Universidad Nacional
SAN LUIS GONZAGA

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"

ESCUELA DE POSGRADO

EVALUACION DE ORIGINALIDAD

CONSTANCIA

El que suscribe, deja constancia que se ha realizado el análisis con el software de verificación de similitud al **BORRADOR DE TESIS** cuyo título es:

"IMPORTANCIA JURÍDICA SOCIAL DE LA IMPLEMENTACIÓN EN LA CALIFICACIÓN Y TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN LA PROVINCIA DE ICA".

Presentado por:

RODRÍGUEZ VEGA PERPETUA EMELINA.

De la **MAESTRIA EN DERECHO mención CIENCIAS PENALES**

Que, se ha recibido del operador del programa informático evaluador de originalidad de la Escuela de Posgrado de la UNICA, el informe automatizado de originalidad, el mismo que concluye de la siguiente manera:

El documento de investigación APRUEBA los criterios de originalidad con un porcentaje de 1%.

Para dar fe, se adjunta al presente el reporte de similitud de las bases de datos de iThenticate. En Ica 11 de mayo del 2022

Atentamente

UNIVERSIDAD NACIONAL "SAN LUIS GONZAGA"
ESCUELA DE POSGRADO
Dr. ROBERTO H. CASTAÑEDA TERRONES
DIRECTOR (e) DE LA ESCUELA DE POSGRADO

UNIVERSIDAD NACIONAL “SAN LUIS GONZAGA” DE ICA

ESCUELA DE POSGRADO

TITULO

“IMPORTANCIA JURÍDICA SOCIAL DE LA IMPLEMENTACIÓN EN LA CALIFICACIÓN Y TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN LA PROVINCIA DE ICA”

TESIS

PARA OPTAR EL GRADO DE

MAESTRA EN DERECHO Y CIENCIA POLÍTICA

MENCIÓN CIENCIAS PENALES

PRESENTADO POR:

PERPETUA EMELINA RODRÍGUEZ VEGA

Ica – Perú

2021

LÍNEA DE INVESTIGACIÓN

ESTADO DE DERECHO Y DERECHOS HUMANOS

DEDICATORIA

A MI FAMILIA

AGRADECIMIENTO

A la Universidad por la oportunidad y a mi familia por el apoyo.

ÍNDICE

RESUMEN

El avance de la tecnología, como herramienta indispensable para el ser humano en su desarrollo como civilización, ha sido de gran ayuda para la realización de actividades más complejas, pero también es de resaltar que no todas las actividades humanas han venido siendo para bien de la especie como tal, sino nos hemos sumido tal como lo demuestra la historia en una dialéctica violenta entre nosotros mismos los seres humanos. Usando herramientas tecnológicas para empoderarnos sobre nuestros semejantes.

Esta constante histórica, ha sido muchas veces el motor del surgimiento de nuevas tecnologías, o la corrupción de algunas de estas para obrar delictivamente y causar daño, tanto a nivel individual o a nivel social. Es por ello que es fundamental tratar esta problemática, y que mejor que tratarla y regularla a través del derecho.

Siendo una obligación de los Estados, el de rechazar y dar las pautas permisibles y tipificar aquellas que constituyen delitos, en el que hacen los ciudadanos con la tecnología. Estas regulaciones han sido tomada y positivizadas a lo largo del mundo en los distintos estados con acceso a las nuevas tecnologías, por lo que el Perú no es una excepción, sin embargo persisten aún ciertas problemáticas al respecto, debido a que al ser aún un país en vías de desarrollo, las nuevas tecnologías se están implementando de manera progresiva, y por ende debe esta ser acompañada y regulada mediante la ley, con la finalidad de que éstas no sean empleadas para realizar actos ilícitos o sean usadas como medio delictivo.

Es por ello que hemos realizado la indagación y procesamiento de información, bibliográfica, doctrinaria y jurídica a fin de tratar este tema, elaborándose un marco teórico realizando un análisis crítico y síntesis doctrinaria sobre el derecho y las nuevas tecnologías de la información; así como también en los usos delictivos que puedan tener.

Para determinar esta problemática se realizó un diagnóstico aplicado con el levantamiento de información del área legislativa y revisión de normativa actual, revisión legislativa comparada y experiencias internacionales exitosas al respecto, recolección de datos y análisis estadístico de información judicial y de instituciones relacionadas, entrevista con usuarios para identificar problemas actuales y se aplicó la entrevista y encuesta con actores relevantes del área de justicia (jueces, fiscales y abogados).

SUMMARY

The advancement of technology, as an indispensable tool for the human being in its development as a civilization, has been a great help for the accomplishment of more complex activities, but it is also worth noting that not all human activities have been for the good of the Species as such, but we have sunk as history shows in a violent dialectic between ourselves human beings. Using technological tools to empower our peers.

