UNIVERSIDAD PRIVADA DE TRUJILLO

FACULTAD DE DERECHO

CARRERA PROFESIONAL DE DERECHO

TESIS PARA OPTAR EL TITULO PROFESIONAL DE ABOGADO

“MEDIDAS DE PROTECCIÓN INFORMATICA Y SU EFICACIA EN LA PREVENCION DEL DELITO DE SUPLANTACION DE IDENTIDAD CIBERNETICA EN LA CIUDAD DE TRUJILLO, 2020”

BACHILLERES:

Juan Carlos Caycho Pinchi

Dante Evelio Saguma Rivera

ASESOR:

Mg. Carlos Jesús Alza Collantes

Trujillo - Perú

2021

HOJA DE FIRMAS

PRESIDENTE

SECRETARIO

VOCAL

DEDICATORIA:

Dedico este trabajo a mis hijos, por ser el motor más fiel y confiable que me impulsan a culminar mi carrera. De igual manera, a una persona muy especial por su comprensión y apoyo.

AGRADECIMIENTO

Agradezco a Dios, a mis hijos, madre y hermanos por ser los principales forjadores de mi desarrollo como persona y como profesional. Así como a todas aquellas personas que de una u otra forma han colaborado conmigo, para la realización del presente trabajo.

INDICE DE CONTENIDOS

RESUMEN

La presente investigación tiene como objetivo estudiar el Derecho Informático y las medidas de protección informática que ayudan a prevenir la comisión del Delito de Suplantación de Identidad Cibernética, en la ciudad de Trujillo durante el año 2020. Se analiza como corresponde, la Ley N° 30096 – Ley de Delitos Informáticos, a fin de determinar si esta ha cumplido la finalidad preventiva que le asigna el artículo 1° de su propio texto al declarar "*La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia".* Si bien la aludida norma prevé diferentes mecanismos de participación y colaboración interinstitucional que propenden asegurar el tratamiento del delito informático (agente encubierto, coordinación interinstitucional, cooperación operativa, entre otros), la presente investigación enfatiza el análisis respecto de las Medidas de Seguridad que la Oficina Nacional de Gobierno Electrónico e Informático (ONGEI) en coordinación con instituciones del sector público y otras del sector privado, han creado y puesto al alcance de la población, con la finalidad de limitar el actuar delictivo de quienes se predisponen a afectar con su actuar, los datos personales sensibles y la integridad de los sistemas informáticos que las contienen.

ABSTRAC

The present research aims to study Computer Law and computer protection measures that help prevent the commission of the Crime of Cyber Identity Impersonation, in the city of Trujillo during the year 2020. Law No. 30096 is analyzed accordingly - Computer Crimes Law, in order to determine if it has fulfilled the preventive purpose assigned to it by article 1 of its own text by stating “The present Law is intended to prevent and punish illicit behaviors that affect computer systems and data and other legal assets of criminal relevance, committed through the use of information or communication technologies, in order to guarantee the effective fight against cybercrime ". Although the aforementioned norm provides for different mechanisms of participation and inter-institutional collaboration that tend to ensure the treatment of computer crime (undercover agent, inter-institutional coordination, operational cooperation, among others), this research emphasizes the analysis regarding the Security Measures that the Office National Electronic Government and Information Technology (ONGEI) in coordination with institutions of the public sector and others of the private sector, have created and made available to the population, in order to limit the criminal act of those who are predisposed to affect with their actions, sensitive personal data and the integrity of the computer systems that contain them.

CAPITULO I

INTRODUCCION

1.1 REALIDAD PROBLEMÁTICA

En el Perú existe un gran desconocimiento por parte de un sector de la población, respecto de las consecuencias que conlleva la pérdida de los documentos privados (DNI, tarjetas de crédito, licencia de conducir, etc.) y el uso ilícito de los mismos, pues por esta situación, se puede ser denunciado y hasta declarado (reo contumaz) porque otra persona usurpó su identidad.

En la casuística peruana concurre una variedad de casos, según los cuales, diferentes personas fueron sindicadas por un delito que nunca llegaron a cometer y que, por tan solo una muestra de la ficha RENIEC son denunciados por algún tipo de delito que no perpetraron. También se han visto casos en los cuales la Policía Nacional, con solo una muestra de la Ficha C-4 o ficha RENIEC, logran identificar a la supuesta persona que incurrió en el delito.

Según el Boletín de Estadísticas de Seguridad Ciudadana en el período de noviembre del 2018 – abril 2019 emitido por el Instituto Nacional de Estadística e Informática (INEI), en una tasa por cada 100 habitantes de 15 a más años edad, muestra que el 26,0% han sido víctimas de algún hecho delictivo sobre hurto o robo de sus documentos; de éstos, el 13,4 han sido víctimas de robo, sin embargo, lo más alarmante es que en el trabajo de campo efectuado sobre los “motivos de la no denuncia”, la causa que encabeza esta lista la conforman el 32,4% que manifestó que es “una pérdida de tiempo”, siguiéndole el 24,4% quien dijo “desconocer al delincuente” y un no menos importante 16,1% que consideró tal hecho como un “delito de poca importancia”, quizá porque aún no se aprende a dar el valor que tienen ciertos documentos.

Hay que tener en cuenta que, el robo de pertenencias, dentro de ellas los documentos privados, es una de las causantes de la usurpación de identidad, ya que, mediante la comisión de este

delito es que se obtiene diferentes documentos y como consecuencia de ello, se utilizan para incurrir en otros tipos de delitos haciendo uso de la identidad del dueño de las documentaciones.

Por lo tanto, las personas que han sido víctimas de hurto, robo o extraviado sus documentos personales y han caído en el descuido de no denunciar el hecho ante las autoridades competentes, en un futuro podrían verse afectadas cuando por algún motivo, decidan tramitar su certificado de antecedentes policiales, pues, se darán con la sorpresiva noticia que se encuentran denunciados por un hecho que no cometieron y es allí, cuando por el descuido o desconocimiento, se vieron envueltos en un hecho de usurpación de identidad habiendo cometido supuestamente diferentes delitos.

Ahora, no solo la pérdida, robo o hurto de los documentos privados es una causal de la usurpación de identidad, sino que también la utilización de datos de otra persona a través de un medio tecnológico también es una causal de usurpación de la identidad.
En la actualidad vivimos una “Era tecnológica” que a la sociedad le ayuda en ciertas formas a que pueda evolucionar, pero consigo también trae una evolución y sofisticación en la comisión de diferentes tipos de delitos.

El uso de internet, dentro de ello, de las redes sociales, tiene un carácter imprescindible en la cotidianidad de los individuos, es por ello, que es necesario que nos lleguemos a identificar tanto en un contexto digital como en un contexto real. El uso que le damos a nuestra identidad personal en esta “Era tecnológica”, nos obliga a manifestarnos de una manera transparente, genuina y honesta como lo hacemos en la realidad.

Una modalidad de obtener datos es: Las diferentes páginas web falsas que crea la delincuencia para obtener datos privados de personas o los famosos “correos electrónicos” también falsos de entidades bancarias, a través de los cuales la cybercriminalidad solicita, la actualización de datos y la clave secreta de la cuenta bancaria. Pero no solo es la obtención de datos personales sino que también la delincuencia hace uso de nombres, ya sean de personas naturales o personas jurídicas, para poder cometer sus actos ilícitos, como por ejemplo, la creación de un perfil en una red social, ya sea *Facebook, Twitter, Instagram*, etc., para atentar contra la integridad moral de la víctima, siendo pernicioso para la persona en su vida familiar, personal y laboral, así como también perjudicando gravemente su honor, reputación y dignidad. Por otro lado, también harían uso de este método para la obtención económica de variados bienes y/o servicios tales como realizar préstamos bancarios u obtener créditos.

Los delitos contra la libertad también son perpetrados por estos personajes, ya sea en su tipo acoso, secuestro, trata de personas, etc. cometidos por medio del internet, las redes sociales; utilizando los datos personales de otra persona o empresa, para poder captar a las víctimas ya sea ofreciéndoles pasar un casting, oferta de trabajo, recoger el premio de algún sorteo, etc. logrando así su cometido de atraerlas con el fin de explotarlas sexualmente, explotarlos laboralmente o traficando sus órganos.

El Informe desarrollado en noviembre del 2018 por el Instituto Nacional de Estadística e Informática (INEI), en el período de 2011-2018 sobre las estadísticas de la Trata de Personas, indica que en el período enero – setiembre del 2018 hubo un total de 991 casos registrados, siendo las regiones más afectada Lima (227), Puno (88), Madre de Dios (71) y Arequipa (70). Siendo utilizada como una de las modalidades para cometer este delito, la captación por redes sociales.

Según Juan Manuel Moretti, mayor PNP de la División de Investigaciones de Delitos de Alta Tecnología **Divindat, (2016)**: "*Los delitos informáticos son iguales o más peligrosos aún que los delitos que se cometen en la calle, ya que los hampones se valen del anonimato. Las víctimas no pueden identificar a las personas que los están agrediendo".*

Finalmente, la suplantación de identidad por el medio digital es uno de los métodos que utilizan los delincuentes para perpetrar diferentes tipos de delitos y que puedan lograr su cometido, por otro lado, no poner en conocimiento la pérdida o robo de los documentos privados puede causar diferentes problemas legales y personales en un futuro.

1.2 FORMULACIÓN DEL PROBLEMA

¿Son eficaces las medidas de protección informáticas contra el delito de suplantación de identidad cibernética en la ciudad de Trujillo, año 2020?

