de la transacción que realiza el pago para el vendedor y el comprador. El método puede resolver los problemas de fugas de información personal y violación de privacidad que pueden ocurrir cuando un comprador envía su información personal a un vendedor para el comercio electrónico. Dado que el token es un solo uso de datos, incluso si un token de seguridad enviado es falsificado o robado, la pérdida puede ser minimizada. Además, puede garantizarse la autenticación, integridad y no repudio de un mensaje transmitido mediante la escritura de una firma electrónica de lenguaje de marcado extensible (XML), ya través de la tecnología de seguridad de protocolo de acceso a objetos (SOAP), se mantiene la confidencialidad. Joo, Ki y Sung, (2005) "*Method for electronic commerce using security token and apparatus thereof*"

Es por ello que el E-commerce (comercio electrónico) o EC es la compra y venta de bienes y servicios, o la transmisión de fondos o de datos, a través de una red electrónica, principalmente internet. Se producen estas transacciones comerciales, ya sea como b a b (de empresa a empresa), b a c (negocio a consumidor), c a c (consumidor a consumidor) o C a B (de consumidor a negocio). Es la negociación o en los productos o servicios a través de redes informáticas como Internet o las redes sociales en línea.

Aquí funciona el negocio a través del uso de los ordenadores, teléfonos, máquinas de fax, los lectores de códigos de barras, tarjetas de crédito, cajeros automáticos (ATM) u otros aparatos electrónicos sin el intercambio de documentos en papel o físicamente en movimiento a un centro comercial. Incluye actividades como las compras, entrada de pedidos, procesamiento de transacciones de pago en línea, autenticación, control de inventario, pedidos, envío y atención al cliente. Cuando un comprador paga con una tarjeta bancaria se pasó a través de una banda magnética, lector, él o ella está participando en el comercio electrónico. Seguridad el comercio electrónico es una parte del marco de seguridad de la información y se aplica específicamente a los componentes que afectan el comercio electrónico incluyendo la seguridad de datos y otros reinos más amplios del marco de seguridad de la información.

La seguridad del comercio electrónico es la protección de los bienes de comercio electrónico frente al acceso, uso, alteración o destrucción. Dimensiones del comercio electrónico de seguridad en la integridad, no repudio, autenticidad, confidencialidad, privacidad, disponibilidad. Comercio electrónico ofrece la industria bancaria gran oportunidad, pero también crea un conjunto de nuevos riesgos y vulnerabilidad, como amenazas a la seguridad, hackings.

Por lo tanto, se trata de una gestión esencial y requisito técnico para cualquier actividad de transacción de pago eficiente y eficaz a través de Internet. Debido al cambio tecnológico y empresarial constante y requiere un partido coordinada de algoritmo y soluciones técnicas. En este trabajo discutimos con visión general de seguridad para el comercio electrónico, varios pasos para realizar un pedido, el propósito de seguridad en el comercio electrónico, varios problemas de seguridad en el comercio electrónico, las directrices para la compra segura en línea, etc. Prasad, Neelamadhab y Panigrahi (2016) "*Security Issues over E-Commerce and their Solutions*"

Peixlan (1998) "*Issues of Security and Privacy in Electronic Commerce"* La mayor lista de encuestas de opinión "la inseguridad de las

transacciones financieras" y "pérdida de privacidad" entre los principales impedimentos para el comercio electrónico, pero en realidad la mayoría de los usuarios tienen ideas solamente fiebres intermitentes sobre las amenazas y riesgos, y un conocimiento muy limitado de las posibilidades técnicas y legales para minimizar su riesgo. Como resultado de ello existen todo tipo de percepciones erróneas. Hay cuatro componentes que intervienen en el comercio electrónico de seguridad: software de cliente, software de servidor, el sistema operativo del servidor, y el transporte de red. A lo cual cada componente tiene su propio conjunto de problemas y retos asociados con el abastecimiento de ellos siendo los siguientes parámetros que seguir:
El software de cliente es cada vez más centrado en la seguridad, sin embargo, los sistemas operativos de escritorio de un único usuario históricamente no han tenido funciones de seguridad implementadas. Software de comercio electrónico que se basa en la seguridad del sistema operativo de escritorio se ve comprometida fácilmente sin la aplicación de los controles físicos estrictos.
El software de servidor está constantemente bajo ataque de prueba y por la comunidad de usuarios.

Aunque ha habido casos de inseguridades, un administrador de sistema de mantenerse al día con los últimos parches y la información del proveedor puede proporcionar un alto grado de confianza en la seguridad del propio servidor.

Los sistemas operativos utilizados para servidores de alojamiento de comercio electrónico son asegurables, pero rara vez enviados desde el proveedor en una configuración por defecto que son seguras. Servidores de comercio electrónico debe proteger la base de datos de información de los clientes acumular en el servidor, así como garantizar la seguridad mientras el servidor está manejando una transacción. Si es más fácil para un ladrón para comprometer el servidor para obtener números de tarjetas de crédito, ¿por qué molestarse olfateando la red de números de tarjetas de crédito individuales?

Transporte sesión entre el cliente y el servidor utiliza protocolos de red que pueden tener poca o ninguna seguridad incorporado. Además, los protocolos de red como TCP / IP no fueron diseñados para tener capacidades de confidencialidad o de autenticación.

La seguridad constituye un problema central para las transacciones que se realizan en Internet, al existir la probabilidad que esta transacción pueda ser objeto de interceptaciones para alterar, modificar y robar bienes que circulan en dichas redes, por los conocidos hackers o craqueas. Si bien la seguridad en estos procesos tiene un sistema de clasificación basado en niveles de seguridad otorgada a estos sistemas. Las cuales tienen un sistema de seguridad lógico que debe contemplar ciertas medidas.

La privacidad y la seguridad son una preocupación importante para las tecnologías electrónicas. El comercio móvil (Mobile - Comercio) comparte las preocupaciones de seguridad con otra y organizaciones comprometidas con el comercio electrónico. En la web e- aplicaciones de comercio que manejan los pagos como la banca en línea, las transacciones electrónicas o el uso de tarjetas de débito, tarjetas de crédito, PayPal, E-Money en efectivo, tarjetas de prepago, tarjetas maestras, tarjetas visa u otros símbolos tienen más problemas de cumplimiento, las tecnologías en el campo. Preocupaciones sobre la privacidad han sido encontradas, que revela una falta de confianza en una variedad de contextos, incluyendo el comercio, la historia clínica electrónica, tecnología de la contratación electrónica y las redes sociales, y esto ha influido directamente en los usuarios. La seguridad es uno de los factores más importantes que limitan los clientes y organizaciones comprometidas con el comercio electrónico.

El comercio electrónico ahora abordar lentamente por los problemas de seguridad en sus redes internas. Hay tal tipo de directrices para asegurar los sistemas y redes disponibles para el personal de sistemas de comercio electrónico para leer y poner en práctica. Como la mayoría de los clientes de los que están utilizando las compras en línea algunos son gente que tiene conocimiento y algunos son tan novatos, por ende se necesita educar al consumidor sobre cuestiones de seguridad se encuentra todavía en la etapa de la infancia, pero resultará ser el elemento más crítico de la arquitectura

de seguridad del comercio electrónico. Virus, gusanos, caballos de Troya lanzados contra los sistemas cliente plantean la mayor amenaza al comercio electrónico, ya que pueden pasar por alto o subvertir la mayor parte de los mecanismos de autenticación y autorización utilizados en una transacción de comercio electrónico. Estos programas pueden ser instalados en un equipo remoto por los medios más simples: adjuntos de correo electrónico.
Por lo que alguno de privacidad se ha convertido en una preocupación importante para los consumidores con el aumento de robo de identidad y la suplantación, y cualquier preocupación para los consumidores deben ser considerados como una preocupación importante para los proveedores de comercio electrónico.

La seguridad es una de la parte crucial restringir clientes y organizaciones comprometidas con el comercio electrónico. El objetivo de este trabajo es explorar la percepción de seguridad en el comercio electrónico, básicamente, en viaje de negocios a B2C cliente y el cliente a sitios web C2C cliente, tanto de los clientes y las perspectivas de la organización. Halaweh y Fidler (2008) "Percepción de Seguridad en Comercio electrónico: Conflicto entre el Cliente y organizacional Perspectivas". Actas de la multiconferencia Internacional sobre Ciencias de la Computación y Tecnología de la Información,

Con el rápido crecimiento del mercado global en el comercio electrónico, los problemas de seguridad están surgiendo de atención de la gente. La seguridad de la transacción en línea es las cuestiones básicas y fundamentales del desarrollo del comercio electrónico. Este artículo acerca de los problemas de seguridad de las actividades de comercio electrónico presentado estrategia de solución a partir de dos aspectos que son I. Tecnología y el Sistema, con el fin de mejorar el entorno para el desarrollo del comercio electrónico y II. Promover el desarrollo del comercio electrónico. Yuanqiao y Chunhui (2008) Investigación Sobre Cuestiones de Seguridad en el Comercio Electrónico". Seminario Internacional de Negocios e Información Administración.

2.2. Teorías relacionadas al tema

2.2.1. Ley de los Servicios de la Sociedad de la Información y Comercio Electrónico- Fuentes del Derecho Ley de España

Mediante esta Ley, el Estado español ha pretendido dinamizar el tejido empresarial español y, al mismo tiempo, establecer la necesaria protección de los derechos de los usuarios de manera que estos no pierda sus derechos a favor de la seguridad internacional (López, 2006:180). Indudablemente, la legislación española, regulariza una expresión de la forma del ciberespacio en la era globalizada, acotando experticias de la comunidad económica europea en dicha materia, análisis que tiene acierto acorde a lo que señala Suñe (2006) La humanidad ha entrado en una nueva etapa de su desarrollo, en la que la sociedad de la información representa como el máximo exponente de las profundas transformaciones tecnológicas acaecidas en los últimos años. Parece entonces evidente que la configuración y difusión de la información contenida en este caudaloso flujo tiene una repercusión directa sobre el mundo de los derechos, las libertades y los comportamientos de muchas personas, a las que se puede generar indefensión. Concretamente, los problemas jurídicos se manifiestan como los más relevantes, puestos que la adecuación de la reglamentación legal del flujo interno e internacional de la información y datos se constituye en un reto esencial al que se deben enfrentarse los diversos ordenamientos jurídicos.

Está ley engloba la contratación de los bienes y servicios por vía electrónica, el suministro de información por dicho medio, las actividades de intermediación relativas a la provisión de acceso a la red, a la transmisión de datos por redes de telecomunicaciones, a la realización de copia temporal de las páginas de internet solicitadas por usuarios, al alojamiento en los propios servidores de información, servicios o aplicaciones facilitados por otros o a la provisión de instrumentos que sirven de búsqueda o de enlaces a otros sitios de internet, así como cualquier otro servicio que se preste a petición individual de los usuarios, siempre que represente una actividad económica para el prestador. Estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a internet los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio

en internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico.