This historical constant has often been the engine of the emergence of new technologies, or the corruption of some of these to act criminally and cause harm, both individually or socially. It is for this reason that it is fundamental to deal with this problem, and that better than to treat and regulate it through the law.

Being an obligation of the States, to reject and give the permissible guidelines and to typify those that constitute crimes, in which citizens do with the technology. These regulations have been taken and positiivized throughout the world in the different states with access to the new technologies, reason why Peru is not an exception, nevertheless still certain problems persist in the respect, since to the being still a country New technologies are being implemented in a progressive way, and therefore must be accompanied and regulated by law, with the purpose that these are not used to perform illegal acts or be used as a criminal means.

That is why we have done the investigation and processing of information, bibliographical, doctrinal and legal in order to address this issue, for it was developed a theoretical framework performing a critical analysis and doctrinal synthesis on law and new information technologies; As well as in the criminal uses they may have.

In order to determine this problem, an applied diagnosis was made with the collection of information from the legislative area and revision of current regulations, comparative legislative revision and successful international experiences in this regard, data collection and statistical analysis of judicial information and related institutions, interviews with users To identify current problems and applied the interview and survey with relevant actors in the area of justice (judges, prosecutors and lawyers).

MAESTRÍA EN DERECHO Y CIENCIA POLÍTICA

TITULO

"IMPORTANCIA JURÍDICA SOCIAL DE LA IMPLEMENTACIÓN EN LA CALIFICACIÓN Y TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS EN LA PROVINCIA DE ICA"

PRESENTADO POR:

PERPETUA EMELINA RODRÍGUEZ VEGA

INTRODUCCIÓN

Los hechos muestran que las computadoras son un activo valioso en casi todos los campos sociales. El uso generalizado de computadoras allanó el camino para mejoras significativas en la eficiencia y la productividad en el comercio, las comunicaciones, el mantenimiento de registros y la investigación.

Aunque la sociedad depende en gran medida de las computadoras y las redes que proporcionan, las computadoras y la información almacenada en ellas son extremadamente vulnerables a la manipulación criminal. En vista de la existencia de equipos de red en casi todos los aspectos de la vida moderna, la cantidad de información confidencial almacenada en las redes informáticas y la relativa facilidad de los delitos informáticos, la investigación de delitos informáticos requiere la atención de investigadores, policías e investigadores.

Los sitios de comercio electrónico, las tiendas de comestibles de las organizaciones hasta el almacenamiento electrónico de la información financiera de sus clientes pueden verse afectados por la pérdida o el uso indebido de la información confidencial del cliente. Independientemente de si las medidas tomadas para garantizar la seguridad de los datos son contra amenazas externas, el robo de empleados en la protección interna de la empresa causa daños. Aunque el robo de secretos comerciales o información confidencial ocurrió antes de la era de la información, la simplicidad del robo y la gran cantidad de posibles víctimas de delitos cibernéticos lo convirtieron en una gran amenaza para el mundo actual.

CAPITULO I

MARCO TEÓRICO

1.1. ANTECEDENTES

1.1.1. ANTECEDENTES INTERNACIONALES

“DELITOS COMETIDOS A TRAVÉS DE SISTEMAS INFORMÁTICOS”. Universidad Internacional del Ecuador**.**

Concluye:

El delito informático es el resultado de considerar la nocividad. La sociedad ha reconocido los derechos legales tradicionales derivados de ataques a través de las tecnologías de la información y las comunicaciones a través de legisladores. Estos derechos tradicionales son dignos de reformar la Ley Penal y considerar los delitos. Utilice la información como un activo legal protegido para evitar afectar otros activos legales tradicionales. Aunque la gente argumenta que los delitos informáticos son estrictamente un delito o una nueva forma de delito, porque son una respuesta a la sociedad y la sociedad. Los administradores del programa necesitan la impunidad de determinadas conductas en los procesos judiciales, porque sus métodos de ejecución no son tradicionales, lo que debilita la responsabilidad del infractor y evita ajustes ilimitados a este tipo, lo que evitará que la conducta sea atribuida. Es ilegal. Conducir a la impunidad

“DAÑOS INFORMÁTICOS DEL ARTÍCULO 264 DEL CÓDIGO PENAL Y PROPUESTA DE REFORMA”. Universidad Complutense de Madrid.

Conclusiones:

No cabe duda de que hoy, tanto las instituciones públicas como privadas, así como los particulares y diversos tipos de asociaciones, están destinadas a utilizar equipos informáticos y sistemas de información. Esto es inevitable. Con el desarrollo de la sociedad, parece difícil volver a la situación anterior. Nos guste o no, este es el camino que se ha decidido seguir. Sin embargo, la introducción de nuevas herramientas 356 diseñadas para hacer que la vida de las personas sea más cómoda en la sociedad significa que se pueden utilizar para terminaciones indiscutiblemente contradictorios a los que había cuando se instituyeron las personas.