1.3 JUSTIFICACIÓN

a) Justificación Teórica:

Nuestra investigación nos permitirá conocer las medidas de protección y de seguridad informática y su eficacia en la prevención del Delito de Suplantación de Identidad Informática, teniendo en cuenta el Derecho Penal Informático, mediante la interpretación de leyes penales sobre Delitos Informáticos, proponiendo un sistema orientador en la toma de decisiones para adoptar medidas de prevención a fin de minimizar la comisión del delito de suplantación de identidad cibernética.

b) Justificación Práctica:

Siendo la investigación no experimental - básica, el presente trabajo tiende a determinar si las medidas de protección y prevención de Delitos Informáticos son eficaces en la lucha contra el delito de Suplantación de Identidad Cibernética, a través de conocimientos orientados acerca de los delitos informáticos en sus diversas manifestaciones conforme al Derecho Penal. Se explican los fenómenos de tecnificación de la información, como medios de protección contra la Suplantación de la Identidad Cibernética.

c) Justificación Doctrinal:

La doctrina nacional ha desarrollado estudios sobre los Delitos Informáticos a través de las redes sociales, no obstante, resultó necesario investigar sobre los medios de protección y su eficacia en la prevención del delito de suplantación de identidad cibernética, con la finalidad de mejorar nuestro ordenamiento jurídico sobre el tema.

d) Justificación Social:

En el entorno social nacional llama la atención que a pesar de existir el artículo 9 de la Ley N° 30096, las personas no acuden a la justicia para entablar un proceso penal, por no encontrar en ésta una solución eficaz y digna. Los operadores de justicia no disponen del conocimiento adecuado de la tecnología informática que conlleve a una aplicación correcta de la norma sobre el Delito Informático. La justificación de la presente investigación radica además en que la comisión del Delito de Suplantación de Identidad Cibernética no solo afecta su identidad, sino también su patrimonio, intimidad, imagen; incluyendo puede afectar bienes colectivos y la seguridad jurídica.

1.4 OBJETIVOS

1.4.1 Objetivo General

Analizar las medidas de protección y su eficacia en la prevención del Delito de Suplantación de Identidad Cibernética en el distrito de Trujillo, año 2020.

1.4.2 Objetivos Específicos

1. Identificar cuáles son las Medidas de Protección Informática que se aplican actualmente para prevenir la comisión del Delito de Suplantación de identidad Cibernética.
2. Determinar la eficacia de las Medidas de Protección Informática que se aplican actualmente en la prevención del Delito de Suplantación de Identidad Cibernética.
3. Analizar la Influencia de las redes sociales de la Comisión del Delito de Suplantación de Identidad Cibernética.

1.5 ANTECEDENTES

Alcívar,C.(2016) investigó **"Los medios de comunicación y la estafa electrónica. Nueva forma de delito".** La estafa electrónica es un fenómeno delictuoso que ha tomado parte en las leyes de Ecuador debido al gran progreso mundial que existe actualmente, lo que ha hecho que tome suma importancia en la esfera de la delictuosidad informática, descrito como una novedosa modalidad de delito informático, abriendo camino a la "ciberdelincuencia". Pese a que no es fácil definirlo, pues está basado en diversas acepciones cibernéticas, en Madrid, el equipo de abogados de Portaley lo define como "*aquello que produce un perjuicio patrimonial contable a través de una conducta externa e inadecuada de un procedimiento computarizado informático, donde se gestiona la alteración de datos, con el fin de lucrar,*

ocasionando daño a un tercero" (Portaley). Esta especie de fraude se lleva a cabo al usar ordenadores, algún tipo de sistema informático, o cualquier dispositivo que sirva para comunicarse. Su finalidad es ocasionar daños, generar pérdidas o imposibilitar la utilización de información de terceros. Por lo que, ante este delito, cuyo autor suele ser anónimo, es necesario indagar y prescribir un castigo, para que de este modo se imparta justicia. El tema escogido es de suma importancia, en razón a que una gran cantidad de ecuatorianos han sido víctimas de dicha estafa y siguen siéndolo, pues desconocen sus derechos, así como el riesgo que sobrelleva. El objetivo general es examinar la legislación ecuatoriana, revisando algunos códigos existentes que traten sobre este delito de estafa electrónica. Así como definir los delitos informáticos, realizando las encuestas respectivas, para arribar a una conclusión en base a los resultados de la investigación **Alcívar, T. (2016).**

En el año 2014, se realizó el estudio titulado "**Un análisis de la naturaleza de los grupos involucrados en delitos cibernéticos".** Este documento explora la naturaleza de los grupos involucrados en el delito cibernético. Describe brevemente la definición y el alcance del delito cibernético, los retos teóricos y empíricos para abordar lo que se sabe acerca de los delincuentes cibernéticos y el papel probable de los grupos del crimen organizado. El documento da ejemplos de casos conocidos que ilustran el comportamiento individual y grupal y las motivaciones de los delincuentes típicos, incluyendo los actores estatales. Se describen diferentes tipos de ciberdelincuencia y diferentes formas de organización delictiva, basándose en la tipología sugerida por **McGuire, (2012)**. Es evidente que una gran variedad de estructuras organizativas está involucrada en el delito cibernético. Las actividades empresariales o con fines de lucro, y especialmente la ciberdelincuencia cometida por actores estatales, parecen requerir liderazgo, estructura y especialización. Por el contrario, la actividad de protesta tiende a ser menos organizada,

con una cadena de mando débil (si es que la hay). **Broadhurst, (2014).**

Dhillon,G. y Moores,S. (2015) investigaron "**Delitos informáticos: teorizar sobre el enemigo dentro".** La mayoría de los delitos informáticos ocurren porque un empleado actual de una organización ha subvertido los controles existentes. Al considerar dos estudios de caso, este trabajo analiza los crímenes informáticos resultantes de violaciones de las salvaguardias por parte de los empleados. El documento sugiere que se deben poner en marcha varios controles técnicos, de procedimiento y normativos para prevenir actos ilegales y maliciosos. En última instancia, un buen equilibrio entre varios tipos de controles ayudaría a instituir un medio rentable para hacer que la conducta accidental e intencional fuera difícil. Esto también garantizaría, siempre que fuera posible, la rendición de cuentas individual de todas las acciones negativas potencialmente sensibles.

Vinit,V.(2014) Realizo la investigación titulada **"Paradigmas actuales y futuros del delito cibernético y de la seguridad - Tendencias de crecimiento y aumento".** El crimen cibernético es todo aquello que se acerca a los crímenes involucrados con el medio ambiente donde siempre está involucrada una red y los pasos implementados para controlar o superar esta ciber seguridad. La cultura de trabajo de todos los sectores está avanzando hacia la digitalización y los sistemas basados en la nube con el fin de aumentar la eficiencia del trabajo con mayor precisión. Además de esto, la mayoría de las personas les gusta usar sitios de redes sociales y servidores de correo electrónico de muchas maneras directa o indirectamente. El delito cibernético es un tipo de delito en el que se requiere de conocimientos técnicos no sólo para romperlo, sino para hacer un usuario seguro o para aplicar cualquier especialidad preventiva. En este artículo hemos descrito acerca de los fundamentos de este terrible crimen, la

reciente investigación y desarrollo en el ámbito de la seguridad cibernética, los tipos de crímenes y una pequeña encuesta con una empresa de TI. Nuestro objetivo con esta investigación es comprobar el nivel de conciencia de los delincuentes cibernéticos y de seguridad y sugerir pasos necesarios que realmente pueden ser útiles para hacer que el entorno cibernético sea seguro, robusto y digno de confianza. **Kumar, (2014).**

Carter, D. (2000) Investigo **"Cómo funcionan los criminales tecnológicos".** Si bien hay cuatro tipos principales de delitos informáticos, múltiples delitos pueden ocurrir durante cualquier transacción penal. Los crímenes en los que el equipo es el objetivo incluyen el robo de la propiedad intelectual o la información de marketing, el chantaje o el sabotaje de los sistemas operativos y programas. En todos estos crímenes, el delincuente usa la computadora para obtener información o para dañar los programas operativos. En el segundo tipo de delito, los procesos de la computadora, es decir, su instrumentalidad, más que el contenido de los archivos reales, se utiliza para cometer el crimen. Los delitos en esta categoría incluyen el uso fraudulento de cajeros automáticos, fraude de tarjetas de crédito y fraude de telecomunicaciones. En otro tipo de delito informático, la computadora no es esencial para que ocurra el delito, sino que está relacionada con el acto criminal. Por ejemplo, los infractores de drogas pueden usar computadoras para registrar información sobre su lavado de dinero, tráfico y otras actividades ilegales. La cuarta categoría incluye los delitos recientemente inventados relacionados con la proliferación de computadoras, como la piratería de software, el mercadeo negro y el robo de equipos informáticos. Algunos problemas únicos relacionados con la delincuencia informática se refieren a cuestiones de propiedad intelectual, el concepto de malversación por computadora y las cuestiones internacionales.

A nivel nacional tenemos los datos **Temperini, M**. en su estudio titulado **"Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte"**. De los diversos estudios realizados en la actualidad, se dice que, en los últimos años los delitos informáticos, han sido lo que se han acrecentado con mayor intensidad. Considerando que es posible que se cometa este delito vía Internet, le da esa potestad al delincuente que sin complicación alguna, esté en un país, utilice los servicios de otro, y ataque a personas de un tercer país. De cualquier modo, se han obtenido estadísticas actuales del ranking de los estados, para conocer la situación en la que se encuentran los delitos informáticos en el ordenamiento jurídico penal, asimismo, la lista de delitos informáticos que menos se sancionan.

1.6 BASES TEÓRICAS

1.6.1 Red Social en Internet

Toda red social es un sitio web que brinda servicios y funciones a través de los cuales nos podamos comunicar, y de esta manera los usuarios nos mantenemos en contacto con otros. Las redes sociales están basadas en un software especial que une innumerables funciones particulares: foros, wikis, mensajería, blogs, chat, etc., pero en la misma interface, proporcionando así la conexidad entre todos los usuarios que forman parte de la red. La red social es aquella que sirve para relacionarse personalmente, formando las conocidas comunidades, de modo que socializamos y nos informamos. Lo conforman un grupo de individuos cuyos intereses son equivalentes, aquellos que les une un vínculo, en donde se sienten parte del grupo, y que pertenecen a una cultura común, compartiendo normas, lenguaje y valores, dentro de un ambiente de confianza. **Rodríguez, A. (2011).**

Tenemos tres clases de redes sociales según **Trejo,A.(2016)**

a) **Redes personales:** Está compuesta por millones de usuarios en donde cada uno posee su propia información, ya sean música, datos, fotos, vídeos, etc., pero se vinculan unos con otros a través de la utilización de Internet. Verbigracia: Facebook, WhatsApp, Instagram, Facebook, etc.

b) **Redes temáticas:** Tienen algún parecido con las antes mencionadas, pero no iguales, ya que éstas tratan de concentrarse en un determinado tema, proporcionando las funciones esenciales. Verbigracia: una red deportiva, de cine, de informática, etc.

c) **Redes profesionales:** Es una clase especial, ya que es exclusiva de la esfera laboral, en todos sus aspectos. Este tipo de redes ayuda para que los que están en búsqueda de un trabajo, puedan contactarse con los que los ofrecen, con sus equipos de investigación y captación de personal, entre otros.