Falsedad Informática, la tipificación de esta conducta pretende proteger todo tipo de documentos privados o públicos, que tengan carácter probatorio. Hoy, la mayoría de las transacciones en comercio electrónico se hace en este formato y son muy pocas las oportunidades que se registran en soporte papel. Piénsese, por ejemplo, en la transacción que realiza un comerciante colombiano con zapatos italianos y, a través de accesos ilegales al sistema.

2.2.2 Ley 30096 Delitos Informáticos- Teoría del Delito

Un delito informático o ciberdelito es toda aquella acción antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito", por lo cual se definen como abusos informáticos (los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas), y parte de la criminalidad informática. La criminalidad informática consiste en la realización de un tipo de actividades que, reuniendo los requisitos que delimitan el concepto de delito, sean llevados a cabo utilizando un elemento informático.

Los también conocidos como Ciberdelitos que son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas atípicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico) (Téllez, 2004).

2.2.3 Convenio internacional de Budapest (Hungría)

Buscar adherirse a la legislación contra el ciberdelito o cibercriminalidad, suscrito en 2001 por distintos países, implementar los equipos preparados en

emergencias informáticas y a su vez la fortificación de la ley destinada a aplicar herramientas de informática forense.

El estado peruano hace algunas interpretaciones auténticas del texto referente a lo establecido en el convenio de Budapest, mas no fortalece equipos preparados para emergencias informáticas, ni crea instrumentos para desarrollar informática forense.

2.3. Principios relacionados con el tema

2.3.1 Principios de la Protección de datos

2.3.1 Principio de legalidad de la protección de datos

El tratamiento de los datos personales se hace conforme a lo establecido en la ley. Se prohíbe la recopilación de los datos personales por medios fraudulentos, desleales o ilícitos

2.3.1.2 Principio de consentimiento de la protección de datos

Para el tratamiento de los datos personales debe mediar el consentimiento de su titular.

Rebollo (2008) que el consentimiento para el tratamiento de datos es una facultad de libertad del individuo para decidir acerca de sus datos, aunque se encuentra muy mediatizada en la norma por el conjunto de excepciones a que se ve sometida. El art. 6.1 contiene una regla general y una excepción, también general, amparada en una disposición legal. Según la Agencia Española y las Recomendaciones emitidas por el Comité de Ministros del Consejo de Europa son los siguientes: libertad en la prestación el consentimiento, específico, informado e inequívoco y expreso para el caso de los datos sensible. Otra regla general es la revocación del consentimiento para los casos en que la entrega de los datos se realiza en forma libre, con la inexistencia de efectos retroactivos

2.3.1.3 Principio de finalidad de la protección de datos

Los datos personales deben ser recopilados para una finalidad determinada, explicita y lícita. El tratamiento de los datos personales no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación, excluyendo los casos de actividades de valor histórico, estadístico o científico cuando se utilice un procedimiento de disociación o anonimización.

Los datos solo podrán utilizarse para las finalidades para la cual fueron recogidos. Sobre el principio de finalidad ampliaremos en el punto siguiente. Este principio de veracidad aparece en el Considerando 28 de la Directiva 95/46/CE que dice: "Considerando que todo tratamiento de datos personales debe efectuarse de forma lícita y leal respecto al interesado; que debe referirse en particular, a datos adecuados, pertinentes y no excesivos en relación con los objetivos perseguidos; que estos objetivos han de ser explícitos y legítimos y deben estar determinados en el momento de obtener los datos; que los objetivos de los tratamientos posteriores a la obtención no pueden ser incompatibles con los objetivos originariamente especificados.

2.3.1.4 Principio de proporcionalidad de la protección de datos

Todo tratamiento de datos personales debe ser adecuado, relevante y no excesivo a la finalidad para la que estos hubiesen sido recopilados.

Los datos de localización, ya que permiten conocer la posición geográfica de una persona, constituyen datos personales y su tratamiento debe respetar los principios. En el caso del informe la finalidad era garantizar la seguridad de la persona escoltada. Por tanto, el informe considera que se respeta el principio de proporcionalidad respecto a la utilización de esos datos en la jornada laboral, pero no respeta dicho principio el tratamiento de los datos de localización fuera del horario de trabajo, ya que la finalidad no requiere ese tratamiento.

El informe de la Agencia Española de protección de datos 368/2006 resuelve sobre si era lícito establecer un sistema de control para gestionar las

ausencias y retrasos de los alumnos de un colegio, basado en la obtención de la huella dactilar de éstos. El informe concluye que la obtención de la huella dactilar para identificar a los alumnos de un centro resulta excesivo y desproporcionado para el fin que se persigue, ya que no se considera justificado el tratamiento de datos de menores para la finalidad pretendida.
Es por ello que se busca definir lo que es cancelación y se realizara mediante lo que define la normativa española,

A) Bloqueo de datos: procedimiento mediante el cual se reservan datos con el fin de impedir su tratamiento, excepto para ser puestos a disposición de los Poderes del Estado, o instituciones que estén legalmente habilitadas, a los efectos de atender las posibles responsabilidades surgidas del tratamiento.

B) Cancelación o Supresión de datos: procedimiento mediante el cual el responsable cesa en el uso de los datos. La supresión o cancelación implicará el bloqueo de dichos datos durante el plazo establecido en la normativa vigente; vencido éste se deberá proceder a su eliminación definitiva. También el Real Decreto español en el artículo 5 b) define que se entiende por cancelación.

2.3.1.5 Principio de calidad

Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible actualizados necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopiladas. Deben conservarse de forma tal que se garantice su seguridad y solo por el tiempo necesario para cumplir con la finalidad de tratamiento.

2.3.1.6 Principio de seguridad

El titular del banco de datos personales y el encargado de su tratamiento, deben estar compuestas por técnicas organizadoras y dispositivos de ley de importancia para tener por garantizada de seguridad de los datos personales. Las medidas de seguridad deben ser oportunas y acorde con el procedimiento que se van a ejecutar y con la clasificación de

datos personales que contengan. Esto hace referencia al desarrollo de instrumentos de soportes informáticos que permitan garantizar las políticas normativas de privacidad y base de datos.

2.3.1.7 Principio de disposición de recurso

Este principio hace noción al hecho del titular de algún dato personal en caso de haber sido vulnerado en sus derechos tiene una tutela jurisdiccional efectiva sea la vía administrativa o las necesarias para reclamar y hacer valer su derecho.

2.3.1.8 Principio del nivel de protección adecuado

La estandarización acorde a las normas internacionales o nacionales para desarrollar un nivel de seguridad eficiente en el marco del desarrollo de la transferencia.

2.3.1.9 Valor de los principios

Los criterios interpretativos para resolver cuestiones previstas sobre los bancos de datos personales y en general a estos, tienen que estas regidos por los dispuestos en la Ley N° 29733.

2.3.2 Principios Fundamentales del Comercio Electrónico

2.3.2.1 Confianza.

Conseguir la confianza de un consumidor, esta meta se lograría de acuerdo con los parámetros de un mercado electrónico propicio para su desarrollo eficiente.

2.3.2.2 Privacidad.

Con la privacidad se ofrece el máximo grado de reserva de las transacciones realizadas, así como la identidad de los clientes y sus datos personales.

2.3.2.3 Seguridad.

La seguridad es un rol fundamental en el dinamismo del internet para mantener un nivel seguro en los accesos y datos a tratar

2.3.2.4 Autentificación.

La certitud de la fuente de datos, de que quien envía los mensajes y datos es por la firma autorizada.

2.3.2.5 Orientación al cliente.

Información que recibe el cliente es de vital importancia, por lo que se debe realizar un esfuerzo por crear un ambiente propicio para la satisfacción de los requisitos que necesite el cliente, incluso superando sus expectativas.

2.4. Conceptos relacionados con el tema

2.4.1 Conceptos básicos de Variable dependiente- Bloqueo del IP Dinámico dentro del Comercio Electrónico

2.4.1.1 Protocolo de internet fijo, protocolo de internet dinámico y Proxy

Una dirección de IP es una serie de números los cuales identifican de manera lógica y jerárquica a una interfaz de un dispositivo que está en una red la cual utiliza el protocolo de IP, este protocolo se encuentra en el nivel de Red en el modelo de OSI. Está dirección se diferencia de manera significativa de la dirección MAC, dicha dirección se utiliza para identificar la tarjeta de Red y esta no depende del protocol que se esté utilizando en la Red

El protocolo de Internet (IP), como componente fundamental de la familia de protocolos (una colección de cerca de 500 protocolos de red) es un protocolo no orientado a conexión responsable del direccionamiento y la fragmentación de paquetes de datos en redes digitales. Junto al protocolo de control de transmisiones (TCP o Transmission Control Protocol), IP sienta las bases de Internet. Para que el remitente pueda enviar un paquete de datos al destinatario, el protocolo de Internet define una estructura de paquetes que agrupa los datos que se tienen que enviar. Así, el Internet Protocol establece cómo se describe la información sobre el origen y el destino de los

datos y los separa de los datos útiles en la cabecera IP. Un formato de paquetes como tal recibe el nombre de datagrama IP.

2.4.1.2 Dirección de IP fija

Una dirección IP estática se parece a una dirección postal fija o a un número de teléfono y se asigna a un dispositivo de manera permanente. Las direcciones IP estáticas se localizan, sobre todo, en servidores web o en servidores de correo electrónico, o en general allí donde tanto las ofertas como los contenidos (de páginas web) estén disponibles a través de un URL fijo. El objetivo de ello es que los usuarios o los procesos las encuentren (o vuelvan a encontrarlas) sin problemas. Asimismo, los ordenadores de una red o los periféricos como las impresoras tienen direcciones IP fijas para que cada uno de los dispositivos de una red pueda comunicarse fácilmente entre sí.

Para que los usuarios no tengan que hacer frente a paquetes de cifras complejos, las IP estáticas son capaces de asignar un nombre de dominio, como por ejemplo *www.example.org*. La IP numérica, el "número de puerto" de un dispositivo en la red, se traducirá en un nombre que sea fácil de recordar, aunque esto es algo que solo es de aplicación en las IP estáticas. En el caso de las IP dinámicas no tendría apenas sentido, ya que estas cambian de usuario continuamente. 1&1 Internet España S.L.U. (2017)

Una dirección de IP estática, hace que se pueda geolocalizar dispositivos digitales conectados a una red, lo que hace de ello una condición fundamental para la distribución de paquetes de datos electrónicos de manera fidedigna.

2.4.1.3 Dirección de ip dinámico

Detallar sobre lo que es una IP Dinámica, tiene que darse la noción de cómo es que funciona una dirección de IP, por ende, es

que se define al Internet como el cumulo de conexiones establecidas por muchos ordenadores a través de cables de redes, fibra óptica y herramientas receptoras inalámbricas que transfieren o transmiten datos entre sí programadas en un lenguaje común. Este estándar es el (IP), de este modo aquellos ordenadores que puedan interpretar esta transferencia de datos, es porque se entiende el mismo protocolo.