La conclusión final que se extrae de la preparación de este trabajo de investigación es que se han adoptado internacionalmente las herramientas legales (e incluso policiales) apropiadas para proteger a la sociedad de nuevos tipos de delitos internacionales que son indispensables. Según nuestro orden interno. Sin embargo, aunque las leyes y normativas españolas sobre delitos de daños informáticos pueden ser suficientes en la actualidad, cumplen la mayoría de las leyes internacionales y son similares a las de los países vecinos, pueden reformularse. Nuevos principios de integración. Esta estructura textual despierta sospechas de interpretación en la gente. En este caso, debido al raro caso enviado a la corte, aún no hemos encontrado la respuesta porque este crimen conocido aún no existe.

Debido a las engorrosas regulaciones, no es difícil comprender y explicar el éxito de los nuevos problemas que surgen con el desarrollo de nuevas tecnologías. Ha habido formas de proteger a la sociedad de nuevos delitos, pero esto debe

hacerse con la máxima eficacia. Por lo tanto, sobre la base del reconocimiento de que debemos implementar medidas específicas a nivel profesional a nivel nacional e internacional, se debe alentar a las personas a continuar sus esfuerzos para mejorar mejor nuestro sistema legal relacionado con las nuevas tecnologías, especialmente en el ámbito penal. (González J. A. 2013: 355-356)

“**LOS DELITOS INFORMÁTICOS QUE AFECTAN A LOS USUARIOS DEL SISTEMA NACIONAL DE CONTRATACIÓN PÚBLICA”** “Universidad Central Del Ecuador.

Conclusiones:

En términos de aplicación, el sistema nacional de compras públicas se ha convertido en un medio eficaz para implementar un proceso de contratación que permita a las entidades públicas alcanzar metas institucionales o satisfacer sus necesidades. Esto se debe a diversas circunstancias en las que se han establecido nuevos contratos, como subastas electrónicas inversas. , El proceso de fusión con LOSNCP, utilizado para la firma de contratos de consultoría y otras normativas. Anteriormente, este proceso estaba regulado por leyes independientes, principalmente a través de la implementación y uso obligatorio de herramientas electrónicas (portales de contratación pública) para permitir su implementación de manera rápida, simplificada y transparente. El portal COMPRASPÚBLICAS siempre está en peligro, principalmente porque no cuenta con un sistema proteccionista completo y no puede establecer la seguridad regulatoria del sistema nacional de contratación pública.

Los avances en la ciencia y la tecnología nos han permitido mejorar nuestra forma de vida, pero también ha hecho posible el desarrollo y evolución de la conducta delictiva, que se encuentra rezagada en los tipos de delitos informáticos en el Ecuador, lo que lo hace vulnerable. Este tipo de delito. Ecuador cuenta con un sistema proteccionista que puede evitar delitos informáticos dispersos y desactualizados porque este delito no enfrenta las realidades técnicas de nuestras vidas, por lo que el Código Penal Integral de Ecuador no prevé un sistema que permita la expresión de este tema. La "Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos" y su reglamento promulgado a través del Addendum al Documento Oficial N ° 557 de 17 de abril de 2002, no constituyen medidas de seguridad efectivas, ni pueden establecer políticas de TI claras y obligatorias y de información remota. Sanciones, y estas sanciones se pueden aplicar junto con estas nuevas sanciones de los sistemas delictivos.

1.1.2. ANTECEDENTE NACIONAL:

“DELITOS INFORMÁTICOS EN EL PERÚ”. Universidad Nacional Mayor de San Marcos.

Conclusiones:

Este artículo estudia la propuesta de Perú para el desarrollo de un nuevo marco teórico para la delincuencia informática y la analiza como soporte científico teórico para el personal judicial (policía, fiscal y juez) y otros aspectos de la delincuencia informática. Instituciones y organizaciones dedicadas a solucionar este problema. Los marcos teóricos publicados por el INEI, Julio Núñez, Julio Téllez y Blossiers Calderón están disponibles públicamente en Internet, y estos marcos teóricos

son considerados como casos de estudio. En primer lugar, describe el estado de desarrollo del delito cibernético y cuenta con el apoyo de los principales expertos. Los temas y los métodos de investigación son la dirección de desarrollo de esta investigación. Este último primero estudió la literatura sobre el tema, luego aplicó el "método histórico" y luego entrevistó a los trabajadores judiciales sobre las opiniones de los graduados sobre los delitos informáticos.

“DELITOS INFORMÁTICOS EN EL PERÚ”. Universidad Nacional Mayor de San Marcos.