1.6.2 Delitos Informáticos

1.6.2.1 Definición de Términos Básicos

Algunas definiciones que autores nos brindan sobre el Delito Informático:

- **Tellez, (2007)** “desde un enfoque típico y atípico, definiéndolo como comportamiento contrario a ley, conducta típica, antijurídica y

culpable, en donde las computadoras son el instrumento para cumplir el fin".

- **Suarez, (2009)** manifiesta: "tiene vinculación con realizar un comportamiento delictivo por medio de miembros o elementos informáticos, o a las conductas ilícitas en donde se afecte la información como bien jurídico protegido, distinto a los intereses tradicionalmente jurídicos".

- **Davara, (2007)** precisa: "es aquél acto que se realiza juntando las peculiaridades que definen al delito, y usando un dispositivo telemático e informático, que trasgreda los derechos del titular".

1.6.2.2 Clasificación de los Delitos Informáticos

a) Sabotaje informático.

Este término alcanza a todos los comportamientos o acciones que se dirigen a ocasionar perjuicios en el software o hardware de un sistema. **López, J. (2011)**

b) Fraude a través de computadoras.

Es aquella maniobra ilegal, en donde se crean datos que no son verdaderos, se alteran éstos o procedimientos que se encuentran en algún sistema informático, para lucrar indebidamente.

c) Delitos informáticos contra la privacidad.

Acciones que de una u otra forma afectan a la privacidad de algún habitante; al acumular,

archivar y divulgar indebidamente datos del sistema informático.

Las **situaciones agravantes** se encuentran en función de:

- Las características de los datos: origen, raza, ideología, creencias, religión, salud y vida sexual.
- La calidad de la agraviada: incapaz o menor de edad.

Abarca la interceptación de las comunicaciones, el uso de artimañas técnicas de transmisión, escucha, grabación, reproducción de sonido, imagen, de cualquier otra señal de comunicación.

d) Interceptación de e-mail:

Aquí es propuesta que se amplíen los criterios que sancionan la violación de correspondencia, e interceptación de telecomunicaciones, de tal manera que el que lee un mensaje electrónico ajeno, posee esta gravedad.

e) Pornografía infantil.

La distribución de pornografía infantil por el mundo está en aumento. En el transcurso del tiempo se han presentado un considerable número de condenas por transmisión o posesión de pornografía infantil, la misma que en un país norteamericano aumentó de 100 a 400 al año. Pero, este problema se complica con la aparición de novedosas tecnologías,

como el uso de la criptografía, el cual permite ocultar la pornografía y demás material "ofensivo".

Según el Instrumento, Medio o Fin u Objetivo, TELLEZ proporciona una clasificación de estos actos delincuenciales de la siguiente manera:

a) Como instrumento o medio.

En esta clase se encuentran las acciones delincuenciales que tienen como medio de comisión a los ordenadores, para dar más claridad a estos mostramos unos ejemplos:

- Adulteración de documentaciones vía digital (cheques, tarjetas de débito, de crédito, y demás)
- Desviación de los estados de cuenta en los casos de contabilidad empresarial.
- Premeditación y simulación de delitos comunes.
- Información personal leída, sustraída o copiada.
- Modificatoria de datos.
- Aprovechamiento indebido o violación de leyes para incluir conductas inadecuadas al sistema.
- Variación del destino del dinero a otra cuenta de ahorros a donde no es la correcta.
- Uso de programas de computación sin autorización.
- Ingreso de pautas que inducen "paralizaciones" en la interna lógica de los sistemas.

- Variación en cuanto a las funciones de los programas, por medio de virus informáticos.
- Obtención de información excedente después de ejecutar los trabajos.
- Accesibilidad a sitios informatizados sin autorización.
- Intervención en una línea de comunicación.

b) Como fin u objetivo:

En esta clase, se encuentran las conductas delincuenciales que afectan a los ordenadores, programas o accesorios:

- Programar pautas que bloqueen totalmente el sistema.
- Destruir los programas mediante alguna técnica.
- Dañar la memoria.
- Atentar físicamente la computadora o los accesorios.
- Retener soportes magnéticos en donde exista una valiosa información para luego chantajear.

Según su gravedad delictiva, el internet facilita y permite la comisión de ciertos actos muy peligrosos como son:

a) **Terrorismo:** a través de las cuales cierto grupo de terroristas envían mensajes anónimos con el único fin de amedrentar a la población remitiendo en estos mensajes sus métodos de acción internacionales, y con la

coexistencia de ciertos programas que encubren la identificación del difusor de dichos mensajes, estos grupos terroristas viven en la impunidad. Los materiales difundidos vía internet, que no solo son usados a nivel de amenazas, sino también de adiestramiento tales como los mensajes sobre fabricación de material explosivo.

b) **Narcotráfico:** Así como en el caso de terrorismo se han dado mensajes donde se difunden recetas para fabricar narcóticos, blanquear dinero y coordinar las formas de entrega y recojo.

c) **Espionaje:** no obstante, todo lo mencionado han surgido casos donde facinerosos han logrado acceder a sistemas no autorizados tales como los sistemas gubernamentales, también acciones como apropiación del e-mail del servicio oculto de un país, y demás actuaciones que se puedan calificar como espionaje si estos actos fuesen realizados por otro gobierno.

d) **Espionaje industrial:** Así como en el espionaje propiamente dicho y descrito un párrafo arriba, también se han producido casos donde se han apropiado de los sistemas operativos de grandes empresas, usurpando diseños industriales, fórmulas, sistemas de fabricación, etc. Dicha información ha sido aprovechada posteriormente por empresas competidoras o

éstas las han divulgado sin ninguna autorización.

e) **Otros delitos:** con las mismas opciones y facilidades que brinda el internet para la comisión de los otros delitos graves vistos con anterioridad, también pueden cometerse algunos actos delincuenciales que puedan trasladarse de la realidad al espacio virtual o viceversa.

1.6.2.3 Clasificación de acuerdo a las Naciones Unidas:

Según esta entidad, para prevenir y controlar los delitos informáticos precisa lo siguiente: “si la problemática es de jurisdicción internacional, se engrandecen los obstáculos y escaseces, puesto que componen un nuevo modo de delinquir y para combatirlo es necesaria que exista cooperación mundial eficiente y establecida”. Ante ello, esta entidad manifiesta la falta de acuerdo internacional en cuanto a estos tipos de infracciones de la siguiente manera:

- Inexistencia de pactos integrales sobre que conductas constituyen delitos informáticos.
- Falta de acuerdos de carácter global en la tipificación de ciertos comportamientos delictivos.
- Autoridades u funcionarios no especializados en el ámbito de delitos informáticos.
- Inexistencia de armonía en las normas procesales del país relacionado con los delitos informáticos.

- Aspecto internacional de innumerables delitos consumados a través de la utilización de ordenadores.
- Falta de convenio de extradición y que fomenten la cooperación internacional.

1.6.2.4 Características de los Delitos Informáticos

a) Son acciones criminales de cuello blanco, por ello para que se configure la comisión de éstas, tendrían que ser un concluyente número de personas con ciertos conocimientos específicos en temas computacionales e informáticos.

b) Son conductas ocupacionales porque al tener el tiempo ocupado las víctimas, estos bandidos aprovechan estos espacios para cometer sus actos delincuenciales.

c) Son acciones de oportunidad puesto que se beneficia del avance tecnológico que emerge en la actualidad, para tener conocimientos especializados en estos temas y así lograr lo cometido, ya que las víctimas son abundantes por el uso de estas tecnologías.

d) Provocan graves y cuantiosos desfalcos económicos, ya que en su mayoría generan “beneficios”.

e) Prometen la comisión fácil de espacio y tiempo debido a que estos delitos son cometidos en breves espacios de tiempo; además para su realización no es necesaria la presencia física.

f) Los casos que se presentan en la realidad son muchos, lo preocupante son las escasas denuncias al respecto debido a la falta de regulación en el fuero internacional penal.

g) Poseen grandiosos problemas para su demostración, por su representación técnica.

El elemento subjetivo que concurre en la comisión de los delitos informáticos es el dolo, sin embargo, existen también casos de carácter culposo.

h) Inducen a menores de edad, ofreciéndoles facilidades para que lo cometan.

i) Estos se están expandiendo cada vez con más frecuencia, por lo que merece mayor atención en cuanto a una regulación jurídica en el ámbito internacional

1.6.3 Seguridad Cibernética

La seguridad cibernética alude a las innovaciones y procedimientos para asegurar las máquinas, los sistemas y la información, vulnerabilidades y agresiones no aprobadas a través de Internet por delincuentes digitales. El ISO 27001 es el estándar universal de seguridad cibernética que da un modelo para crear, actualizar, trabajar, comprobar, auditoría, mantenimiento y mejora de la seguridad de la información en los sistemas de gestión de la información virtual.

Dentro de los dispositivos de seguridad de la red que monitorea el tráfico de la misma y decide si permite o bloquea el tráfico específico en función de un conjunto definido de reglas de seguridad, tenemos las siguientes:

.

a) Firewall

Un firewall o cortafuego es un sistema que permite proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red (expresamente de Internet). El firewall es un sistema que permite filtrar los paquetes de datos que andan por la red. Se trata de un «puente angosto» que filtra, al menos, el tráfico entre la red interna y externa.

Un firewall puede ser un programa (software) o un equipo (hardware) que actúa como intermediario entre la red local (o la computadora local) y una o varias redes externas.[1]

Numerosos accesorios de firewalls basados ofrecen además otros Utilidad al sistema interior aseguran, por ejemplo, Pasando como un servidor DHCP para ese sistema. Numerosos switches que pasan información entre sistemas Segmentos de cortafuegos y, nuevamente, numerosos Los firewalls pueden realizar capacidades de dirección fundamentales. La ingeniería de cortafuegos se desarrolló a finales de los Internet era una innovación razonablemente nueva en cuanto a su utilización mundial y la red.

b) Antivirus

El anti-virus es un tipo de software que se utiliza para evitar, buscar, detectar y eliminar virus en una computadora. La programación antivirus fue creada inicialmente para descubrir y evacuar las infecciones de la máquina, sin embargo, con la expansión de los

[1] http://www.tecnologia-informtaica.com

tipos de malware o software malicioso, la programación antivirus empezó a dar seguridad a otros peligros de la máquina. Específicamente, la programación antivirus puede proteger de: Browser vengativo Objetos auxiliares (BHOS), ladrones del programa, ransomware, llave Madereros, pasajes secundarios, rootkits, caballos de Troya, gusanos, LSPS maligno, dialers, herramientas de fraude, adware y spyware.