Cuando un ordenador se conecta a Internet, suele ser el proveedor de servicios de Internet (ISP, Internet Service Provider) el que le asigna una dirección IP dinámica. Dichas IP dinámicas son la opción más rentable tanto para los usuarios como para los proveedores y se caracterizan por el hecho de que se asignan a un mismo aparato de manera temporal y se modifican en intervalos de tiempo determinados que en ocasiones son fijos (por ejemplo, cada 24 horas) y en otras irregulares. En estos casos, el usuario recibe una nueva dirección IP para su ordenador por parte del proveedor correspondiente, mientras que la dirección IP anterior se le asigna a otro usuario.

Cuando es que una IP dinámica puede configurar daños a otros usuarios es cuando con estás se montan Proxys.

2.4.1.4 Proxy

La necesidad de definir este término es en medida el uso de navegación la cual es ventajosa porque cierne la privacidad del anonimato en la navegación, pero es por ello que dentro del comercio electrónico esta sería un déficit ya que convertiría un medio para facilitar el delito del fraude electrónico, Caché de datos entre 2 ordenadores. Algunos proxies pueden guardar copias de las transferencias, lo que supone cierta intromisión e inseguridad dentro de los servidores de transferencia en el comercio electrónico y sus distintas modalidades de desarrollo, ya que para montar un proxy solo requiere una IP dinámica, un servidor, un dominio, configurar el

servidor (Linux o Windows) para ello, una sencilla página web, banners de publicidad y promocionarse.

Es así que un proxy es un ordenador intermedio que se usa en la comunicación de otros dos. La información (generalmente en Internet) va directamente entre un ordenador y otro. Mediante un proxy, la información va, primero, al ordenador intermedio (proxy), y éste se lo envía al ordenador de destino, de manera que no existe conexión directa entre el primero y el último.

En casi la totalidad de los casos, el proxy sólo sirve para ocultarse, y la mayoría de las veces estos proxies se usan para realizar prácticas ilegales (spam, fraudes, etc.). Es por ello, por lo que siempre es deseable evitar los proxies, sobre todo cuando son servidores de foros, chat o redes sociales.
En otros casos (esa minoría de los casos), es cuando se usa un proxy como interconexión entre muchos ordenadores de una red, con Internet. En ese caso, se puede usar un proxy por las ventajas añadidas que posee.

2.4.1.5 Bloqueo del ip dinámico

Desarrollo del Bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención en los delitos informáticos de la Ley 30096, tiene como punto de partida inicial desde el diseño del Comercio electrónico y el desarrollo de este en sus modalidades de B2B, B2C, C2C.

El enfoque general del desarrollo de esta investigación es el centrarse en proponer un ambiente propicio análogo al de una plataforma masiva de personas conectadas online similar al de un video juego pero diseñada con los arquetipos propicios para originar un mundo virtual abocado al comercio electrónico a nivel global en tiempo real manteniendo como medida de seguridad una restricción de IP o bloqueo de IP dinámico para el mejoramiento de su

servidores análogos en las diversas plataformas web que permitan que el IP se configure como un geo localizador a tiempo real de las personas que se sujetan a una transacción electrónica o al desarrollo de un negocio a través del internet.

2.4.1.6 Comercio Electrónico

Desde el enfoque de las Comunicaciones, el comercio electrónico es aquel que distribuye información, productos, servicios o transacciones financieras, a través de Redes de Telecomunicación Multimedia, conformando estructuras empresariales de carácter virtual. Teniendo en cuenta los Procesos de Negocio, el comercio de red es el que utiliza las tecnologías que facilitan el soporte y la automatización de los flujos de trabajo y procedimientos de negocio de la empresa, con lo que esta consigue eficiencias en los costes, servicios con una mejor calidad y ciclos de producción más cortos.

Por último, desde una perspectiva Temporal, el comercio electrónico es el instrumento que permite establecerse nuevos canales para el intercambio de productos, servicios e información en tiempo real. (ANTEPORTAMLATINAM 2014).

Siendo su clasificación y sus formas de pago las expuestas a continuación de manera en la cual el desarrollo modalidades de prevención que puedan ser normativizadas para su pertinente desarrollo y eficiencia.

Comercio entre consumidores (C2C) Los propios consumidores realizan transacciones entre ellos. En este tipo de comercio electrónico destacan las subastas online (e-Bay, e-Schwab). Aunque para la mayoría de los autores se trata de una categoría monolítica, para otros como el profesor Skyrmeme, 2001: 55-56), es merecedora de una subdivisión:

Subastas (Auctions) las efectuadas mediante sistemas como e-Bay).

Las subastas en la Red permiten la venta de infinidad de productos por medio de pujas entre compradores. Su negocio se basa en la comisión sobre el precio de adjudicación que se genera. Esta comisión suele oscilar entre el 0 % y el 30%, en función del producto y la web específica. Facilitan el contacto entre compradores y vendedores, así como la presentación de productos y la información de los mismos, permite a los clientes y subastadores negociar entre ellos directamente eliminando intermediarios que encarecía los precios.

Reserve Auctions (subastas reservadas) (Comparaciones de precios de distintas tiendas online: el cliente elige donde comprar. El sitio que efectúa la comparación está realizado por consumidores.

Comercio Electrónico Entre Empresa y Consumidor (B2C) El desarrollo de esta modalidad de comercio electrónico está vinculado a los sujetos que interactúan dentro de esta relación que son la empresa y el consumidor a través de cualquier medio electrónico.

Siendo en este espacio favorable para el desarrollo económico, es que se suscitan nuevas formas de proceder delincuencial que buscan obtener beneficios a través de ilicitudes a través de internet, configurando así la clasificación de dos grupos: los delitos patrimoniales vinculados a la informática y aquellos con relación a la acumulación de datos de carácter personal en los sistemas informáticos, mencionando, sin indagar demasiado en ello, la problemática que podía surgir con la posible comisión de delitos contra intereses supraindividuales, o de cualquier otro tipo, a través de los ordenadores.

Es así que se enmarca la subdivisión de variables por cuanto la variable independiente arraigada a la medida de prevención en los delitos informáticos y cómo es que las interdisciplinariedades de dos

carreras hacen el papel de brindar medidas efectivas de enfoque preventivo y legislativo sancionador ante la evolución de los delitos, que en cuestión se desarrolla como delitos en los comercios electrónicos.

2.4.2 Medida de Prevención ante los Delitos Informáticos de la Ley 30096

Este enfoque se subsume a una prevención una medida de seguridad que permita en parte asegurar de forma eficiente usando una sistematización de intercambio de moneda análoga al bit coin, y absorbiendo a las otras medidas de seguridad en un solo ambiente para el desarrollo del comercio electrónico, el propósito es buscar crear un ambiente propicio, con cual el desarrollo de este mercado virtual en expansión se vea afectada en el menor rango posible por las ilicitudes del accionar ciber delincuencial que se suscitan en estas negociaciones a posterior se convierten en posibles pérdidas económicas y desconfianza en los usuario, producto del uso frecuente de computadoras y de la posibilidad de interconexión global da lugar a un verdadero fenómeno de nuevas dimensiones denominado: “El Delito Informático”.

La modalidad en esta fase de irrumpir ilícitamente en cualquier forma de inejecución de la obligación a la que se sujetaron los individuos configura un Fraude Electrónico,

2.4.2.1 Soportes informáticos

Han influenciado en la nueva forma de hacer comercio, es la herramienta con la que se ha viabilizado la comercialización entre ausentes en tiempo real mediante soportes electrónicos, que al margen de permitir la comunicación entre los contratantes también permite de acuerdo a su potencial, el almacenamiento y procesamiento de información hardware; conjugado con el del programa instalado en el soporte físico almacena y hace réplicas los datos o mensajes introducidos o confeccionados por dichos soportes, perdiendo el sentido de original y copia, significando para el comercio electrónico la ventaja de la indistinguibilidad de la fidelidad al perder sentido

copia y original, con un bajo costo de las reproducciones, permitiendo el soporte informático digital que el documento sea maleable al permitir combinaciones y transformaciones. Arata (2002) et al.

A pesar de los soportes de telecomunicaciones regulados no se puede ir directamente a Internet, sino que es todo un proceso, donde previamente, tenemos que contar con un dominio genérico de nivel superior (TLD) a cargo de una Corporación de Asignación de Nombres de Dominio, a nivel mundial el ICANN Internet Corporation for assigned name and numbers. Siendo que quien tiene a cargo el registro de nombre de dominio y de la administración del dominio "pe" es la Red Científica Peruana, siendo proveniente de una institución conocida como PE-NIC (Network Information Center). Hoy está supervisada por INDECOPI.

2.4.2.2 Geolocalización de las partes y seguridad en las transacciones del comercio electrónico

Está siendo sujetada a dar por determinada a las partes, en el plano físico y real y no virtual la cual se puede encontrar a través de la IP, siendo requisito primordial la consignación de esta para toda clase de negociación virtual.

La nueva tecnología y el avance de las comunicaciones han variado la forma de delinquir, y asociado a ello, de investigar al delincuente. Son múltiples las variantes que la técnica pone a nuestra disposición para averiguar la ubicación de una persona, y no todas están recogidas por la norma o gozan de una regulación pormenorizada al respecto. Estamos ante un complejo y escaso entramado normativo que, en muy pocas ocasiones, hace referencia concreta a la geolocalización, y no es excepción a ello la obtención de datos a través de la dirección IP. Hemos de plantearnos cómo deben acceder las Fuerzas y Cuerpos de Seguridad del Estado a dicha información

con total respeto a los derechos fundamentales de los ciudadanos, sin que se produzca vulneración alguna, con el objeto de poder usar la misma como fuente de prueba en el proceso penal. (Cabello, 2017)

Descendiendo al tipo concreto de dato de geolocalización que nos ocupa, debemos de partir de la posición del Tribunal Supremo en relación con la dirección IP. Su jurisprudencia afirma que la misma, si bien sí identifica a un ordenador determinado con una concreta conexión, no lo hace por sí respecto del usuario, por lo que estima que no se precisa autorización judicial para conseguir lo que es público, no encontrándose protegido ni por el apartado 1 ni por el 3 del artículo

18 de la Constitución Española. Sentencia del tribunal supremo de España, sala segunda, 292/2008

Por tanto, la obtención de esa IP, en el sentido de conexión a Internet, no ha de considerarse como comunicación, y sí como presupuesto técnico necesario para hacerla posible. López (2012)

Cuestión distinta de la conexión técnica como tal, son las subsiguientes actuaciones de identificación y localización de la persona que tiene asignado esa IP, ya que éstas sí se deben efectuar al amparo judicial, porque a diferencia de la dirección IP, el nombre del usuario al que corresponde es un dato proporcionado al proveedor en el marco de una relación contractual sometido únicamente al régimen de protección de datos. Así, la averiguación de la dirección de IP estática debe considerarse como dato de suscripción, mientras que si fuera dinámica se hallaría vinculada como una comunicación concreta.