Conclusiones:

El propósito de la "Ley de Delitos Informáticos" es prevenir y sancionar actos ilegales que afecten los sistemas y datos informáticos, la confidencialidad de las comunicaciones, las violaciones de los derechos de propiedad, las creencias públicas y el uso de la tecnología de la información y las comunicaciones para lograr la libertad sexual. Según el artículo 2, los delincuentes con derechos de acceso ilícitos se clasifican como actividades puramente delictivas, pues en este acto ilícito, el acto delictivo se realiza en el mismo acto que viola las medidas de seguridad del sistema informático. El acto delictivo de intentar destruir la integridad de los datos informáticos conforme al artículo 3 se tipifica como delito puro, pues en este acto ilícito el delito se realiza introduciendo, suprimiendo, exacerbando, modificando, borrando y realizando el mismo acto de. No se puede acceder a los datos de la computadora

Según el artículo 4, los delitos que ponen en peligro la integridad de los sistemas informáticos se clasifican como delitos consecuentes porque la configuración de dichos delitos

no es suficiente para realizar las operaciones requeridas, pero los resultados posteriores son necesarios, incluido el bloqueo del acceso a la computadora ejecutora El sistema no puede funcionar o no puede prestar sus servicios. Las figuras delictivas que utilizan medios técnicos para proponer matrimonio a niños, niñas y adolescentes de acuerdo con el artículo 5 son una tendencia interna trascendente, porque trae un factor subjetivo diferente de la intención a la intención y expresa la intención especial del agente. El resultado de perseguir a la persona es obtener material pornográfico o participar en ciertos actos sexuales, por lo tanto, el número de personas se clasifica como delito de mala conducta.

1.1.3. Antecedentes Locales

No se encontraron.

1.2. BASES TEÓRICAS

2.2.1. ANTECEDENTES HISTÓRICOS DE LOS DELITOS INFORMÁTICOS.-

El primer delito informático registrado ocurrió en 1820. Esto no es sorprendente teniendo en cuenta que el ábaco (considerado la forma más antigua de computadora) existe desde el 3500 a. C. C. En India, Japón y China. Sin embargo, la era de la informática moderna comenzó con el motor de análisis de Charles Babbage. En 1820, un fabricante textil francés Joseph-Marie Jacquard produjo un telar. Este equipo permite repetir una serie de pasos para tejer tejidos especiales. Esto hace que los empleados de la empresa de jacquard se preocupen de que sus trabajos tradicionales y sus medios de vida se vean amenazados. Realizaron actividades de sabotaje para evitar

que la máquina jacquard siguiera utilizando la nueva tecnología. Este es el primer delito informático registrado

Se registró una amplia variedad de delitos a principios del siglo XX, incluido el descifrado del código Morse y el envío de mensajes insultantes para descifrar números misteriosos. Con la llegada de las computadoras a fines de la década de 1960, los delitos se relacionaron principalmente con daños físicos a las computadoras y las redes telefónicas. Estos casos involucraron la destrucción de computadoras, principalmente en los Estados Unidos, como el bombardeo de Wisconsin en 1970, que destruyó $ 16 millones en datos informáticos. La década de 1970 dio lugar a delitos más sensacionales, como el caso Blue Box de John Draper, al que llamó sin cargo y publicó un libro en línea. Durante un período de tiempo, con el continuo desarrollo de la tecnología relacionada con los sistemas informáticos, la naturaleza y el color de los delitos también han cambiado.

En la década de 1980, los piratas informáticos fueron pirateados, por ejemplo, las computadoras de AT&T fueron pirateadas, lo que cambió el ciclo de facturación y proporcionó a los consumidores precios preferenciales. En 1982, nació el primer virus Applell. Se inventó un "gusano" de código de computadora autorreplicante como código Morris, que paralizó 6.000 computadoras antiguas en la red del gobierno de Estados Unidos. El fraude con tarjetas de crédito comenzó en la década de 1990 y causó enormes pérdidas financieras a las empresas financieras. El robo de identidad comienza a exponer lugares donde las personas se hacen pasar por otra persona para visitar u obtener algo que alguien no tiene derecho a obtener. Las computadoras de hoy han recorrido un largo

camino. Se espera que las redes neuronales y la nanocomputación transformen cada átomo de un vaso de agua en una computadora que pueda realizar billones de operaciones por segundo.

El delito informático es un delito derivado de la creciente dependencia de las computadoras en la vida moderna. En esta época, cuando todo, desde hornos microondas y refrigeradores hasta plantas de energía nuclear, funciona en computadoras, el ciberdelito tiene un impacto bastante malo. Los principales delitos cibernéticos recientes incluyen el robo de Citibank. Se transfirieron fraudulentamente $ 10 millones del banco a una cuenta bancaria en Suiza. Un grupo de hackers rusos liderados por el famoso hacker Vladimir Kevin llevó a cabo el ataque. La organización destruyó el sistema de seguridad del banco. Aparentemente, Vladimir irrumpió en la computadora Citibank en la computadora de la oficina de la compañía de computadoras AO Saturn en San Petersburgo, Rusia. Finalmente fue arrestado en el aeropuerto de Heathrow cuando se dirigía a Suiza.