Algunos artículos incorporan adicionalmente seguridad de otros peligros de las máquinas, URLS viciadas y contaminadas, spam, truco y ataques de phishing, personalidad en línea (protección), Web de mantenimiento de asaltos de dinero, estrategias de construcción social, amenaza persistente avanzada (APT), botnets, ataques DDOS.

c) Honeypots

Es un sistema de trampa o señuelo, una herramienta de seguridad informática dispuesta en una red o sistema informática ante un posible ataque informático, y así poder detectarlo y obtener información del mismo y del atacante.

La característica principal de este tipo de programas es que están diseñados no solo para protegerse de un posible ataque, sino para servir de señuelo invisible al atacante, con objeto de detectar el ataque antes de que afecte a otros sistemas críticos. El *honeypot*, sin embargo, puede estar diseñado con múltiples objetivos, desde simplemente alertar de la existencia del ataque u obtener información sin interferir en el mismo, hasta tratar de ralentizar el ataque —*sticky honeypots*— y proteger así el resto

del sistema. De esta forma se tienen *honeypots* de baja interacción, usados fundamentalmente como medida de seguridad, y *honeypots* de alta interacción, capaces de reunir mucha más información y con fines como la investigación.

Si el sistema dispuesto para ser atacado forma toda una red de herramientas y computadoras dedicadas en exclusiva a esta tarea se le denomina *honeynet*.[2]

1.6.4 Beneficios de la Seguridad Cibernética

La seguridad cibernética busca fomentar la confianza en el uso de las Tecnologías Informáticas de la Comunicación (TIC); en consecuencia, representa todas las actividades y operaciones encaminadas a reducir y prevenir amenazas y vulnerabilidades, y tener políticas de protección; respuesta al incidente; recuperación, aseguramiento de datos, aplicación de la ley y operaciones militares y de inteligencia relacionadas con la seguridad del espacio cibernético. **Mona A. Jabbour, A. (2016)**

Por lo tanto, la seguridad cibernética toca prácticamente todas las actividades y todos los ciudadanos de todo el mundo; ofrece enormes oportunidades para mejorar el desarrollo humano y lograr una mejor integración de la información en la sociedad. También apoya un mayor acceso al conocimiento y a la educación, así como al desarrollo de políticas y estrategias.

Por otra parte, impone nuevos tipos de paradigmas comerciales, profesionales y sociales, dando lugar a una serie de problemas jurídicos y técnicos que deben

[2] http://www.es.wikipedia.org

abordarse sobre la base del respeto de su naturaleza y necesidades especiales. Por lo tanto, se necesita un enfoque diferente y metodologías diferentes a las adoptadas antes de la era de la tecnología de la información y la comunicación.

Sin embargo, muchos gobiernos y sociedades temen el impacto negativo que las TIC pueden tener sobre sus propios ciudadanos debido a los peligros potenciales que conlleva y por los desafíos económicos, sociales y de seguridad que plantea. En consecuencia, la falta de seguridad en el ciberespacio socava la confianza de la información en la sociedad. Esto es especialmente el caso con muchas intrusiones en todo el mundo, lo que resulta en el robo de dinero, activos y sensible información militar, comercial y económica.

En las instituciones legales y reguladoras que carecen de ciberespacio, la seguridad socava la realización de todo el potencial de la revolución de la tecnología de la información.

En consecuencia, se necesita una atención especial para evitar que el ciberespacio se convierta en una fuente de peligro para los estados y ciudadanos y para prevenir la aparición de un paraíso cibernético.

Las autoridades encargadas tratan de encontrar una forma de prevenir y castigar nuevas formas de actividad delictiva, como los delitos relacionados con las TIC que implican asaltos informáticos. Muchos gobiernos ya han adoptado reglamentos y legislaciones particulares como respuesta a la necesidad de asegurar la adopción de medidas de seguridad.

1.6.5 Regulación Jurídica Internacional

a) Argentina. " Argentina sancionó el 4 de junio de 2008 la Ley 26.388 (promulgada de hecho el 24 de junio de 2008) que modifica el Código Penal a fin de incorporar al mismo diversos delitos informáticos, tales como la distribución y tenencia con fines de distribución de pornografía infantil, violación de correo electrónico, acceso ilegítimo a sistemas informáticos, daño informático y distribución de virus, daño informático agravado e interrupción de comunicaciones".

b) Uruguay. " El Estado uruguayo aprobó en el año 2007 la **Ley Nª 18.237** denominada EXPEDIENTE ELECTRÓNICO cuyo único artículo autoriza el uso de expediente electrónico, de documento electrónico, clave informática simple, firma electrónica, firma digital y domicilio electrónico, constituido en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales. Los delitos informáticos no son de tratamiento específico por la legislación uruguaya, puesto que no existe una ley de ilícitos informáticos (no puede haber delito sin ley previa, estricta y escrita que lo determine - principio de legalidad-), ni tampoco un título específico relativo a los mismos en el Código Penal Uruguayo".

c) Colombia. " En Colombia el 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 "Por medio del cual se

modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado “De la Protección de la información y de los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales. En Colombia existen instituciones de educación como UNICOLOMBIA que promueven capacitaciones en temas relacionados con Delitos Informáticos, el mejor manejo y uso de la prueba digital, establecer altos estándares científicos y éticos para informáticos forenses, llevar a cabo investigación y desarrollo de nuevas tecnologías y los métodos de la ciencia del análisis forense digital e Instruir a los estudiantes en diversos campos específicos sobre nuevas tecnologías aplicadas a la informática Forense, la investigación científica y el proceso tecnológico de las mismas”.

d) **España. “**En España, los delitos informáticos son un hecho sancionable por el Código Penal, estas sanciones se recogen en la Ley Orgánica 10/1995, de 23 de noviembre en el BOE número 281, de 24 de noviembre de 1995. A la hora de proceder a su investigación, debido a que una misma acción puede tener consecuencias en diferentes fueros, comenzará la investigación aquel partido judicial que primero tenga conocimiento de los hechos delictivos cometidos a través de un medio informático, si durante el transcurso de la

investigación, se encuentra al autor del delito y pertenece a otro partido judicial, se podrá realizar una acción de inhibición a favor de este último para que continúe con la investigación del delito".

e) **México. "**En México, los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática son hechos sancionables por el Código Penal Federal - Título Noveno capítulo I y II. El artículo 167 fr. VI del Código Penal Federal sanciona con prisión y multa al que intencionalmente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio, de video o de datos".

f) **Venezuela. "**El 30 de octubre de 2001 la Asamblea Nacional formulo la Ley Especial contra los Delitos Informáticos donde se decreta, a través de 32 Artículos, como se protege a todos los sistemas y tecnologías de información en Venezuela, cuáles son los delitos relacionados con estos y que sanciones se aplican en cada delito específico".

1.6.6 Formas de Control

1.6.6.1 Preventivo

Este tipo de ilícitos requieren un control necesario por no encontrarse en la actualidad una adecuada protección jurídica, por lo mismo, tanto el sector privado como el público han tomado algunas medidas para protegerse frente

a estos actos ilícitos; éstas servirían mucho al momento de elaborar una legislación más completa y coherente para frenar este delito.

Entre las cuales están:

- Elaboración de un examen psicométrico previo al ingreso a áreas de sistemas en las empresas.
- Inclusión de cláusulas especiales en los contratos de trabajo con el personal informático que así lo requiera por el tipo de labores a realizar.
- Establecimiento de un código ético de carácter interno en las empresas.
- Adopción de estrictas medidas en el acceso y control de las áreas informáticas de trabajo.
- Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes.
- Identificación y en su caso, segregación de personal informático descontento.
- Rotación en el uso de acceso al sistema.

1.6.6.2 Correctivo

Este tipo de control podrá ser aplicados cuando ya exista un conjunto de normas que regulen todos los supuestos de hechos configurativos de estos ilícitos penales, ya que una adecuada legislación no solo traería efectos correctivos sino también preventivos, de tal forma que se reducirían de una manera muy notable estos ilícitos que tanto mal causan a los interesados individuales y sociales.

1.6.7 Impacto de los delitos informáticos

1.6.7.1 Impacto a nivel General

Hoy en día los usuarios online superan los 200 millones, lo que es un incremento muy significativo comparado con los 26 millones en el año 1995. Es que las tecnologías nos han facilitado muchas cosas, entre ellas comprar, vender, realizar pagos, consultar a nuestros médicos, entre muchas acciones que nos facilitan las redes para nuestro obrar cotidiano, sin tener que acudir personalmente a las instituciones que brindan este servicio. Por lo cual, las personas que cometen estos delitos son tan diversos, y tan escurridizos para ley, que en reiteradas ocasiones pasan desapercibidos a través de las fronteras, ocultarse tras incontables enlaces o simplemente desvanecerse sin dejar documento alguno que pueda indicar rastro de ellos. Como se observa son diversos los modus operandi de estos delincuentes, que no solo van en esconder pruebas delictivas, sino que también sabotean las computadoras, manipulan datos, mandan virus que dañen programas cibernéticos, etc. y un sin fin de accionares ilícitos.

1.6.7.2 Impacto a nivel Social

Este hecho ha provocado en la sociedad que ésta sea cada vez más desconfiada a la hora de utilizar las tecnologías informáticas. Entonces este hecho viene afectando una nueva forma de negociación, hasta el punto que

podría menguar el comercio electrónico por la falta de apoyo por parte de la población en general.

Las personas que cometen estos delitos son aquellas que tienen ciertos conocimientos especiales en tecnología, quienes día tras día, vienen perfeccionando sus actos delictivos; cuyas víctimas no solo son personas naturales, sino que su mira ahora está mucho más alta, como lo es el ámbito empresarial y global. Por lo cual aquellas personas que no tienen conocimientos básicos en tecnología, serán siempre blanco fácil para estos malhechores, entonces es necesario contar con algo de conocimiento en este campo para no ser víctimas de ellos. El componente clave para hacerle frente a este mal es la educación a la población en cuanto a tecnología informática, para que de esta manera ellos no sean engañados y manipulados de manera fácil y sencilla.