Lo anterior puede complicarse aún más, y ello sucede cuando se utiliza para la navegación por Internet una dirección IP de un servidor que no aporta datos sobre sus usuarios, de modo que se logra poner un intermediario entre el ordenador y la web o el servicio al que se accede, quedando únicamente en éste sólo los datos del servidor, pero no los del usuario. Estos intermediarios son conocidos como servidor Proxy.

2.4.2.3 Delitos informáticos

Los delitos informáticos se vinculan con la idea de la comisión del crimen a través del empleo de la computadora, internet, etc; sin embargo, está forma de criminalidad no solo se comete a través de estos medios, pues estos son solo instrumentos que facilitan, pero no determinan la comisión de estos delitos. Está denominación es poco usada en las legislaciones penales, no obstante, bajo ella se describe una nueva forma de criminalidad desarrollada a partir de un elevado uso de la tecnología informática. Coello (2010)

En este tipo de delitos no se puede establecer a la información como el único de bien jurídico afectado, por ser el principal y el más importante; sino a un conjunto de bienes que son afectados, debido a la característica de la conducta típica en esta modalidad delictiva que colisiona de diversos intereses colectivos. Villavicencio (2015)

2.4.2.4 Principales problemas del mundo informático, la economía y la afectación al derecho

Proceso de integración cultural, económica y social a nivel mundial viene acompañado del gran desarrollo de la tecnología de la información y comunicación (en adelante TI C), y la masificación de la misma aparece jugando un papel importante en el desarrollo cultural de la sociedad. Las nuevas herramientas que ponen las TI C al servicio del hombre están relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de información, así como un conjunto de procesos y productos que simplifican la comunicación, y hacen más viables la interacción entre las personas. Un invento tecnológico que reforzó el poder de las TIC es, sin lugar a dudas el internet (por ejemplo, a través del desarrollo de *messenger*, correo electrónico, *facebook*, *twitter*, *web*, etcétera). Este nuevo descubrimiento superó el paradigma real del tiempo-espacio en la interacción humana, en tanto la comunicación se podía dar en tiempo real sin importar la distancia. Por otra parte, las aplicaciones

de las TIC a partir de internet (entre ellas *cibergobierno*, *cibereducación* y *cibersalud*) se consideran habilitantes para el desarrollo social, puesto que proporcionan un canal eficaz para distribuir una amplia gama de servicios básicos en zonas remotas y rurales, pues estas aplicaciones facilitan el logro de los objetivos de desarrollo prospectivo, mejoras en las condiciones sanitarias y medioambientales.

Si bien los diversos ámbitos de interacción se ven favorecidos por la fluidez que le brinda esta nueva alternativa tecnológica, no obstante, crecen los riesgos relacionados al uso de las tecnologías informáticas y de comunicación. (AROCENA, 2012).

III. MÉTODO

3.1. Tipo y diseño de investigación

3.1.1. Tipo de Investigación

La presente investigación se desarrollará teniendo la base de una Investigación Descriptiva, ya que representa un grado de integración y combinación entre los enfoques:

3.1.1.1. Descriptiva.

Se tendrá como fase descriptiva el perfil del objeto de estudio que son los datos recolectados y puestos en observación de como el bloqueo del IP dinámico en las relaciones del C2C a través del E-Commerce, sirviendo de medida de seguridad como soporte informático y es a la vez una medida de prevención ante delitos informáticos, el proponer un nuevo parámetro referente una nueva forma de combatir a los delitos informáticos, aludido al comercio ilegal, fraude y estafa informática haciendo la implementación de este soporte informático, proponiendo y consignándola como medida de prevención.

Cervo y Bervian (1989), afirman: "una actividad encaminada a la solución de problemas. Su objetivo consiste en hallar respuestas a preguntas mediante el empleo de procesos científicos" (p. 41).

Si bien es cierto que, desde el punto de vista científico, la investigación se trata de realizar un proceso metódico y sistemático, el cual será dirigido a la solución de problemas o preguntas, a su vez se producirán diferentes e innovadores conocimientos y éstos conllevarán a las respuestas o soluciones para dichas preguntas formuladas.

Dankhe (1986), afirma: "Los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis" (p. 60).

3.1.2. Diseño de investigación

3.1.2.1. No experimental o transversal

En el diseño no experimental o transversal, se procura no utilizar intencionalmente las palabras, es decir, estas solo se emplean cuando es realmente necesario; esencialmente se hace uso de la observación de los hechos o1 circunstancias relacionadas al tema de estudio, los cuales una vez observados y captados, se analizarán con mayor detenimiento durante el desarrollo de la investigación. También es llamada investigación "ex post facto", porque se trata de observar a las variables, luego de que han ocurrido hechos o sucesos, para relacionarlas con el entorno presente que se está estudiando.

Kerlinger (1979), afirma: "La investigación no experimental o expost-facto es cualquier investigación en la que resulta imposible manipular variables o asignar aleatoriamente a los sujetos o a las condiciones" (p. 116).

3.2. Métodos de la investigación

Se ha estimado conveniente para la presente investigación, emplear:

3.2.1. Método científico descriptivo

Jiménez (1998) refiere a los estudios descriptivos como una fuente de conocimientos más concreta que los exploratorios. En los que el problema científico ha logrado cierto nivel de esclarecimiento pero aún se necesitan contenidos que sustenten o lleguen a establecer caminos que conduzcan a la claridad de las relaciones causales.

El problema es muchas veces de naturaleza práctica y su solución concurre por el conocimiento de las causas. Pero las hipótesis causales sólo pueden tener como punto de partida la descripción completa y profunda del problema en cuestión.

3.2. Variables, operacionalización

La operacionalización de variables, se basa en establecer el método apropiado mediante el cual las variables serán estudiadas, de acuerdo al tipo y diseño de investigación.

Hempel (1952) señala que "La definición operacional de un concepto consiste en definir las operaciones que permiten medir ese concepto o los indicadores observables por medio de cuales se manifiesta ese concepto"

3.2.1. Variables

3.2.1.1. Tipos de variable.

3.2.1.1.1. Variable Independiente. Bloqueo del IP Dinámico dentro del Comercio Electrónico.

Para describir, explicar el objeto de estudio durante su investigación. Cabe precisar, que estas variables generan y explican en la variable dependiente. Que según Pino (2010) variable independiente es aquella que el experimentador modifica a voluntad para averiguar si sus modificaciones provocan o no cambios en las otras variables, o sea, en variables dependientes. Recuerde que la variable dependiente es la que toma valores diferentes en función de las modificaciones que sufre la variable independiente.

3.2.1.1.2. ***Variable Dependiente. Medida de prevención ante los delitos informáticos de la ley 30096***

La variable medida de prevención ante los delitos informáticos, depende a la ejecución del Bloqueo del IP dinámico dentro del comercio electrónico; la prevención de la estafa informática o fraude informático mediante la observación, descripción y teorización de como la suscripción de la IP fija permite una geo localización oportuna de las partes acreedoras y deudoras, haciendo

un parámetro de bloqueo de IP su ubicación a través de un bloque de regiones plasmadas en una plataforma virtual que permita poner en ejecución al bloqueo de la IP dinámica para poner en marcha la prevención de los delitos informáticos establecidos en la ley 30096 que deriven del Comercio Electrónico.

Variables	Dimensiones	Indicadores	Técnicas e instrumento de recolección de datos
Variable dependiente: Medida de prevención de los delitos informáticos de la Ley 30096.	- Plataformas web de adaptadas al sistema VPN para el E-commerce.	Soportes Informáticos. - Geolocalización de las partes a través del IP. -Seguridad en las transacciones del E-Commerce. -Fraude en los E-commerce (Impago, phishing, hackers y otros) -	- Cuestionario/Encuesta
Variable Independiente: El bloqueo del IP dinámico dentro del Comercio Electrónico	Posibilidad jurídica suscripción de la IP. Propuesta para mejorar el desarrollo de soportes informáticos Seguridad acotada en el comercio electrónico -	.- Bases Teóricas y Doctrina. -Legislación comparada. -La Ley N° 30096 - - Ley Modelo de la CNUDMI sobre Comercio Electrónico.	- Cuestionario/Encuesta

3.3. Población y muestra

3.3.1. Población

La población es un término polisémico que abarca diversos significados, pero en lo referente a la presente investigación, y delimitada en nuestro proyecto de estudio al ser del tipo descriptivo, el área de la población estará entendida como un conjunto de diversos desarrollos de soportes informáticos o medidas de prevención que se toman en las actividades del comercio electrónico para brindar seguridad en las relaciones del C2C, además de documentos

legislativos vinculados entre sí por presentar características comunes las cuales servirán de base para la investigación y elaboración del desarrollo de una propuesta que de una posible solución al problema que se está estudiando en el presente trabajo.

a. Población de Informantes: responsables en la ejecución del nuevo código procesal penal y de nociones preventivas de actos antijurídicos que den configuración a delitos informáticos, por lo que su conocimiento dará posibles soluciones o márgenes de error de la investigación: Los Jueces, abogados y catedráticos de Derecho comercial, Penal se entrevistará a todos los informantes (50), ello le da carácter censal, y ningún censo requiere muestra.

3.3.2. Muestra

La muestra seleccionada por el investigador es la misma manifestada en la población

N°	TRABAJADORES PÚBLICOS	CANTIDAD DE FUNCIONARIOS Y SERVIDORES PÚBLICOS
01	Juez	20
02	Fiscal	10
03	Servidor Público	10
04	Abogados	10
	TOTAL, DE LA MUESTRA	**50**

Fuente: elaboración propia.

3.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

3.4.1. Criterios para la construcción y elaboración de las técnicas de recolección de datos

Los parámetros que permiten el desarrollo de la investigación experimental están establecidos dentro de los siguientes acápites:

3.4.1.1. Validez interna.

La validez interna es la directriz de la pregunta inicial, con cierta alusión al experimento determinado, la cual ha demostrado una relación inequívoca.

3.4.1.2. Validez externa.

En la amplitud del desarrollo de la investigación la validez externa dirige una pregunta más global, con alusión al escalón con que pueden generalizarse los resultados del experimento presentado en la investigación.

3.4.1.3. Fiabilidad.

Los instrumentos usados medirán con exactitud y certeza, en medida de que la data errónea sea reducida al mínimo. (Cortez, 2013)

3.4.1.4. Objetividad.

El interés de cada investigador no afectará al desarrollo de su investigación, pues la subjetividad no es una forma de asegurar resultados fehacientes y con rigor científico.

3.5. Métodos de análisis de datos

La aplicación de técnicas e instrumentos permitirán la obtención de datos los cuales serán incorporados a programas computarizados, como los aplicativos de IBM SPSS, siendo así las precisiones porcentuales y prelaciones u ordenamientos, los promedios serán presentados como información en forma de gráficos.