1978: Spam

El primer correo electrónico no deseado fue enviado por el director de marketing de Digital Equipment Corp. a través de ARPAnet en la red del Departamento de Defensa de EE. UU. En 1978. Hoy en día, una gran cantidad de correos electrónicos se envían a través de varios canales (correos electrónicos, grupos de noticias, mensajería instantánea, teléfonos móviles). No son necesarios y el destinatario no se puede eliminar de la lista de correo. El spam se ha vuelto más malicioso porque los delincuentes lo han convertido en una herramienta para una gran cantidad de estafas

1982: Virus

Un estudiante de secundaria llamado Rich Skrenta escribió un "clon de alce" para la computadora Apple II. Escondido en el disquete que se usa para cargar el sistema operativo en la computadora, cuando el usuario, sin saberlo, comienza con el disquete infectado, el disquete se desmorona. Los virus informáticos son programas informáticos que pueden replicarse e infectar equipos. Cuando el host del virus llega a la computadora de destino, puede propagarse de una computadora a otra (en alguna forma de código ejecutable). Por tanto, el virus se propagará cuando el usuario lo envíe o lo lleve a través de la red o Internet.

1988: Gusanos

El estudiante graduado de la Universidad de Cornell, Robert T. Morris, desarrolló un software que se puede copiar automáticamente en una computadora conectada a ARPAnet (Pionero de Internet) del gobierno. Un gusano informático es un programa informático autorreplicante que envía copias de sí mismo a otros nodos a través de la red. A diferencia de los virus informáticos, no es necesario que se conecte a programas existentes. Los gusanos casi siempre causan al menos algo de daño a la red, o incluso solo ocupan ancho de banda, mientras que los virus casi siempre dañan o modifican archivos en la computadora de destino.

1989: El software del caballo de Troya

En 1989 (o 1987, dependiendo de con quién esté hablando), se envió un disquete, que se suponía que era una base de datos de información sobre el SIDA, a miles de investigadores del SIDA y suscriptores del British Computer Journal. Un programa

de caballo de Troya es un programa destructivo que dice ser una aplicación benigna y lleva el nombre de un programa de caballo de Troya en la mitología griega. Antes de la instalación y / o ejecución, el software parece inicialmente realizar las funciones requeridas por el usuario, pero puede robar información o dañar el sistema. A diferencia de los virus o gusanos, los programas de caballo de Troya no se replican

Crimen de los años 90

Esto evolucionó de una broma. Una broma es una pieza de software. Si abre un correo electrónico infectado, se instalará un mensaje estúpido en la pantalla de su computadora.

1996: Phishing

Las necesidades de los delincuentes organizados en Internet han producido muchos paquetes de software malintencionado que son fáciles de descargar. El phishing intenta engañar a los usuarios de Internet para que divulguen su información personal para que los delincuentes la utilicen o la divulguen. El phishing también se conoce comúnmente como ingeniería social y generalmente contradice a los usuarios a través de correos electrónicos aparentemente reales que se vinculan a sitios web que imitan instituciones financieras o minoristas respetados. El spear phishing se creó diez años después, es una estafa en línea más compleja dirigida a personas u organizaciones.

1998: Man-in-the-middle ataque

La Agencia de Seguridad Nacional informó que un hombre fue atacado en 1998, pero el ataque más famoso ocurrió en octubre de 2005, cuando los bancos globales fueron atacados. El intermediario se basa en la interceptación y existe desde el

nacimiento del espía. Sin embargo, la tecnología le ha dado un nuevo impulso. Es tan simple como monitorear el correo electrónico de alguien a través de Wi-Fi sin cifrar en un cibercafé. Los ataques más maliciosos utilizan sofisticados programas de caballo de Troya para interrumpir las transacciones bancarias y robar miles de millones de dólares. MITM se ha convertido recientemente en la persona más hostil en el navegador. El malware acecha en el navegador de la víctima, que se lanzó en 2003 y Facebook se lanzó en 2004, anunciando una nueva era de las redes sociales. Este medio fue rápidamente colonizado por delincuentes, hasta que se convirtió en una forma de negocio exitosa, hasta que pasó con éxito el proceso de autenticación.

Los 00: los sitios de redes sociales despegan

Mi espacio es el canal principal para difundir malware y ataques de ingeniería social. 2000: Denegación de servicio y ataques distribuidos de denegación de servicio. Los piratas informáticos canadienses de la mafia lanzaron un ataque distribuido de denegación de servicio, destruyendo muchos sitios web conocidos, incluidos Amazon, CNN y Yahoo !. Los ataques AD (D) o S hacen que los usuarios objetivo no puedan usar los recursos informáticos (generalmente sitios web). Un método de ataque común es llenar la computadora de destino con solicitudes de comunicación externa para que no pueda responder al tráfico legítimo o responder. Lentamente, no se puede hacer de manera efectiva

2003: Botnets

El gusano de correo electrónico SoBig se considera el primer intento organizado de crear una gran botnet. Una botnet es una colección de equipos o robots infectados que están ocupados

por piratas informáticos y que se utilizan para realizar tareas o funciones maliciosas. Cuando una computadora descarga un archivo incrustado con un software bot, se convierte en un bot.