1.6.7.3 Impacto en la esfera judicial:

A raíz del crecimiento de estos delitos, también ha surgido la preocupación de muchos países por legislar estas conductas antijurídicas que están dañando la seguridad de su población. Son muchos las naciones que han promulgado leyes para regular esta situación creciente, otros han actualizado sus leyes obsoletas, para que aquellos delitos considerados tradicionales, sean a su vez considerados ilegales en el mundo virtual.

Otros países cuentan con un grupo especializado en la investigación de estos

delitos, tal es el caso de la Oficina de Investigaciones Especiales de la Fuerza Aérea de los Estados Unidos, los Investigadores del Internet de Australia; grupos que son especialistas en el recojo de pruebas.

1.6.8 La Identidad

El término identidad se muestra a menudo como una abstracción muy amplia y compleja, la cual parte de la noción que del mismo se tiene, pues se utiliza tanto para reflejar la realidad íntima de un individuo, como su relación con otra u otras realidades externas a él. Es decir, la identidad puede definirse en un principio, como el modo de ser de cada persona, proyectada a la realidad social; de este modo, la identidad de la persona no se agota con los caracteres que externamente la individualizan, y que conforman sus signos distintivos, sino que incluyen un conjunto de valores espirituales que definen la personalidad de cada sujeto, sus cualidades, atributos, pensamientos; que permiten traducirlos en comportamientos efectivos de proyección social, no interno. Consiste en que cada persona no vea alterada, ni negada la proyección externa y social de su personalidad" (Ynchausti Pérez & García Martínez, 2012).

Igualmente, Del Gatto Reyes define a la identidad como "un atributo de la persona humana, Derecho Humano absoluto, personal e imprescriptible, objeto de protección nacional e internacional". (Del Gatto Reyes, 2000).

A decir de ello, según Zea plantea: "la identidad, como la cultura que le da sentido, es algo propio del ser humano, querámoslo o no la tenemos como el cuerpo tiene su sombra. El problema está en reconocer lo propio y aceptarlo. Hombres iguales todos, por ser entre sí

distintos, por poseer una personalidad, por ser hombres concretos y no reflejos de una abstracción vacía.

En tal sentido, el término identidad constituye un derecho humano y como tal es de carácter universal, inalienable, intransferible e irrenunciable; puede expresar tanto aquello que caracteriza, especifica y singulariza a un individuo, lo más íntimo de éste, como su relación de cercanía y pertenencia a ciertas realidades". (Zea, 1990).

"El derecho a la identidad personal se circunscribía prácticamente al derecho al nombre en el marco de los derechos de la personalidad, definidos por Ferrara como: "Los derechos supremos del hombre, los que le garantizan el goce de sus bienes personales, el goce de sí mismo, la actuación de sus propias fuerzas físicas o espirituales" (Diéz-Picazo & Gullón, 2003).

De esta manera, se aprecia que la evolución teórica – doctrinal y legislativa del Derecho a la Identidad Personal abarca mucho más que el Derecho al Nombre; ampliando sus horizontes a una perspectiva integral de la persona humana. De esta forma el derecho a la identidad personal comprende no solo el nombre, sino además la filiación y las relaciones familiares, las relaciones de índole políticas, culturales, entre otras dimensiones de la personalidad.

1.6.9 Regulación Jurídica del Delito de Suplantación a la Identidad:

LEY Nº 30096

LEY DE DELITOS INFORMÁTICOS

CAPÍTULO II

Delitos contra Datos y sistemas informáticos

Artículo 2. Acceso ilícito

"El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado".

Artículo 3. Atentado contra la integridad de datos informáticos

"El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

Artículo 4. Atentado contra la integridad de sistemas informáticos

"El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa".

CAPÍTULO III

Delitos informáticos contra la indemnidad y libertad sexuales

Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

"El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor

de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal".

CAPÍTULO IV
Delitos informáticos contra la intimidad y el secreto de las comunicaciones

Artículo 6. Tráfico ilegal de datos

"El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años".

Artículo 7. Interceptación de datos informáticos

"El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia. La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales"

CAPÍTULO V
Delitos informáticos contra el patrimonio

Artículo 8. Fraude informático

“El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social”.

CAPÍTULO VI
Delitos informáticos contra la fe pública

Artículo 9. Suplantación de identidad

“El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años”.

CAPÍTULO VII
Disposiciones comunes

Artículo 10. Abuso de mecanismos y dispositivos informáticos

“El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta

servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa".

Artículo 11. Agravantes

"El juez aumenta la pena privativa de libertad hasta en un tercio por encima del máximo legal fijado para cualquiera de los delitos previstos en la presente Ley cuando:

1. El agente comete el delito en calidad de integrante de una organización criminal.
2. El agente comete el delito mediante el abuso de una posición especial de acceso a la data o información reservada o al conocimiento de esta información en razón del ejercicio de un cargo o función.
3. El agente comete el delito con el fin de obtener un beneficio económico, salvo en los delitos que prevén dicha circunstancia.
4. El delito compromete fines asistenciales, la defensa, la seguridad y la soberanía nacionales".

1.7 PLANTEAMIENTO DE LA HIPÓTESIS:

¿Las medidas de protección informática adoptadas en nuestra legislación son eficaces para prevenir el delito de suplantación de identidad cibernética?

1.8 VARIABLES:

Variable 1:

Eficacia de las Medidas de Protección Informática

Variable 2:

Delito de Suplantación de Identidad Cibernética.

CAPITULO II

MATERIALES Y METODOLOGIA

2.1 MATERIAL

2.2 MATERIAL DE ESTUDIO

2.2.1 Población

La población está conformada por abogados especializados en Derecho Civil y Penal capacitados en el rubro del Derecho a la Identidad y Delitos Informáticos, ubicados en la ciudad de Trujillo.

2.2.2 Muestra

Hernández (1991) señala que la muestra es un conjunto seleccionado dentro de una determinada población, la cual la representará y se convertirá en materia de estudio dentro de esta investigación, estando a ello, la muestra del presente proyecto estará compuesta por:

- 20 abogados especializados en Derecho Civil y Derecho Penal, en el rubro del derecho a la identidad.

2.3 Técnicas, Procedimientos e Instrumentos

2.3.1 Para Recolectar Datos

En la recolección de datos se procedió de la siguiente forma:

a) **Primer paso**: Visitamos las Bibliotecas especializadas en Derecho de las universidades UPN, UCV, UNT, UPAO y Colegio de Abogados de La Libertad, con la finalidad de recolectar

información especializada compuesta por: la legislación, libros, artículos y ensayos jurídicos que se han publicado en las revistas de Derecho de Familia, además de documentación que desarrolle el tema abordado en la presente investigación. En este paso, se utilizó la técnica del fotocopiado, la cual nos permitió contar con reproducciones de dichos documentos, y servir como soporte bibliográfico en el desarrollo del tema de investigación. Para ello, fue necesario realizar las coordinaciones administrativas a efectos de averiguar los horarios de atención de las mismas.

b) **Segundo paso**: Realizamos la búsqueda de la información desmaterializada, visitando las bibliotecas virtuales y blogs, los cuales nos permitió recabar la información sobre el tratamiento legal que el tema investigado ha tenido en nuestro país como en otros.

c) **Tercer paso**: Se creó el archivo correspondiente del esquema de desarrollo del presente Informe, conforme a la estructura aprobada por la Universidad. Posteriormente se identificó los capítulos y subcapítulos del mismo, para la realización de una ordenada recopilación de información.

d) **Cuarto paso**: Realizamos el análisis de los instrumentos.

e) **Quinto paso**: Organizamos, ordenamos, clasificamos y depuramos la información materializada que se encontró, teniendo en cuenta el grado de aportación al presente Informe.

f) **Sexto pasó**: Se elaboró los instrumentos necesarios, en este caso, la guía de observación a efectos de realizar el análisis de los instrumentos.

g) **Séptimo paso**: Aplicamos las técnicas y los instrumentos señalados, los mismos que han permitido alcanzar los resultados y posteriormente contrastar y comprobar la hipótesis.

2.3.2 De procesamiento de información

Luego de haber recolectado la información y haber utilizado las técnicas y los instrumentos de investigación, se ha realizado el procedimiento siguiente:

a) **Depuración de la Información**: Se seleccionó la información más importante y trascendente, escogiendo la información más actual y excluyendo la que no se estimó oportuna por no tener relevancia con el tema investigado. Este procedimiento resultó ventajoso en la investigación, exclusivamente al elaborar el Marco Teórico, así como los Resultados y Discusión de los resultados.

b) **Clasificación de la Información**: Se procedió a clasificar la información en relación a la dispersión temática y su importancia, utilidad y actualidad.

c) **Orden y organización**: Se procedió a organizar la información por grupos, los mismos que posteriormente conformó cada título y sub capitulo en la presente investigación.

d) **Tabulación de la información**: Por último, se procedió a presentar la información que se recolectó, esto es, trasladar nuestros resultados a tablas, facilitando su procedimiento. Posterior a ello, se trasladó las tablas a los gráficos, a fin de analizar, interpretar y discutir, como corresponda.

2.4 Operacionalización de Variables:

VARIABLE	DEFINICIÓN OPERACIONAL	DIMENSIÓN	MARCO TEÓRICO
Delito de Suplantación de Identidad	Es el delito que regula los hechos de suplantación de identidad.	Derecho Penal	**1.** Derecho penal. **1.1.** Concepto. **1.2.** Fundamentos. **1.3.** Protección. **1.4.** Finalidad. **1.5.** Ley penal.
Medidas de Protección Cibernética	Son mecanismos con los se busca la protección del delito de suplantación de identidad que son: □ Seguridad Jurídica □ Identidad	Derecho a la identidad	1. Seguridad Jurídica. **1.1.** Concepto. **1.2.** Fundamentos. **1.3.** Protección del derecho penal. 2. Identidad. **2.1.** Concepto. **2.2.** Fundamentos.

CAPITULO III

RESULTADOS

Aplicados los instrumentos realizados para esta investigación, se tuvo los siguientes resultados en las encuestas, que fueron realizadas en cuatro grupos, siendo de la siguiente manera:

Encuesta realizada a 20 abogados especializado en Derecho de Civil y Penal, en el rubro Derecho a la identidad.

Estas encuestas realizadas, se aplicaron a abogados especialistas en Derecho de Civil y Derecho Penal, respecto del Derecho a la Identidad y los Delitos Informáticos.
El resultado fue el siguiente, conforme a las preguntas:

1. **Considera Usted que las medidas de protección en la prevención del delito de suplantación de identidad cibernética previstas en nuestro ordenamiento legal son eficaces :**

   De los 20 abogados encuestados, se obtuvo que el 40% opinó estar totalmente de acuerdo en que las medidas previstas en nuestra legislación son eficaces respecto de la prevención del delito de “suplantación de identidad cibernética” pero deben incorporarse otras.