La modalidad de análisis de las informaciones a utilizarse en la presente investigación es mediante datos recopilados, gráficos, tablas y otros medios informativos al que se pueda acceder mediante los programas de Microsoft Excel o SPSS.

3.6. Aspectos éticos

La presente investigación está basada en principios fundamentales de la ética y la ética profesional. El “ethos” o ética de una profesión se define como la disciplina que estudia el conjunto de aquellas actitudes, normal éticas específicas y formas de juzgar las conductas morales, que la caracterizan como grupo sociológico. (Haring, 1977)

La "recopilación de buenas prácticas en la investigación" es visualizar el marco normativo y regulador de las actividades ligadas a la investigación, y que siguen las directrices

marcadas en los Estatutos de la Universidad Autónoma de Barcelona, basadas en los principios de libertad, democracia, justicia, igualdad y solidaridad. Este compromiso implica, por tanto, la orientación de la docencia, la investigación y la actividad universitaria hacia la cultura de paz, el respeto de los derechos humanos, el progreso social, el respeto por el medio ambiente y el desarrollo sostenible y la renuncia explícita a la investigación orientada directamente a finalidades militares. Esta investigación se basa en principios éticos principales:

3.6.1. El consentimiento informado

El uso del consentimiento informado responde a una ética kantiana donde los seres humanos deben ser tratados como un fin en sí mismos y nunca como un medio para conseguir algo. Así, los participantes del estudio deben estar de acuerdo con ser informantes y, a su vez, deben conocer tanto sus derechos como sus responsabilidades dentro de la investigación (Christians CG, 2000).

3.6.2. La confidencialidad

Los códigos de ética hacen énfasis en la seguridad y protección de la identidad de las personas que participan como informantes de la investigación. La confidencialidad se refiere tanto al anonimato en la identidad de las personas participantes en el estudio, como a la privacidad de la información que es revelada por los mismos, por tanto, para mantenerla se asigna un número o un pseudónimo a los entrevistados. El pseudónimo puede ser elegido por el participante, lo cual permitirá que este sienta confianza en el proceso y tenga credibilidad en la confidencialidad en los resultados de la investigación (Tod A., 2008).

IV. RESULTADOS

4.1. Resultados en tablas y figuras

TABLA 1 : Comercio Electrónico

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	10	50%		
b)	5	25%		
c)	4	20%		
d)	1	5%		
			20	14

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 1: Comercio Electrónico

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	7	70%		
b)	-	-		
c)	2	20%		
d)	1	10%		
			10	9

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 1: Comercio Electrónico

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	4	40%		
b)	2	20%		
c)	4	40%		
d)	-	-		
			10	8

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 1: Comercio Electrónico

SERVIDORES PUBLICOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	4	40%		
b)	3	30%		
c)	3	30%		
d)	-	-		
			10	7

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo

TABLA 1 : Comercio Electrónico

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	10	50%		
b)	5	25%		
c)	4	20%		
d)	1	5%		
			20	14

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 1: Comercio Electrónico

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	7	70%		
b)	-	-		
c)	2	20%		
d)	1	10%		
			10	9

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 1: Comercio Electrónico

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	4	40%		
b)	2	20%		
c)	4	40%		
d)	-	-		
			10	8

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 1: Comercio Electrónico

SERVIDORES PUBLICOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	4	40%		
b)	3	30%		
c)	3	30%		
d)	-	-		
			10	7

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo

Descripción:
De acuerdo a los datos obtenidos se puede establecer que, de un total de 50 personas que corresponde al 100%, señalaron que:

Fiscales: 9 de 10 encuestados equivalente al 90%, identificaron como concepto básico de comercio electrónico a la Compra Venta a través de Internet.

Abogados: 8 de 10 encuestados equivalente al 80%, identificaron como concepto básico de comercio electrónico a la Compraventa a través de Internet y secuencialmente Negociar en Plataforma Web.

Jueces: 14 de 20 encuestados equivalente al 70%, identificaron como concepto básico de comercio electrónico a la Infraestructura de Interfaces.

Servidores Públicos: 7 de 10 encuestados equivalente al 70%, identificaron como concepto básico de comercio electrónico a la Compraventa a través de Internet y secuencialmente Negociar en Plataforma Web.

TABLA 2: Geolocalización de las Partes por medio del IP

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	14	70%		
b)	6	30%		
			20	14

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 2: Geolocalización de las Partes por medio del IP

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	9	90%		
b)	1	10%		
			10	9

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 2: Geolocalización de las Partes por medio del IP

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	3	30%		
b)	7	70%		
			10	3

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 2: Geolocalización de las Partes medio del IP

SERVIDORES PUBLICOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	7	70%		
b)	3	30%		
			10	7

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo.

Descripción:
De acuerdo a los datos obtenidos se puede establecer que, de un total de 50 personas que corresponde al 100%, señalaron que:

Fiscales: 9 de 10 encuestados equivalente al 90%, considera que es eficiente brindar una plataforma que permita el bloqueo de la dirección de IP para asegurar las transacciones de pago en el comercio electrónico.

Abogados: 3 de 10 encuestados equivalente al 30%, considera otros medios de pago para garantizar la seguridad las transacciones de pago en el comercio electrónico.

Jueces: 14 de 20 encuestados equivalente al 70%, considera que es eficiente brindar una plataforma que permita el bloqueo de la dirección de IP para asegurar las transacciones de pago en el comercio electrónico.

Servidores Públicos: 7 de 10 encuestados equivalente al 70%, considera que es eficiente brindar una plataforma que permita el bloqueo de la dirección de IP para asegurar las transacciones de pago en el comercio electrónico.

TABLA 03-A: Transacción Electrónica Segura

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	7	35%		
b)	2	10%		
c)	-	-		
d)	2	5%		
e)	4	20%		
f)	6	30%		
			20	7

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 3: Transacción Electrónica Segura

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	2	20%		
b)	3	30%		
c)	-	-		
d)	-	-		
e)	1	10%		
f)	4	40%		
			10	2

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 3: Transacción Electrónica Segura

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	8	80%		
b)	-	-		
c)	-	-		
d)	-	-		
e)	-	-		
f)	2	20%		
			10	8

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 3: Transacción Electrónica Segura

SERVIDORES PUBLICOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	3	30%		
b)	5	50%		
c)	-	0-		
d)	-	-		
e)	-			
f)	2	20%		
			10	3

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo.

Descripción:

De acuerdo a los datos obtenidos se puede establecer que, de un total de 50 personas que corresponde al 100%, señalaron que:
Abogados: 08 de 10 encuestados equivalente al 80%, considera una forma de transacción segura a la modalidad de pago en depósito de cuenta débito o crédito de una de las partes.

Jueces: 07 de 20 encuestados equivalente al 35%, considera una forma de transacción segura a la modalidad de pago en depósito de cuenta débito o crédito de una de las partes.

Servidores Públicos: 3 de 10 encuestados equivalente al 30%, considera una forma de transacción segura a la modalidad de pago diferido con moneda virtual intercambiable a cualquier divisa.

Fiscales: 2 de 10 encuestados equivalente al 20%, considera una forma de transacción segura a la modalidad de uso de tarjeta virtual PayPal en compraventa en internet.

TABLA 4: Seguridad en la Tarjeta de Crédito en las Transacciones del Comercio Electrónica.

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	Si	40%		
b)	No	50%		
c)	No Opina	10%		
			20	0

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 4 – Seguridad en la Tarjeta de Crédito en las Transacciones del Comercio Electrónica.

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	Si	30%		
b)	No	60%		
c)	No Opina	10%		
			10	0

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 4: Seguridad en la Tarjeta de Crédito en las Transacciones del Comercio Electrónica.

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	Si	20%		
b)	No	60%		
c)	No Opina	20%		
			10	0

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 4: Seguridad en la Tarjeta de Crédito en las Transacciones del Comercio Electrónica.

Servidores P.				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	Si	20%		
b)	No	50%		
c)	No Opina	30%		
			10	0

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo.

Descripción:

De acuerdo con los datos obtenidos se puede establecer que, de un total de 50 personas que corresponde al 100%, señalaron que:

Abogados: 06 de 10 encuestados equivalente al 60%, indicaron no conocer sobre el bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención frente a los delitos informáticos, mientras que un 20% indico si conocer y el 20 % restante se limitó a no opinar.

Fiscales: 06 de 10 encuestados equivalente al 60%, indicaron no conocer sobre el bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención frente a los delitos informáticos, mientras que un 20% indico si conocer y el 20 % restante se limitó a no opinar.

Jueces: 10 de 20 encuestados equivalente al 50%, indicaron no conocer sobre el bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención frente a los delitos informáticos, mientras que el 40% indico si conocerlo y solo el 10% se limitó a no opinar.

Servidores Públicos: 5 de 10 encuestados equivalente al 50%, indicaron no conocer sobre el bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención frente a los delitos informáticos, el 30% indico si conocer el tema y solo 20% dijo si conocerlo.

TABLA 5: Reforzamiento de la Ley N°30096

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	-	-		
b)	18	90%		
c)	-	-		
d)	2	10%		
			20	0

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 5: Reforzamiento de la Ley N°30096

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	-	-		
b)	8	80%		
c)	2	-		
d)	-	-		
			10	0

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 5: Reforzamiento de la Ley N°30096

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	6	60%		
b)	4	40%		
c)	-	-		
d)	-	-		
			10	4

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 5– Reforzamiento de la Ley N°30096

SERVIDORES PUBLICOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	-	-		
b)	-	-		
c)	6	60%		
d)	4	40%		
			10	0

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo

Descripción:

De acuerdo a los datos obtenidos se puede establecer que, de un total de 50 personas que corresponde al 100%, señalaron que:

Fiscales: 8 de 10 encuestados equivalente al 80%, considera como opción de reforzamiento a la Seguridad en el Comercio Electrónico en la Ley N° 30096 en los casos de delitos informáticos en su modalidad de fraude al mejor desarrollo de

Jueces: 18 de 20 encuestados equivalente al 60%, considera como opción de reforzamiento a la de la Ley N° 30096 en los casos de delitos informáticos en su modalidad de fraude al mejor desarrollo de Seguridad en el Comercio Electrónico.

Servidores Públicos: 6 de 10 encuestados equivalente al 60%, considera como opción de reforzamiento a la Responsabilidad en la Ley N° 30096, en los casos de delitos informáticos en su modalidad de fraude.

Abogados: 04 de 10 encuestados equivalente al 40%, considera como opción de reforzamiento a la Conciencia de Seguridad en la Ley N° 30096, en los casos de delitos informáticos en su modalidad de fraude.

TABLA 6: Fraude Informático

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	10	50%		
b)	-	-		
c)	-	-		
d)	10	50%		
e)	-	-		
			20	10

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 6: Fraude Informático

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	5	50%		
b)	2	20%		
c)	-	-		
d)	3	30%		
e)	-	-		
			10	3

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 6: Fraude Informático

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	4	40%		
b)	2	20%		
c)	-	-		
d)	4	40%		
e)	-	-		
			10	4

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 6: Fraude Informático

SERVIDORES PUBLICOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	3	20%		
b)	5	50%		
c)	-	-		
d)	3	30%		
e)	-	-		
			10	3

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo.