Julio 2010: Stuxnet

La botnet puede tomar medidas sin que el pirata informático tenga que iniciar sesión en la computadora del cliente. En julio de 2010, se descubrió un gusano informático de Microsoft Windows dirigido a computadoras y software industriales.

2011: Amenaza Persistente Avanzada (APT)

Este es el primer malware descubierto para monitorear y destruir sistemas industriales. Es un acrónimo de todos los profesionales de la seguridad de redes. APT generalmente se refiere a un grupo que tiene la capacidad y la intención de perseguir de manera efectiva un objetivo específico de una entidad, como un gobierno extranjero.

1.2.2. LOS DELITOS INFORMÁTICOS O CIBERNÉTICOS.-

Los técnicos, policías, abogados, criminólogos y expertos en seguridad nacional tienen diferentes entendimientos del concepto de "ciberdelito". El ciberdelito se refiere al derecho, la sociología, la tecnología, el derecho o el crimen, y las definiciones generales aún son esquivas (Kshetri, 2010), lo que se está volviendo más claro. Los analistas intentan enmarcar las características básicas del ciberdelito con poco consenso (Gordon y Ford, 2006; Snyder, 2001; Wall & Williams, 2001; Yar, 2005). Las definiciones actuales varían ampliamente, dependiendo del instrumento legal u organización que define el término (Pocar, 2004). El abuso de la tecnología de la información por parte de los delincuentes se denomina indistintamente delito cibernético, delito informático, abuso

informático, delito informático, delito de alta tecnología, delito electrónico, delito tecnológico, etc.

El principio básico de la mayoría de los sistemas legales es el principio de "no culpable y no culpable", es decir, no importa cuán dañino sea el comportamiento, no se permite el enjuiciamiento a menos que esté prohibido por la ley formal (Grabosky, 2007; Tikk, 2011) . A los efectos de esta investigación, los siguientes elementos deben clasificarse como ciberdelincuentes:

• La tecnología de la información y las comunicaciones facilita este comportamiento;

• El comportamiento está motivado para dañar a un individuo u organización;

• El daño causado o causado intencionalmente incluye el comportamiento que interfiere o daña cualquier propiedad tangible o intangible propiedad de un individuo u organización; ÿ

• El acto generalmente se lleva a cabo dentro de la jurisdicción de la víctima o dentro de la jurisdicción del acusado. Según esta definición, la ciberdelincuencia es solo un subconjunto de la delincuencia tradicional, en la que las TIC se utilizan como herramienta o herramienta.

Esta definición sigue la base de la interpretación jurídica aplicable a los delincuentes tradicionales. Los legisladores deben ser conscientes de que modificando la ley para adaptarla a los cambios tecnológicos, se puede evitar la creación de categorías legales de delitos informáticos "especiales". Los teóricos de Internet creen unánimemente que el ciberespacio puede realizar el acceso instantáneo y la interacción entre individuos en el espacio remoto, creando así

la posibilidad de nuevas formas de contacto, que a su vez conducirán al ciberdelito y la transferencia de redes. En resumen, el ciberdelito es un delito promovido o cometido con la ayuda de equipos informáticos o Internet (Kshetri, 2010). La computadora o dispositivo puede ser el agente del crimen, el iniciador del crimen o el objetivo del crimen.

1.2.3. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS.-

1.2.3.1 Delitos Informáticos Violentos:

El ciberdelito violento es un delito que representa un peligro personal para cualquier persona. Se clasifican de la siguiente manera: a) Ciberterrorismo El aumento de las actividades en Internet también ha dado lugar a un nuevo tipo de delito cibernético denominado “ciberterrorismo”. Como implica el término "ciberterrorismo", es básicamente una fusión entre el ciberespacio y el terrorismo. Sin embargo, la comprensión tradicional del terrorismo representa una forma diferente de comportamiento delictivo, que se caracteriza por una combinación de violencia y política. Estados Unidos ha tomado la iniciativa de formular disposiciones legales para proteger los sistemas informáticos estadounidenses de ataques terroristas, y el 11 de septiembre de 2001 se dirigieron a Nueva York y Washington.