   Por otro lado, se obtuvo que el 20% de los abogados encuestados, respondió estar de acuerdo en que resulta necesario incorporar medidas de mayor eficacia en la prevención del delito de suplantación de identidad cibernética, lo cual sumado al 40% de los que respondieron estar totalmente de acuerdo, suman el 60 % de abogados que coinciden en opinar que resulta necesario incorporar medidas de protección en la prevención del delito de suplantación de identidad cibernética

Además, el 30% señalaron no estar de acuerdo en que resulta necesario incorporar otras medidas de prevención en la consumación del delito de suplantación de identidad cibernética.

Por último, el 10% señaló que están en muy desacuerdo que resulta necesario incorporar otras medidas de prevención en la consumación del delito de suplantación de identidad cibernética, lo cual sumado al 30 % que opinaron estar en desacuerdo, hacen un total del 40% que coinciden no estar de acuerdo.

Sin embargo, es la mayoría, esto es el 60% que como se repite, opinan de manera afirmativa y precisan que resulta necesario incorporar otras medidas de protección en la prevención del delito de suplantación de identidad cibernética.

2. **Considera usted que la ausencia de medidas de protección en la prevención del delito de "suplantación de identidad cibernética" vulnera el derecho a la identidad y la seguridad jurídica:**

Del 100% de los abogados encuestados se obtuvo que el 45% opinaron que están totalmente de acuerdo que la ausencia de medidas de protección en la prevención del delito de suplantación de identidad cibernética vulnera el derecho a la identidad y la seguridad jurídica.

Así mismo, el 40% de los abogados precisaron que están de acuerdo que la ausencia de medidas protección en la prevención del delito de suplantación de identidad cibernética vulnera el derecho a la identidad y la seguridad jurídica, lo cual sumado al 45% que opinaron estar totalmente de acuerdo, lo cual resulta el 85% de abogados que afirman que la ausencia de medidas de protección en la prevención del delito de suplantación de identidad cibernética vulnera el derecho a la identidad y la seguridad jurídica.

Sin embargo, el 15% de los encuestados precisaron que no están de acuerdo que la ausencia de medidas de protección en la prevención del delito cibernético vulnera el derecho precisado y la seguridad jurídica; empero, la mayoría confirma lo contrario.

3. **Considera usted que la ausencia de medidas de protección en la prevención en el delito de suplantación de identidad cibernética, coadyuva al delito:**

El 60% de los encuestados precisaron que están totalmente de acuerdo que la ausencia de medidas de protección en la prevención en el delito de suplantación de identidad cibernética, coadyuva a la comisión del delito.

Así mismo, el 35% de los abogados, indicaron que están de acuerdo que la ausencia de medidas de protección en la prevención del delito de suplantación de identidad cibernética, coadyuva a la comisión del delito, lo cual sumado al 60% que indicaron estar totalmente de acuerdo, hacen un total de 95% de personas que consideran afirmativamente que la ausencia de medidas de protección en la prevención en el delito de suplantación de identidad cibernética, coadyuva a la comisión del delito.

Sin embargo, sólo el 5% de los encuestados, opinaron estar muy en desacuerdo que la ausencia de medidas de protección en la prevención en el delito de suplantación de identidad cibernética, coadyuva a la comisión del delito; lo cual, comparado con el resultado anterior, no hace la mayoría.

4. **¿Considera usted que deben adoptarse otras medidas de prevención contra el delito de suplantación de identidad cibernética garantiza el derecho a la identidad?**

De los abogados encuestados se tiene que el 55% opinaron que deben adoptarse otras medidas de prevención contra el delito de sustitución de identificación cibernética para garantizar el derecho a la identidad

Así mismo 40% de los abogados encuestados precisaron que adoptar medidas de prevención contra el delito de suplantación de identidad cibernética garantiza este derecho fundamentales, lo cual sumado al 55% de los que opinaron estar totalmente de acuerdo,

hacen un total de 95% de personas que respondieron afirmativamente.

Empero el 5% de los encuestados respondieron no estar en acuerdo ni en desacuerdo en adoptar otras medidas de prevención contra el delito de sustitución de identificación

5. **¿Considera usted que es deber del Estado, adoptar en su política criminal, medidas de prevención contra el "delito de suplantación de identidad"?**

Del 100% de los encuestados, el 35% respondieron que es deber del Estado, adoptar en su política criminal, medidas de prevención en la comisión del delito de suplantación de identidad cibernética para evitar la vulneración a este derecho.

Así mismo, el 35% respondieron que están de acuerdo que es deber del Estado, adoptar en su política criminal, medidas de prevención en comisión del delito de suplantación de identidad cibernética para evitar la vulneración a este derecho, lo cual sumado al otro 35% que están totalmente de acuerdo, hace un total de 70% que están a favor que es deber del Estado, adoptar en su política criminal, medidas de prevención de este delito.

Por otro lado, el 20% respondió que están en desacuerdo que es deber del Estado, adoptar en su política criminal, medidas de prevención en la comisión del delito de suplantación de identidad cibernética para evitar la vulneración a este derecho.

Por último, el 10% respondió estar muy en desacuerdo que es deber del Estado, adoptar en su política criminal, medidas de prevención en la comisión del delito de suplantación de identidad cibernética para evitar la vulneración de este derecho, lo cual sumado al 20% que respondió estar en desacuerdo, hacen un total del 30% de personas que opinan de manera negativa que si es deber del Estado, adoptar en su política criminal, medidas de prevención en la comisión del delito de suplantación de identidad cibernética para evitar la vulneración de este derecho, empero ello conforme se advierte no es la mayoría.

CAPITULO IV
DISCUSION

A efecto práctico se realizó un análisis íntegro de las encuestas realizadas, clasificando sólo el tipo de preguntas, siendo de la siguiente manera:

1. **Considera Usted que las medidas de protección en la prevención del delito de suplantación de identidad cibernética previstas en nuestro ordenamiento legal son eficaces**

   De los 20 abogados encuestados, se obtuvo que el 40% opinó estar totalmente de acuerdo que resulta necesario incorporar medidas de prevención en la comisión de este delito cibernético.

   Un individuo comete este delito cuando se hace pasar por otro a fin de lograr la obtención de un beneficio para sí mismo.

   Esta acción puede tener la intención de cometer otros hechos que ya constituyen delitos en sí mismos, pero también para la contratación de servicios de telefonía, para obtener una hipoteca o un crédito, para efectuar compras tanto en tiendas físicas como a través de tiendas online, etcétera.

   “En internet, y gracias a las facilidades para crear perfiles en redes sociales con apenas una dirección de correo electrónico (cualquier dirección de correo electrónico), la suplantación de identidad se ha multiplicado. Es bastante habitual que alguien utilice fotografías de otra persona sin su consentimiento expreso y cree un perfil en Twitter, Facebook o cualquier otra red, incluso utilizando también su nombre, y haga uso de esta cuenta para insultar, acosar a terceras personas y hasta para lograr hacerse con datos personales y bancarios de otros usuarios con los cuales continuar cometiendo sus fechorías”.

   En los casos en que el delincuente adopta la identidad de otra personal para falsificar tarjetas de crédito, podría estar incurriendo en delitos de fraude y estafa, mientras que el acceso ilegítimo a perfiles personales mediante el robo de contraseñas constituye un

delito de descubrimiento y revelación de secretos al que se podría sumar un delito de daños a soportes, redes o sistemas informáticos.

Por ello, de los 20 abogados encuestados, se obtuvo que el 40% opinó estar totalmente de acuerdo que resulta necesario incorporar medidas de prevención en la consumación del delito de suplantación de identidad cibernética.

2. **Considera usted que la ausencia de medidas de protección en la prevención del delito de "suplantación de identidad cibernética" vulnera el derecho a la identidad** y la seguridad jurídica**:**

Del 100% de los abogados encuestados se obtuvo que el 45% opinaron que están totalmente de acuerdo que la ausencia de medidas de protección en la prevención de la comisión del delito de suplantación de identidad cibernética vulnera este derecho y la seguridad jurídica.

De lo dicho se tiene que efectivamente, las personas encuestadas consideran que actualmente no existe medidas de protección en la prevención respecto al delito de suplantación de la identidad, lo cual, pues vulnera a este derecho y la seguridad jurídica, el mismo que forma parte del núcleo de los derechos fundamentales de las personas.

Por seguridad jurídica debe entenderse como aquel Deber del Estado mediante el cual, garantiza que el ordenamiento jurídico vigente resguarda todos los bienes jurídicos.

Mientras por derecho a la identidad debe entenderse como aquel derecho fundamental que forma parte de la integridad de la persona, dado que a través de este derecho, la persona aparece en el sistema jurídico.

Siendo así, se tiene que al no tener medidas de prevención, el delito de suplantación de identidad cibernética vulnera estos derechos porque el Estado no ha cumplido con su deber de adoptar en su política criminal, acciones que permitan prevenir estos delitos, así

también porque la víctima queda expuesta a la vulneración de otros tantos derechos fundamentales.

3. **Considera usted que la ausencia de medidas de protección en la prevención en el delito de suplantación de identidad cibernética, coadyuva al delito:**

El 60% de los encuestados precisaron que están totalmente de acuerdo que la ausencia de medidas de prevención en el delito de suplantación de identidad cibernética, coadyuva la consumación del delito.

Debe entenderse por medidas de prevención, aquellos mecanismos que el Estado adopta en este caso específico en su política criminal, para evitar la consumación del delito de suplantación de identidad cibernética.

El delito de suplantación de identidad cibernética como bien se ha mencionado, consiste en las acciones mediante las cuales, el sujeto agente se hace pasar por su víctima de manera informática, utilizando programas, con los que, obtiene ventajas, como por ejemplo, compras por internet, etc.

Como se ha repetido, este delito es pluriofensivo, dado que tiene múltiples bienes jurídicos que protege, entre ellos y principalmente el derecho a la identidad y a la seguridad jurídica.