Descripción:

De acuerdo a los datos obtenidos se puede establecer que, de un total de 50 personas que corresponde al 100%, señalaron que:

Fiscales: 5 de 10 encuestados equivalente al 50%, indica haber tenido conocimiento de Robo de Identidad como tipo de Fraude Informático, un 30% consideran a las Transacciones de Impago y solo un 20% al Phishing.

Jueces: 10 de 20 encuestados equivalente al 50%, indica haber tenido conocimiento de Robo de Identidad como tipo de Fraude Informático, mientras que el otro 50 % consideran a las Transacciones de Impago.

Servidores Públicos: 3 de 10 encuestados equivalente al 50%, indica haber tenido conocimiento del Pishing, como tipo de Fraude Informático, un 30% consideran a las Transacciones Impago y solo un 20% al Robo de Identidad.

Abogados: 04 de 10 encuestados equivalente al 40%, indica haber tenido conocimiento de Robo de Identidad como tipo de Fraude Informático, el otro 40% considera al Phishing y solo un al 20% Transacciones de Impago.

TABLA 7: Medida Preventiva en el Comercio Electrónico

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	-	-		
b)	13	65%		
c)	5	25%		
d)	2	10%		
			20	13

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 7: Medida Preventiva en el Comercio Electrónico

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	-	-		
b)	6	60%		
c)	4	40%		
d)	-	-		
			10	6

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 7: Medida Preventiva en el Comercio Electrónico

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	-	-		
b)	4	40%		
c)	3	30%		
d)	3	30%		
			10	4

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 07: Medida Preventiva en el Comercio Electrónico

SERVIDORES PUBLICOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	-	-		
b)	3	30%		
c)	2	20%		
d)	5	50%		
			10	3

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo.

Descripción:

De acuerdo a los datos obtenidos se puede establecer que, de un total de 50 personas que corresponde al 100%, señalaron que:

Jueces: 13 de 20 encuestados equivalente al 65%, indica como medida preventiva a la Geolocalización de las personas a través de dispositivos o tecnologías, producida dentro del Fraude Informático de la ley 30096 para que no genere excesivas pérdidas económicas dentro del comercio electrónico.

Fiscales: 6 de 10 encuestados equivalente al 60%, indica como medida preventiva a la Geolocalización de las personas a través de dispositivos o tecnologías, producida dentro del Fraude Informático de la ley 30096 para que no genere excesivas pérdidas económicas dentro del comercio electrónico.

Abogados: 4 de 10 encuestados equivalente al 40**%,** indica como medida preventiva a la Geolocalización de las personas a través de dispositivos o tecnologías, producida dentro del Fraude Informático de la ley 30096 para que no genere excesivas pérdidas económicas dentro del comercio electrónico.

Servidores Públicos: 3 de 10 encuestados equivalente al 30**%,** indica como medida preventiva Implementar Arquitecturas a las técnicas de pago suscitada dentro del Fraude

Informático de la ley 30096 para que no genere excesivas pérdidas económicas dentro del comercio electrónico.

TABLA 8 : Deficiencias de la Ley N° 30096

JUECES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	3	15%		
b)	12	60%		
c)	-	-		
d)	5	25%		
e)	-	-		
			20	12

Fuente: Encuestas aplicadas a Jueces de la Sede principal de Chiclayo.

TABLA 8: Deficiencias de la Ley N°30096

FISCALES				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	4	40%		
b)	5	50%		
c)	1	10%		
d)	-	-		
e)	-	-		
			10	5

Fuente: Encuestas aplicadas a Fiscales del Ministerio Público de Chiclayo.

TABLA 8: Deficiencias de la Ley N° 30096

ABOGADOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	-	-		
b)	5	50%		
c)	-	-		
d)	3	30%		
e)	2	20%		
			10	5

Fuente: Encuestas aplicadas a Abogados especializados en Derecho Penal y Comercial.

TABLA 8: Deficiencias de la Ley 30096

SERVIDORES PUBLICOS				
ALTERNATIVAS	**N° RESPUESTAS**	**%**	**N° ENCUESTADOS**	**TOTAL**
a)	3	30%		
b)	3	30%		
c)	-	-		
d)	-	-		
e)	4	40%		
			10	3

Fuente: Encuestas aplicadas a Servidores Públicos de Chiclayo.

Descripción:

De acuerdo a los datos obtenidos se puede establecer que, de un total de 50 personas que corresponde al 100%, señalaron que:

Fiscales: 5 de 10 encuestados equivalente al 50%, considera a la inexistencia de desarrolladores que permitan brindar una mejor seguridad las plataformas de comercio electrónico., como deficiencia normativa de la Ley 30096, respecto de brindar seguridad ante el fraude en el comercio electrónico.

Jueces: 12 de 20 encuestados equivalente al 60%, considera a la inexistencia de desarrolladores que permitan brindar una mejor seguridad las plataformas de comercio electrónico., como deficiencia normativa de la Ley 30096, respecto de brindar seguridad ante el fraude en el comercio electrónico.

Servidores Públicos: 3 de 10 encuestados equivalente al 30**%,** considera al desconocimiento, como deficiencia normativa de la Ley 30096, respecto de brindar seguridad ante el fraude en el comercio electrónico.

Abogados: 5 de 10 encuestados equivalente al 50%**,** considera a la inexistencia de desarrolladores que permitan brindar una mejor seguridad las plataformas de comercio electrónico., como deficiencia normativa de la Ley 30096, respecto de brindar seguridad ante el fraude en el comercio electrónico.

V. DISCUSIÓN

5.1. Discusión de resultados

5.1.1. Primera Discusión

Proponer el bloqueo del IP dinámico dentro de los comercios electrónicos como medida de prevención frente a los delitos informáticos en la ley 30096, acarrea en la posibilidad jurídica de que se tiene que desarrollar un sistema de Geolocalización de las partes que interactúan dentro del comercio electrónico en sus distintas modalidades, previendo su posibilidad jurídica en una propuesta de creación de un soporte informático que establezca un usuario único exponiendo a la IP estática como suscripción de cada consumidor creado con sus datos pertinentes en una plataforma que tenga como subyugación principal que su ingreso sea registrado con una IP estática, bloqueándose en parámetros adecuados las IP dinámica, para que en caso de incumplimiento la cuenta quede bloqueada restringiéndose los movimientos bancarios o saldos que se tengan dentro de la cuenta, hasta que se logre cumplir con la obligación impaga y asegurar las transacciones electrónicas.

Análogo a lo que refiere Méndez (2014) *Análisis, Diseño E Implementación De Una Plataforma Web Basada En Un Esquema C2c Para La Gestión De Entrega De Servicios Generales* El estudio realizado por el ingeniero en informática basa su investigación en la creación de una plataforma que tenga como vínculo entre las partes que configuran el comercio electrónico que son: el proveedor; el cual mediante este soporte informático permitirá que puedan ser localizados y contactados por sus clientes, es por ello que al ejecutarse, está tendrá un desarrollo eficaz, es por ello que funcionalidad el servicio de suministrar insumos requeridos por los proveedores a las tiendas, tenga como objetivo el uso de este soporte informático creado, es por esto que para lograr todo esto, ha llevado a cabo en su proyecto, la necesidad de crear un modelo de negocio de forma novedosa, el cual se enfocara en los requerimientos de cada una de las partes.

El análisis respecto a este se tema se basa a lo que Halaweh y Fidler (2008) describen en su investigación, lo que se ha propuesto en la presente investigación como base teórica acorde a la Percepción de Seguridad en Comercio electrónico: acarreado al Conflicto entre el Cliente y su organización de perspectivas respecto al comercio electrónico, basando su complejidad en el hecho de la autenticidad y la suplantación de la identidad, dando como resultado a lo investigado como una acepción de seguridad el hecho de tener geolocalizada a través del IP a una de las partes para que se someta a cumplir de manera segura la transacción electrónica.

5.1.2. Segunda Discusión

Describir la figura del bloqueo del IP dinámico dentro del comercio electrónico como medida preventiva ante los posibles delitos informáticos, va orientado al desarrollo de plataformas web, que adapten los soportes informáticos a datar la autenticación de las partes que emprenden un comercio electrónico, para que estos tengan una seguridad en las transacciones, se tiene que clasificar y explicar los delitos que se suscitan en el comercio electrónico pero que no se explaya en la normativa, acoplando el delito de fraude informático, sin clasificar dentro de ellos los suscitados en el comercio electrónico. Seguridad en las transacciones del E-Commerce -Fraude en los E- commerce (Impago, phishing, hackers y otros). Teniendo como medida de prevención el bloqueo del IP dinámico frente a los delitos informáticos, a través de dispositivos o tecnologías, producida dentro del Fraude Informático de la ley 30096 para que no genere excesivas pérdidas económicas dentro del comercio electrónico.

La discusión respecto lo que se ejecutó en la investigación con lleva a la teoría propuesta por Neelamadhab y Panigrahi (2016) "*Security Issues over E-Commerce and their Solutions"* el de dar una gestión esencial y que tenga como requisito técnico para cualquier actividad de transacción de pago, que disponga ser eficientes y eficaces a los comercios electrónicos ejecutados través de Internet. Debido al cambio tecnológico y empresarial constante y requiere un partido coordinado de algoritmos y soluciones técnicas. Por lo discutido en el marco de una visión general de seguridad para el comercio electrónico, disponer de los pasos para realizar un

pedido, el propósito de seguridad en el comercio electrónico, los problemas de seguridad en el comercio electrónico, las directrices para la compra segura en línea.

Siendo un tema amplio la seguridad recae en el tema de la privacidad y seguridad, situaciones que no pueden correlacionarse mediante la reseña de la autentificación y el despojo de la privacidad referente al caso de incumplir la obligación, por cuanto se asegura la transacción electrónica mediante la ubicación de las partes y sujetándolas a marcos de derechos y obligaciones que no pueden ser evadidas. Palak y Akshat (2016) *E-Commerce-Study of Pryvacy, Trust and Security from consumer's Perspective*

5.1.3. Tercera Discusión

Identificar los alcances que tendría el bloqueo del IP como medida de prevención ante los delitos informáticos en las plataformas web que están adaptadas al sistema VPN para el E-commerce, para dar freno al Fraude en los E-commerce (Impago, phishing, hackers y otros). Reforzaría la Ley N°30096 en los casos de delitos informáticos en su modalidad de fraude en el comercio electrónico. Considera a la inexistencia de desarrolladores que permitan brindar una mejor seguridad las plataformas de comercio electrónico, como deficiencia normativa de la Ley 30096 la cual no específica la ejecución de, respecto de brindar seguridad ante el fraude en el comercio electrónico.