Las organizaciones terroristas brindan muchas ventajas para los ataques virtuales. Internet permite la operación remota. Otra ventaja (que ha demostrado ser mala para la sociedad) es que requiere recursos limitados, y las finanzas y los materiales son multiplicadores de poder. Al usar un proxy, el anonimato en Internet es muy fácil, por lo que es difícil rastrear el origen del ataque. Alguien señaló que uno de los mayores desafíos que

plantea el delito cibernético a los mecanismos de aplicación de la ley es la medida en que el entorno de Internet proporciona a los delincuentes anonimato u ocultación.

b) **El acecho cibernético.**

Este es un tipo de delito informático en el que el atacante utiliza comunicaciones electrónicas para acosar a la víctima. En algunos casos, el ciberacoso se originó en el acecho en el mundo real y seguirá existiendo en Internet. El acoso es un problema familiar para muchas personas (especialmente las mujeres) en la vida real. Este problema que ocurre a través de Internet se llama "acecho cibernético", que incluye acoso, insultos e insultos a las víctimas. El rastreo en línea también puede causar lesiones personales en línea. El ciberacoso es causado por el odio, la ira, la venganza, los celos, la obsesión y la enfermedad mental. El acoso cibernético es una extensión del acoso físico. Tiene dos formas: abierta y oculta. El acoso público es una forma de agresión personal, que incluye golpes, patadas y contacto sexual. La intimidación pública suele ir acompañada de intimidación secreta. En este caso, la víctima es excluida del grupo de amigos por chismes, acoso verbal y amenazas.

c) La Pornografía.

Puede acceder fácilmente a Internet a través de computadoras, PDA, teléfonos inalámbricos, teléfonos móviles, etc. A fines de la década de 1970 y principios de la de 1980, los programadores estaban interesados en desarrollar software que permitiera la transmisión, reordenación y visualización de imágenes a través del sistema Usenet. En 1996, cinco de los diez grupos más populares en Usenet eran pornográficos, y uno de ellos (atl.Sex.Net) atraía aproximadamente a 5 millones

de lectores cada día. Inesperadamente, la pornografía fue el primer producto de comercio electrónico exitoso.

1.2.3.2. Delitos Informáticos No Violentos:

El ciberdelito no violento no causará ningún daño físico a las personas, no causará pérdidas económicas, angustia psicológica o daño social. Se clasifican de la siguiente manera:

a) El robo cibernético.

El robo cibernético es una forma de robar dinero o información utilizando computadoras e Internet. Este es también el delito cibernético más popular porque la capacidad de robar a distancia reduce el riesgo de detección. El robo cibernético incluye la malversación de fondos públicos por Internet. -El uso indebido de fondos en línea se refiere al uso indebido o la modificación de datos por parte de los empleados de la empresa que tienen acceso legal a los sistemas y redes informáticos de la empresa. Ejemplo: un empleado abusó del sistema de salarios informáticos de la empresa, lo que le hizo recibir una compensación adicional

Malversación. -El individuo obtiene un método de transferencia de fondos y modificación de documentos desde fuera de la organización para que pueda tener derechos legales sobre bienes que no le pertenecen. La diferencia entre la malversación y la malversación de fondos es que los delincuentes no están interesados en objetos de valor, pero pueden usar estos fondos y transferir o modificar cierta información. • Espionaje corporativo. -En este delito, personas dentro / fuera de la empresa utilizan Internet y roban estrategias de marketing, secretos comerciales, datos

financieros, listas de clientes, etc. Obtenga una ventaja competitiva. En espionaje industrial o industrial, persona que utiliza la red de la empresa para robar secretos comerciales, datos financieros, listas de clientes confidenciales, estrategias de marketing o cualquier otra información para obtener una ventaja competitiva.

b) Los fraudes cibernéticos.

Otra forma de ciberdelito que domina firmemente a la sociedad es el fraude en línea y el fraude en línea. Sin embargo, el problema con esto es la falta de datos oficiales sobre el sistema. Internet ofrece valiosas oportunidades para que los delincuentes se oculten a sí mismos y a sus identidades. Estos estafadores también cambian atributos personales, como edad, género, raza, país de residencia, etc. Aunque se detecta el fraude, todavía es difícil identificar al culpable. Las víctimas de fraude en línea pueden ser reacias a denunciar la identidad de la víctima por las siguientes razones: relativamente hablando, el dinero insignificante no vale la pena resolverlo. Es vergonzoso denunciar el fraude, el desconocimiento de la notificación de la infracción a las autoridades competentes, porque el estafador está en otro país / región, este resultado es poco probable. (zhigang, Y, 2011)

c) Traspaso Cibernético (hacking).

En términos de cibernética, los delincuentes pueden inmiscuirse en computadoras o redes sin autorización, pero no deben abusar de ellas. Por ejemplo, un pirata informático adolescente hackeó la red solo para probarse a sí mismo ante sus compañeros o verlo como un desafío. A estos intrusos les gusta leer los correos electrónicos de otras

personas, pero no utilizan la información que encuentran. Sin embargo, en la mayoría de los países, el ciberdelito es un delito. El ciberdelito es más dañino para la sociedad que el crimen tradicional. Los piratas informáticos hacen esto por curiosidad, para aprender libremente, con el propósito de descubrir y compartir el descubrimiento con otros, y con el propósito de destruir deliberada o involuntariamente el sistema. Seguramente no serán capturados por piratas informáticos por las siguientes razones; debido a que no conocen la jurisdicción del mundo en línea, pocas víctimas están interesadas en presentar denuncias.

d) Otros delitos cibernéticos no violentos.