Que, el Estado hace una mala práxis de su política criminal ya que la enfoca o la prioriza dependiendo la coyuntura y la presión mediática, tanto así, que por ejemplo, priorizó la violencia familiar penalizando los actos, lo cual, marca la diferencia con el delito de suplantación de identidad cibernética, la que si bien es cierto, existe incidencia delictiva, esta no será prioridad en las atenciones de la política criminal del Gobierno de turno, porque no es mediático.

En ese sentido, la postura adoptada por el Estado, ocasiona la inexistencia de los mecanismos de prevención lo cual genera vulneración de los derechos a la identidad y seguridad jurídica.

4. **Considera usted que deben adoptarse otras medidas de prevención contra el delito de suplantación de identidad cibernética garantiza el derecho a la identidad** De los abogados encuestados se tiene que el 55% opinaron que adoptar medidas de prevención contra el delito de suplantación de identidad cibernética garantiza el derecho a la identidad.

Como se viene precisando, el delito de suplantación de identidad es un delito pluriofensivo porque busca tutelar o proteger varios bienes jurídicos entre ellos, los derechos a la seguridad jurídica y el derecho a la identidad.

Es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Los delitos informáticos son actividades ilícitas que:

- Se configuran mediante el uso de computadoras, procedimientos informáticos entre otros puntos de conexión de las comunicaciones (el tratamiento de la información científica es el medio o vía para realizar un delito); o
- Tienen por objetivo principal provocar menoscabos, incitar pérdidas o paralizar el uso de sistemas informáticos (delitos informáticos).

Algunas formas de adoptar mecanismos de prevención serían:

- Elaboración de un examen psicométrico previo al ingreso e áreas de sistemas en las empresas.
- Inclusión de cláusulas especiales en los contratos de trabajo con el personal informático que así lo requiera por el tipo de labores a realizar.
- Establecimiento de un código ético de carácter interno en las empresas.
- Adopción de estrictas medidas en el acceso y control de las áreas informáticas de trabajo.
- Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes.

- Identificación y, en su caso, segregación de personal informático descontento.
- Rotación en el uso de acceso al sistema.

5. Considera usted que es deber del Estado, adoptar en su política criminal, medidas de prevención contra el "delito de suplantación de identidad

Del 100% de los encuestados, el 35% respondieron que están totalmente es deber del Estado, adoptar en su política criminal, medidas de prevención en la consumación del delito de suplantación de identidad cibernética para evitar la vulneración de derechos fundamentales.

Según a la contratación de los resultados se establece que la ley de delitos informáticos que se administra es ineficaz, primero porque su tipificación no es precisa, segundo la ley no está debidamente implementada, y al no existir la parte logística o instrumentos adecuados para su investigación, la persecución y sanción de este delito es muy complicado por no decir imposible.

Otro de los temas de gran preocupación es que al no ser precisa esta ley, y no regular todas las conductas infractoras, los delincuentes informáticos tienen una salvedad, quedando impunes frente a sus actos delictivos, esto porque las políticas criminológicas acerca de este delito planteadas en nuestra legislación peruana se encuentran desfasados en cuanto a una realidad tecnológica actual, lo que se evidencia en la falta de preparación para su persecución legal por parte de las entidades persecutoras de estos delitos. Lo que genera una gran preocupación para toda la población.

De los resultados obtenidos de la encuesta también se observa que, la mayoría de fiscales, no adecuan correctamente el tipo penal, esto porque se han dado casos como violación a la intimidad por redes sociales, y fue adecuado al tipo penal de coacción, como se puede observar no se ajustó correctamente al tipo penal que corresponde para estos delitos sino, un artículo de delitos comunes del Código Penal, lo cual denota la mala

adecuación que hace el persecutor del delito frente a un hecho delictivo que merece un trato especial según la ley dada para estos delitos, pero al no ser precisa esta ley, provoca ambigüedad y confusión a los operadores de justicia. Y así otros casos particulares, a las cuales no se dieron el tratamiento adecuado, a la actualidad, en nuestra ciudad existe desconocimiento en los despachos tanto judiciales como fiscales respecto a este tema desafiante para el derecho, esto porque no se ha difundido, ni profundizado estos conocimientos.

Sabemos que todo lo concerniente a la tecnología es un campo nuevo para muchas personas, dada la naturaleza virtual de los delitos informáticos resulta dificultoso su tratamiento y a su vez su tipificación. Lo cierto es que si no se actúa con inmediatez, y no buscamos alternativas nuevas de soluciones frente a este mal social, los delincuentes mejores preparados en este campo nos seguirán llevando la delantera, burlando todos los estándares propuestos para todos estos casos de delitos cibernéticos

CAPITULO V

CONCLUSIONES

1. Las medidas de prevención son mecanismos o acciones realizadas por el Gobierno de turno y que la aplican en su política criminal a efecto de evitar o prevenir la comisión de diversos ilícitos.

2. El delito de suplantación de identidad cibernética es un delito informático mediante el cual, el sujeto agente se hace pasar por su víctima, vía informática, obteniendo beneficio patrimonial o de alguna otra índole.

3. El Estado no aplica en su política criminal, medidas de prevención que eviten la comisión del delito de suplantación de identidad cibernética, vulnerando así la seguridad jurídica.

4. Se deben adoptar medidas de prevención contra el delito de suplantación de identidad cibernética para evitar que se vulnere el derecho a la identidad y la seguridad jurídica.

CAPITULO VI

RECOMENDACIONES

1. Se debe adoptar mecanismos de prevención más eficaces a efecto de garantizar los bienes jurídicos que tutela el delito de suplantación de identidad cibernética y la seguridad jurídica.

2. Conforme a la regulación sobre delitos informáticos, no debe limitarse a la sanción punitiva, sino que deben aplicarse acciones en la política criminal, que prevengan la comisión de este ilícito dotando al Ministerio Público y la PNP de herramientas tecnológicas para tal fin, a citar el patrullaje cibernético.

3. Implementar oficinas especializadas descentralizadas de criminalística que permitan la investigación sobre los delitos informáticos.

4. Imponer a las entidades financieras y comerciales, la adopción de software de protección de datos y restricción a la base que los contiene para evitar la comisión de este ilícito y velar por la seguridad jurídica.

CAPITULO VII

REFERENCIAS BIBLIOGRAFICAS

I. TEMATICOS

1. Bramont, L (2000). Delitos Informáticos. Lima: Revista Peruana de Derecho.
2. Calderón, L. (2010). Delitos informáticos y Derecho Penal. México: Ubijus.
3. Camacho, L (1997). El delito informático. Madrid: Gráficas Condor.
4. Durand (2002). Los delitos informáticos en el Código Penal Peruano. Lima: revista Peruana de Ciencias Penales.
5. Fernández (2002). Los delitos informáticos. Lima: Juristas.
6. Morant (2003). Protección Penal de la intimidad frente a las nuevas tecnologías. Valencia: Ed. Práctica de Derecho.
7. Valdés, T. (2003). Derecho Informático (3° ed.). México: Mac Graw Hill.
8. Orts (2001). Delitos Informáticos y delitos comunes cometidos a través de la informática. Valencia: Tirant Lo Blanch.
9. Villavicencio, F. (2013), Derecho Penal – Parte General. Lima: Grijley.

II. WEBGRAFÍA

1. https://issuu.com/universidaddel/docs/tesis lic derecho ever sanchez u la
2. https://es.wikipedia.org/wiki/Delito inform%C3%A1tico
3. http://www.monografias.com/trabajos6/delin/delin.shtml
4. http://derecho-informado.blogspot.pe/2013/09/tesis-delitos-informaticos.html
5. https://es.scribd.com/doc/63118627/Plan-de-Tesis-DELITOS-INFORMATICOS
6. http://www.oas.org/juridico/spanish/cyb ecu delitos inform.pdf
7. http://bdigital.ces.edu.co:8080/repositorio/bitstream/10946/1334/2/Delito s%20en%20las%20Redes%20Sociales.pdf
8. http://mjv.viegasociados.com/wpcontent/uploads/2011/05/DelitosInform at icos.pdf

ANEXOS

N° DE INSTRUMEN-TOS APLICADOS	MEDIDAS DE PROTECCIÓN INFORMATICA Y SU EFICACIA EN LA PREVENCION DEL DELITO DE SUPLANTACION DE IDENTIDAD CIBERNETICA EN LA CIUDAD DE TRUJILLO				
	ABOGADOS ESPECIALIZADOS EN DERECHO DE FAMILIA: DERECHO DE ALIMENTOS				
	P_1	P_2	P_3	P_4	P_5
1	D	D	D	D	B
2	D	D	D	D	B
3	B	D	E	E	B
4	B	A	D	E	A
5	B	A	E	E	A
6	A	D	A	D	A
7	D	E	D	D	B
8	B	D	E	E	B
9	B	D	E	E	B
10	A	D	D	D	B
11	B	A	D	D	B
12	D	D	E	C	B
13	E	E	E	D	B
14	E	E	E	D	B
15	E	E	E	E	B
16	E	E	E	E	A
17	E	E	D	E	A
18	E	E	E	E	A
19	E	E	E	E	E
20	E	E	E	E	E

MATRIZ DE VALIDACIÓN DE INSTRUMENTO CUESTIONARIO PARA ENCUESTAS A ESPECIALISTAS EN DERECHO CIVIL Y DERECHO PENAL, ESPECIFICAMENTE EN EL RUBRO DEL DERECHO A LA IDENTIDAD

TITULO DE LA INVESTIGACIÓN:

MEDIDAS DE PROTECCIÓN INFORMATICA Y SU EFICACIA EN LA PREVENCION DEL DELITO DE SUPLANTACION DE IDENTIDAD CIBERNETICA EN LA CIUDAD DE TRUJILLO, 2020.