Denotando los resultados propuestos, se considera pertinente decir que para brindar una mejor seguridad en las plataformas de comercio electrónico es en la de desarrollar un sistema que permita acceder al bloqueo de las IP dinámicas, para establecer un soporte informático que permita generar prevención ante los delitos de fraude electrónico que es una de las deficiencias en la normatividad de la Ley 30096 el no definir, especificar y detallar el delito de fraude informático y las diversas modalidades de suplantación de identidad dentro de los aspectos tecnológicos, el cual no cubre el aspecto del desarrollo del comercio electrónico en los parámetros pertinentes.

De acuerdo con lo expresado por Barrera (2014). En la Determinación los delitos de estafa informática según la Ley 67 de Comercio Electrónico en la Legislación

Ecuatoriana. En la actualidad con la creación de la denominada “autopista dela información”, el internet, las posibilidades de comunicación e investigación se han acrecentado, se tiene acceso aún ilimitado número de fuentes de consulta y entretenimiento. No existe una legislación adecuada que pueda contener el avance de esta clase de ilícitos, primero por una inadecuada y obsoleta normativa y, posteriormente por un procedimiento penal que si bien se ha modernizado, aún inadmiten los medios de prueba tecnológicos que se precisa en esta clase de delitos que no conocen fronteras, ya que el delito informático no se ajusta solo al país, pudiendo detectarse, como se analizará en el transcurso de la investigación, como se viola las seguridades de las cuentas bancarias desde el extranjero. Debido a que existe una legislación adecuada en el Ecuador se siguen cometiendo a nivel particular e institucional de los delitos informáticos aprovechándose de que las instituciones informáticas no dan seguridad personal e institucional para el buen uso de estas identificando la esencia del problema es que puede tratarse el tema de delitos informáticos en el comercio electrónico partiendo desde su prevención, desarrollo del comercio electrónico, soportes informáticos para generar a cabo el desarrollo de este ámbito de comercialización de bienes y servicios a través de internet, resguardando los parámetros de seguridad para su ejecución, posterior a esto viene la etapa de que aun habiendo existencia de todos estos procedimientos anteriores, sigue habiendo vulneración, he aquí las deficiencias de las medidas de seguridad tomadas por la Ley 30096.

Identificar los alcances que tendría el bloqueo del IP como medida de prevención ante los delitos informáticos en las plataformas web que están adaptadas al sistema VPN para el E-commerce, para dar freno al Fraude en los E- commerce (Impago, phishing, hackers y otros). Reforzaría la Ley N°30096 en los casos de delitos informáticos en su modalidad de fraude en el comercio electrónico. Considera a la inexistencia de desarrolladores que permitan brindar una mejor seguridad las plataformas de comercio electrónico, como deficiencia normativa de la Ley 30096 la cual no específica la ejecución de, respecto de brindar seguridad ante el fraude en el comercio electrónico.

Denotando los resultados propuestos, se considera pertinente decir que para brindar una mejor seguridad en las plataformas de comercio electrónico es en la de desarrollar un sistema que permita acceder al bloqueo de las IP dinámicas, para establecer un soporte informático que permita generar prevención ante los delitos de fraude electrónico que es una de las deficiencias en la normatividad de la Ley 30096 el no definir, especificar y detallar el delito de fraude informático y las diversas modalidades de suplantación de identidad dentro de los aspectos tecnológicos, el cual no cubre el aspecto del desarrollo del comercio electrónico en los parámetros pertinentes.

De acuerdo con lo expresado por Barrera (2014). En la Determinación los delitos de estafa informática según la Ley 67 de Comercio Electrónico en la Legislación Ecuatoriana. En la actualidad con la creación de la denominada “autopista dela información”, el internet, las posibilidades de comunicación e investigación se han acrecentado, se tiene acceso aún ilimitado número de fuentes de consulta y entretenimiento. No existe una legislación adecuada que pueda contener el avance de esta clase de ilícitos, primero por una inadecuada y obsoleta normativa y, posteriormente por un procedimiento penal que si bien se ha modernizado, aún inadmiten los medios de prueba tecnológicos que se precisa en esta clase de delitos que no conocen fronteras, ya que el delito informático no se ajusta solo al país, pudiendo detectarse, como se analizará en el transcurso de la investigación, como se viola las seguridades de las cuentas bancarias desde el extranjero. Debido a que existe una legislación adecuada en el Ecuador se siguen cometiendo a nivel particular e institucional de los delitos informáticos aprovechándose de que las instituciones informáticas no dan seguridad personal e institucional para el buen

uso de estas. Identificando la esencia del problema es que puede tratarse el tema de delitos informáticos en el comercio electrónico partiendo desde su prevención, desarrollo del comercio electrónico, soportes informáticos para generar a cabo el desarrollo de este ámbito de comercialización de bienes y servicios a través de internet, resguardando los parámetros de seguridad para su ejecución, posterior a esto viene la etapa de que aun habiendo existencia de todos estos procedimientos anteriores, sigue habiendo vulneración, he aquí las deficiencias de las medidas de seguridad tomadas por la Ley 30096.

5.4.1 Cuarta discusión

Plantear el bloqueo del IP dinámico dentro de los soportes informáticos será una medida de seguridad que prevenga los delitos informáticos, es medida de prevención de los delitos de fraude informáticos de la Ley 30096, plataformas web de adaptadas al sistema VPN para el *E-commerce*, seguridad en las transacciones del E-Commerce. La medida preventiva que se suscita dentro del Fraude Informático de la ley 30096 para que no genere excesivas pérdidas económicas dentro del comercio electrónico, siendo medida preventiva a la Geolocalización de las personas a través de dispositivos o tecnologías.

El análisis de los resultados propuestos en la presentación denota similitudes por lo expresado en la propuesta Vorapranee (2003) Enchancing the Security of Electronic commerce transactions. Esta investigación evalúa la seguridad del proceso de transacciones en el comercio electrónico, detalla desde la terminología en la que se basa cada sistema de seguridad proporcionada dentro de un soporte informático, además de la descripción de los requisitos de seguridad para pagos con tarjeta a través de internet, y los posibles protocolos para el procesamiento de transacciones electrónicas, a la actualidad el protocolo Secure Socket layer(SSL) junto con su protocolo estandarizado o genérico TLS (Transport Layer Security) son los medios más utilizados para brindar soportes a las transacciones electrónicas realizadas a través de Internet. Por lo tanto, el análisis y las discusiones que se han integrado en esta investigación basan su teoría en el supuesto de que estos protocolos proporcionan un nivel “Base” de seguridad, contra el cual deben

proporcionarse nuevas medidas de seguridad poniéndose a escalas de medición en su nivel de seguridad, los protocolos SSL Y TLS se analizan de acuerdo a lo bien que satisfacen los requisitos de seguridad que se han de describir, a su vez la proporción del transporte en el que se generan las transacciones de seguridad electrónicas tienen capas de seguridad y algunos de los requisitos de seguridad están en aplicación del nivel, no es sorpresa que no aborden todas las cuestión de requisitos de seguridad, por lo tanto en esta investigación la propuesta el resultado a la investigación es dar a conocer cuatro protocolos que se pueden utilizar para construir sobre las características de seguridad proporcionadas por SSL/TLS, para lo cual su objetivo principal es diseñar sistemas que mejores la seguridad del procesamiento electrónico, de esta forma se imponen gastos 1mínimos a las partes involucradas. En el primer protocolo se proponen utilizar una tarjeta EMV para mejorar la seguridad de transacciones en línea, el segundo protocolo; implica el uso del abonado de la Autenticación en GSM, para proporcionarse una autenticación del usuario a través de internet. En tercer lugar, el investigador propuso el uso del servicio de confidencialidad de datos GSM para proteger, así como garantizar la autenticación del usuario; independientemente del régimen de protección empleado para las transacciones. Por ende, existen tantas amenazas a todos los ordenadores (PCs). Utilizados para realizar transacciones de comercio electrónico, pero estos protocolos examen las amenazas residuales y motivan el diseño el cuarto protocolo, que específicamente está hecho para hacer frente a las amenazas de cookies.

VI. CONCLUSIONES

5.1. Que de conforme a lo planteado se asegurara la transacción electrónica a través del bloqueo de la IP dentro del comercio electrónico por cuanto la autenticación a través de un usuario único y el ingreso de interconexión de una IP estática es la forma más eficiente para restringir el acceso a hackers o atentados contra las transacciones de comercio electrónicas ejecutadas en el C2C,

5.2. Que de conforme a lo investigado se identificó que a través de los resultados, el bloqueo del IP dinámico dentro del soporte informático será una medida de seguridad que prevenga los delitos informáticos, 20 jueces en un 65% que tienen seguridad de que la propuesta de esta investigación es viable

5.3. Lo dispuesto a identificarse se ha demostrado que el 60% de fiscales consideran que se debe efectuar una medida preventiva a través de la geolocalización de las partes y la suscripción de la ip a través de un sistema informático y jurídico, las cuales permiten una seguridad en el principio de la autenticidad y autentificación, asegurando así la transacción electrónica y la responsabilidad de quien incumpla la obligación, teniendo en cuenta el bloqueo del ip.

5.4 Se logró plantear un método informático que cumple con el objetivo específico la averiguación de la dirección IP estática ha de considerarse como dato de suscripción, mientras que si fuera dinámica está no aporta datos del usuario de modo que perjudicaría el principio de autenticidad, es por ello que se dio la figura del bloqueo del IP dinámico dentro del comercio Electrónico como medida de prevención ante los delitos informáticos de la ley 30096.

VII. RECOMENDACIONES

- Debe haber una contribución interdisciplinaria entre el Derecho y la Ingeniería de software para el diseño de diseño del mecanismo contra el delito informático, como podría ser el bloqueo del IP dinámico dentro de un servidor privado, que permita la suscripción de la IP estática y la posible geolocalización de las partes como forma de proponer, protocolos de seguridad, que permitan verificar las identidades de los clientes y comerciantes en la medida necesaria para permitir comercio electrónico seguro. Pero las soluciones son más que un reto técnico, son también una lucha política de alto nivel.
- Adherirse al Convenio de Budapest Hungría, los delitos informáticos no pueden ser manejados de forma aislada es una contribución internacional, acorde a la globalización y la interconexión masiva de personas por la tanto debe de haber uniformidad legislativa para poder combatir los problemas de Responsabilidad Contractual, Sanciones Penales y Seguridad Electrónica.

- El implemento de áreas especializadas y capacitadas en delitos informáticos, desarrollo de Políticas normativas que puedan interpretar la informática jurídica de forma eficiente y una contribución en el desarrollo de mecanismos que brinden seguridad jurídica.

- Las proposiciones en el marco de seguridad de información y transacción electrónica lejos de pasar por el cumplimiento del marco regulatorio**,** recae en la necesidad de que haya una interpretación uniforme de la diversidad de delitos informáticos y la ejecución o desarrollo de estos, habiendo una clasificación de delitos y su configuración o accionar delictual es que se puede configurar un mejor arquetipo de criminalidad informática. Además, precisó que son necesarios el monitoreo en tiempo real y la realización de inteligencia preventiva de riesgos cibernéticos.

VIII. REFERENCIAS

Cañedo (2004) “Una aproximación para la Historia del Internet”

Arata (2002) “Las Nuevas Tecnologías de la Información y la Problemática Jurídica del Comercio Electrónico”

Armas (2002) “Sistema de Contratación por Medios Electrónicos: Manifestación de voluntad y perfeccionamiento contractual”

Méndez (2014) “Análisis, Diseño E Implementación De Una Plataforma Web Basada En Un Esquema C2c Para La Gestión De Entrega De Servicios Generales”

Vorapranee (2003) “Enchancing the Security of Electronic commerce transactions” epartment of Mathematics Royal Holloway, University of London Egham, Surrey TW20 0EX, England. Recuperado de https://www.researchgate.net/publication/ DOI: 48602656_Enhancing_the_security_of_electronic_commerce_transactions

Niranjanamurthy y Dharmendra (2013) “The study of E-Commerce Security Issues and Solutions”

Dilané y Mantas (2005) “Incidencia de los Acuerdos y los Tratados Internacionales en la Aplicación de la Ley 126-02 de Comercio Electrónico en la República Dominicana”

Celenia y Yaneris, (2012) “Incidencias de las leyes fiscales en el Comercio Electrónico de la República Dominicana (2008-2010)”

Fernández, Pujols, Mata y Pérez (1999) “Seguridad en Redes de Internet-Caso de Estudio El Comercio Electrónico”

Barrera (2014). “Determinar los delitos de estafa informática según la Ley 67 de Comercio Electrónico en la Legislación Ecuatoriana”

García (2004). “Seguridad en el Comercio Electrónico”

Romero (2003). “Seguridad en redes y Protocolos Asociados”

Corletti (2011) “Seguridad por niveles” Recuperado de DOI: http://darfe.es/joomla/index.php/descargas/viewdownload/5-seguridad/ DOI:1310-seguridad-en-redes

Monsalve, Aponte y Chaparro Becerra (2014) “Análisis de seguridad de una muestra de redes WLAN en la Ciudad de Tunja Boyacá”

Mamani (2012) “Protocolos de Comunicación Utilizados en Cloud Computing”

Adamu (2015) “Concern for e-Commerce Security”

Mohaned y Cristhine (2008). “Security Perception in E-commerce: Conflict between Customer and Organizational Perspectives”

Raghav (2014) “Network Security Issues in e Commerce”

Palak y Akshat (2016) “E-Commerce-Study of Pryvacy, Trust and Security from consumer’s Perspective” (p. 224-232)

PECOY (2011) “Delito en el Comercio Electrónico” (p. 41-46)

Revathi, Shanthi y Saranya (2015) “A Study on E- Commerce Security Issues”

Joo, Ki y Sung, (2005) *Method for electronic commerce using security token and apparatus thereof*

Prasad, Neelamadhab y Panigrahi (2016) *Security Issues over E-Commerce and their Solutions*

Halaweh y Fidler (2008) *Percepción de Seguridad en Comercio electrónico: Conflicto entre el Cliente y organizacional Perspectivas. Actas de la multiconferencia Internacional sobre Ciencias de la Computación y Tecnología de la Información*, (p 443 -. 449)

Yuanqiao y Chunhui (2008) *Investigación Sobre Cuestiones de Seguridad en el Comercio Electrónico*. Seminario Internacional de Negocios e Información Administración.

Lazaro (2007) *“Medios técnicos en la investigación de los delitos informáticos”.* Especial referencia a la tecnovigilancia, Consejo General del Poder Judicial, Madrid.

IX. ANEXOS

ANEXO N° 01: ENCUESTA

UNIVERSIDAD SEÑOR DE SIPÁN

CUESTIONARIO N° 01

DIRIGIDO A LOS JUECES PENALES, FISCALES, AUXILIARES JUDICIALES, ABOGADO.

Este cuestionario es parte de un estudio acerca de **BLOQUEO DEL IP DINÁMICO DENTRO DEL COMERCIO ELETRONICO COMO MEDIDA DE PREVENCIÓN EN LOS DELITOS INFORMATICOS DE LA LEY 30096** para la realización de una muestra sobre la problemática de este proyecto de investigación. Entiéndase por esto a una modalidad de seguridad en los comercios electrónicos: respecto al pago y el fraude a través transferencias de dinero. El Objetivo principal de este estudio es analizar las compras online para determinar los factores que influyen estos delitos. La encuesta es anónima y responder no le tomará más allá de 10 minutos. Agracemos su colaboración, ya que conocer su opinión es un aporte valioso para este estudio**.**

I.GENERALIDADES.

1. OCUPACION

Juez (___) Secretario Público ( ) Fiscal (____) Abogados (___)

2. EDAD : _____ SEXO: _____ TIEMPO DE SERVICIO: _____

3. **¿CON QUÉ FRECUENCIA UTILIZA INTERNET? MARQUE CON UNA X SOLO UNA RESPUESTA**.

a) Entre 0 y 1 hora diaria

b) Entre 1 y 2 horas diarias

c) Entre 2 y 3 horas diarias

d) Entre 3 y 4 horas diarias

e) Entre 4 y 5 horas diarias

f) Más de 5 horas diarias

II. RESPONSABLES

4. De los siguientes conceptos que se consideran básicos, marque con una (x) todos los que Usted como Conocedor, considera lo que es un comercio electrónico.

a. Compra- Venta a través de Internet. - Servicios de adquirir productos, bienes o servicios a través de las distintas modalidades de B2B, B2C Y C2C. **( )**

b. Transacciones Electrónicas. - pagos a través de internet mediante tarjeta de crédito **( )**

c. Negociar en Plataformas Web. - comprar en plataformas como Amazon, Ebay, plataformas de chat online, Alibaba. **( )**

d. Infraestructura de interfaces. - está asentado en bases de datos, agenda de clientes y aplicaciones, y sus interrelaciones. ( )

5. Marque las alternativas que usted crea conveniente de acuerdo con la pregunta que se leerá a continuación ¿La geolocalización de una las partes a través de la IP (que permitiría ubicar a una de las partes) aseguraría la transacción de comercio electrónico?

a. La seguridad más eficiente brindar un sistema de plataforma que permita el bloqueo de la dirección de IP para el comercio electrónico para asegurar el pago y la prestación el servicio ( )

b. Considera otros medios para garantizar la seguridad en el comercio electrónico. ( )

6. ¿Conoce Ud., sobre el bloqueo del IP dinámico dentro del comercio electrónico como medida de prevención frente a los delitos informáticos?

a. Si

b. No

c. No opina

7. De las siguientes alternativas; marque con una (x) la razón o causa por la que Usted crea que la tarjeta de crédito es el medio de pago, al cual más seguridad debe brindársele en los casos de comercio electrónico para evitar el fraude electrónico.

a. La gran mayoría de personas posee tarjetas de crédito la cual les permite realizar un pago instantáneo. ( )

b. No se necesita ningún conocimiento técnico para su utilización, pero si un mayor apoyo para las transacciones impago ( )

c. Existe una amplia regulación proteccionista al propietario de la tarjeta de crédito mas no al desarrollo al comercio electrónico y los parámetros de seguridad en los negocios de consumidor a consumidor ( )

d. Los fraudes a veces residen no por la inseguridad del soporte informático sino por el desarrollo del comercio electrónico y el ambiente impropio del C2C ( )

e. El riesgo por utilización de la tarjeta de crédito de forma fraudulenta recae en el vendedor ()

8. **Marque la opción que crea oportuna para el reforzamiento de la Ley N° 30096 en los casos de delitos informáticos en su modalidad de fraude en el comercio electrónico.**

   a. **Conciencia de Seguridad. -** Los riesgos en el envío de datos privados a través de internet que ocasionan el acceso a transacciones electrónicas (**)**
   b. **Mejor desarrollo de Seguridad en el Comercio Electrónico. –** El desarrollo de seguridad orientada a ser una parte integral de la arquitectura, el diseño y la implementación que cubra todas las ramas de seguridad. **( )**
   c. **Responsabilidad. -** Los pagos a través de Internet son ejercidas como transacciones de venta por internet, lo que significa que él consumidor no se hace responsable en absoluto y todo riesgo es con el comerciante, lo cual no debería ser. **( )**
   d. **Brindar políticas de mejor desarrollo del Comercio Electrónico. -** Para prevenir la estafa informática con componentes técnicos de seguridad**,** se usan cuatro componentes que intervienen en el comercio electrónico de seguridad software de cliente, software de servidor, el sistema operativo del servidor, y el transporte de red. ( )

9. **Marca una (X) cuál de los tipos de Fraude Informático de las cuales usted haya tenido conocimiento.**
   a. **Robo de Identidad. -** El hecho de que un sujeto se haga pasar por otra persona accediendo a datos de otro para poder obtener una negociación virtual. **( )**
   b. **Phishing. -** Un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. **( )**
   c. **Pharming.-** Constituye otra forma de fraude en línea, muy similar a su pariente, el phishing. Los pharmers, utilizan los mismos sitios Web falsos y el robo de información confidencial para perpetrar estafas en línea **( )**
   d. **Transacciones Impago. -** Modalidad en la que se ejecuta un comercio electrónico, sin ejecutar el pago o haciendo fraude en la cancelación. **( )**
   e. **Scam.-** El timo o estafa, que uno o varios individuos entregan una cantidad de dinero al estafador o "Scamer" con la promesa de recibir a cambio un beneficio generalmente económico **( )**

10. **¿Para Ud., cuál sería la medida preventiva que se suscita dentro del Fraude Informático de la ley 30096 para que no genere excesivas pérdidas económicas dentro del comercio electrónico?**

    a. **Implementación de una normativa frente al comercio electrónico** ( )
    b. **Geolocalización de las personas a través de dispositivos o tecnologías. -** Tecnologías (teléfonos móviles con infrarrojos, Wi-Fi, Bluetooth o GPS, IP) que permita tener la ubicación de las partes que permitan dar confianza al usuario final. ( )
    c. **Hacer uso de Patentes de dominio público en soportes informáticos. -** Sistemas de seguridad que tienen patente de dominio público en comercio electrónico de las cuales el Perú no ha solicitado ninguna para brindar medida de seguridad más efectivas ( )
    d. **Implementar Arquitecturas a las técnicas de pago.** ( )

11. **Marque Usted con una (X) ¿Cuál cree Usted que es la deficiencia de la Ley 30096 en brindar seguridad ante el fraude en el comercio electrónico?**

a. Falta de capacitación ( )
b. No hay desarrolladores que permitan brindar una mejor seguridad las plataformas de comercio electrónico. ( )
c. No esta de acuerdo con las políticas de transferencia de pago ( )
d. No hay normativa respecto al Comercio Electrónico ( )
e. Desconocimiento ( )

"AGRADECEMOS SU AMABLE COLABORACIÓN".