VARIABLE 1: DELITO DE SUPLANTACIÓN DE IDENTIDAD												
DIMENSIÓN 1: DERECHO PENAL												
INDICADORES	**ITEMS**	**CRITERIOS DE VALIDACIÓN DE CONTENIDO**										**OBSERVACIONES**
		REPRESENTATIVIDAD		**PERTINENCIA**		**COHERENCIA**		**COSISTENCIA**		**CLARIDAD**		
		A		**A**		**A**		**A**		**A**		
Suplantación de identidad	Considera usted que resuelta necesario incorporar medidas de prevención contra el delito de suplantación de identidad cibernética	**3**		**3**		**3**		**3**		**3**		
Delito pluriofensivo	Considera usted que la ausencia de medidas de prevención contra el delito de suplantación de identidad cibernética vulnera la seguridad jurídica y el derecho a la identidad	**3**		**3**		**3**		**3**		**3**		

VARIABLE 2: MEDIDAS DE PREVENCION												
DIMENSIÓN 1: LA CONSTITUCION												
INDICADORES	**ITEMS**	**CRITERIOS DE VALIDACIÓN DE CONTENIDO**										**OBSERVACIONES**
		REPRESENTATIVIDAD		**PERTINENCIA**		**COHERENCIA**		**COSISTENCIA**		**CLARIDAD**		
		A		**A**		**A**		**A**		**A**		
- Constitución Política del Perú.	Considera usted que la ausencia de medidas de prevención en el delito de suplantación de identidad cibernética, coadyuva a la comisión del delito.	**3**		**3**		**3**		**3**		**3**		
	Considera usted que adoptar medidas de prevención contra el delito de suplantación de identidad cibernética garantiza la seguridad jurídica y el derecho a la identidad	**3**		**3**		**3**		**3**		**3**		
	Considera usted que es deber del Estado, adoptar en	**3**		**3**		**3**		**3**		**3**		

	su política criminal medidas de prevención contra el delito de suplantación de identidad cibernética para evitar la vulneración a este derecho											

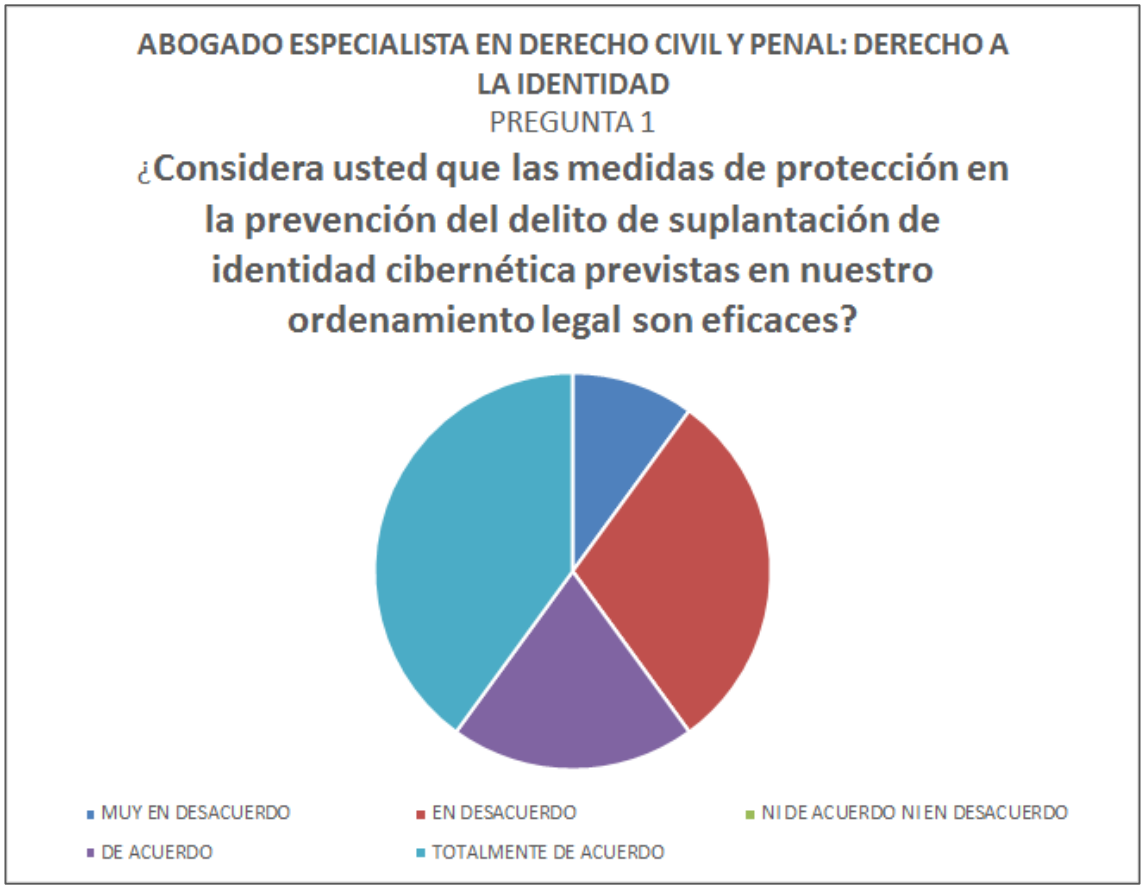
VALIDEZ DE CONTENIDO POR JUICIO DE EXPERTOS

Estimado experto, a continuación, para validar el cuestionario, debe tomar en cuenta:
A.- Los criterios de calidad: la representatividad, consistencia, pertinencia, coherencia, claridad en la redacción, de los indicadores y sus respectivos reactivos del cuestionario:

Representatividad	Consistencia	Pertinencia	Coherencia	Claridad
Es lo más representativo.	Está fundamentado en bases teóricas consistentes.	Convenientes por su importancia y viabilidad.	Los indicadores e ítems se encuentran relacionados hay correspondencia.	Redactado con lenguaje claro.

B.-Para valorar a cada indicador con sus respectivos ítems use la siguiente escala:

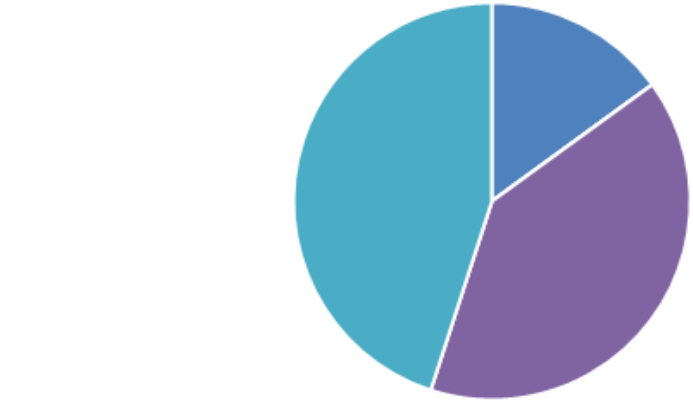
0	1	2	3
Totalmente en desacuerdo	Parcialmente en desacuerdo	Parcialmente de acuerdo	Totalmente de acuerdo



ABOGADO ESPECIALISTA EN DERECHO Y PENAL: DERECHO A LA IDENTIDAD

PREGUNTA 2

¿Considera usted que la ausencia de medidas de protección en la prevención del delito de "suplantación de identidad cibernética" vulnera el derecho a la identidad y la seguridad jurídica?

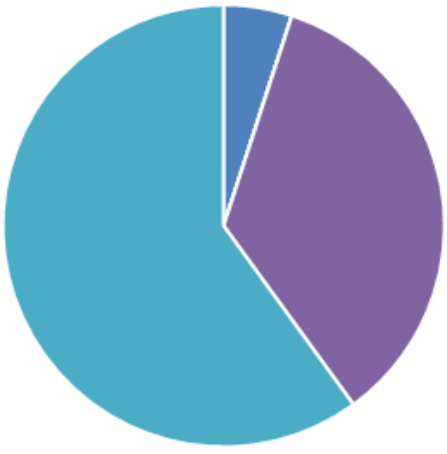


MUY EN DESACUERDO | EN DESACUERDO | NI DE ACUERDO NI EN DESACUERDO | DE ACUERDO | TOTALMENTE DE ACUERDO

ABOGADO ESPECIALISTA EN DERECHO Y PENAL: DERECHO A LA IDENTIDAD

PREGUNTA 3

¿Considera usted que la ausencia de medidas de protección en la prevención en el delito de suplantación de identidad cibernética, coadyuva al delito?

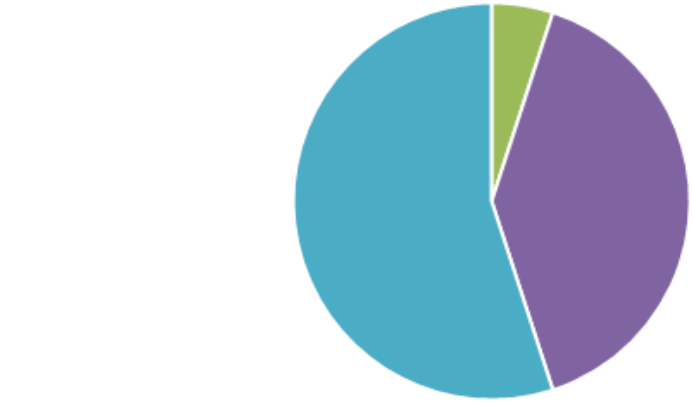


MUY EN DESACUERDO | EN DESACUERDO | NI DE ACUERDO NI EN DESACUERDO | DE ACUERDO | TOTALMENTE DE ACUERDO

ABOGADO ESPECIALISTA EN DERECHO Y PENAL: DERECHO A LA IDENTIDAD

PREGUNTA 4

¿Considera usted que deben adoptarse otras medidas de prevención contra el delito de suplantación de identidad cibernética garantiza el derecho a la identidad?

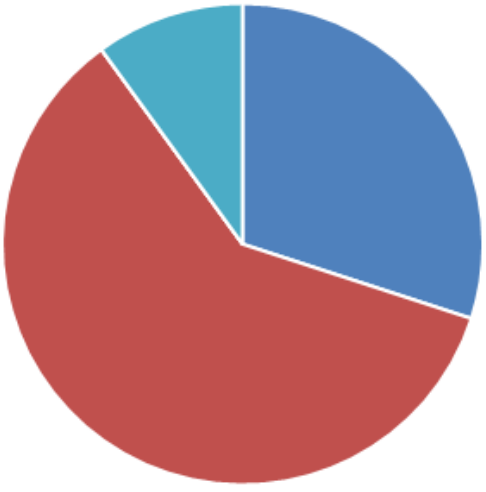


- MUY EN DESACUERDO
- EN DESACUERDO
- NI DE ACUERDO NI EN DESACUERDO
- DE ACUERDO
- TOTALMENTE DE ACUERDO

ABOGADO ESPECIALISTA EN DERECHO Y PENAL: DERECHO A LA IDENTIDAD

PREGUNTA 5

¿Considera usted que es deber del Estado, adoptar en su política criminal, medidas de prevención contra el "delito de suplantación de identidad?



- MUY EN DESACUERDO
- EN DESACUERDO
- NI DE ACUERDO NI EN DESACUERDO
- DE ACUERDO
- TOTALMENTE DE ACUERDO