Muchos delitos cibernéticos no violentos incluyen la prostitución en línea, los juegos de azar, la venta ilegal de drogas en Internet y el lavado de dinero en línea.

• Prostitución online: Implica participar en actividades de prostitución online a través de diversos anuncios en el sitio web. • Juegos de azar por Internet: se refiere a los clientes que utilizan tarjetas de crédito en línea para realizar apuestas en casinos virtuales.

• Venta de medicamentos a través de Internet: las farmacias en línea venden medicamentos a clientes que no pueden comprarlos a través de distribuidores públicos o privados.

• Blanqueo de dinero en línea: esto significa utilizar Internet para ocultar fondos ilegales. La banca en línea brinda a los delincuentes la oportunidad de abrir cuentas bancarias en el extranjero y realizar transferencias bancarias. Después de dar el marco conceptual y la clasificación del ciberdelito, es necesario comprender los factores y motivos detrás del ciberdelito.

1.2.4. MARCO LEGAL PERUANO CONTRA LOS DELITOS INFORMÁTICOS.-

De acuerdo con la Ley No. 27309 emitida el 17 de julio de 2000, se agregó un nuevo capítulo (Capítulo 10) al Título V, que incluye tres artículos (207 ° -A, 207 ° -B y 207 ° C). Intentos de actualización de la normativa interna relacionada con los nuevos avances tecnológicos, este hecho es coherente con las últimas normativas sobre fenómenos informáticos:

INTRUSISMO y/o ESPIONAJE (Art.207-A del C.P.)

"Art. 207-A.- el que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de ciento cuarenta y dos a ciento cuatro jornadas".

Si el mandatario actúa para obtener beneficios económicos, será sancionado con pena privativa de libertad no mayor de tres años ni menor de ciento cuarenta días de servicio comunitario.

EL SABOTAJE INFORMÁTICO (Art. 207-B DEL C.P.)

"Art.207- B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setena a noventa días-multa".

MODALIDAD AGRAVADA. (Art. 207-C DEL C.P.)

“Art. 207-C.- En los casos del artículo 207-A y 207-B, la pena será privativa de libertad no menor de cinco años ni mayor de siete años”, cuando:

El agente utiliza la información privilegiada obtenida en función de su ubicación para acceder a la base de datos, el sistema informático o la red. 2) La inclusión del ciberdelito por agentes que atenten contra la seguridad nacional del Perú es el artículo 5071/99 de su más reciente ley. El proyecto fue propuesto por el congresista Jorge Muñiz y propuso que el Capítulo 11 se incluyera en el Título V (Sobre Derechos de Herencia). Crime) - Similar al texto actual, que contiene ilustraciones. Sin embargo, debido a los comentarios de la administración, se han realizado algunos cambios en 208-A y 208-B, y estos cambios se reflejan en el informe técnico actual. C.P.208-A, B y C

1.2.5. LEGISLACIÓN COMPARADA SOBRE LOS DELITOS INFORMÁTICOS.-

Es necesario realizar un estudio comparativo de la realidad computacional de Estados Unidos y otros países europeos. Estos países incluyen:

América del Norte América

El país aprobó la "Ley Federal de Abuso de Computadoras" en 1994 (Artículo 1030, Título 18 del Código de Regulaciones Federales de los Estados Unidos), que modificó la "Ley de Abuso y Fraude Informático" de 1986. Su propósito es eliminar el debate subcutáneo sobre qué es un virus y qué no es un virus. Programas de virus, gusanos y caballos de Troya. Y debido a que son diferentes a los virus, la nueva ley prohíbe la

transmisión de programas, información, códigos o comandos que puedan dañar computadoras, datos o programas (1. USC: Artículo 1030). La nueva ley es una mejora porque resiste directamente la propagación del virus.

- **CHILE**

Este es el primer país latinoamericano en clasificar a los delincuentes informáticos bajo la Ley N ° 19.223. La ley contra los delitos informáticos entró en vigor el 7 de junio de 1993. Según la ley, el acto de destruir o inutilizar los datos contenidos en la computadora será sancionado con pena privativa de la libertad de un año y medio a cinco años. Además, teniendo en cuenta estos factores, existe un virus, y las siguientes disposiciones dotan a la ley de los siguientes conocimientos:

Artículo 1º.- "El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o sus componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada, en su grado máximo".

Artículo 2º.- "El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado medio".

- **ARGENTINA**

En su legislación comercial y penal, el país ha establecido las siguientes disposiciones sobre comportamientos informáticos ilegales:

“La ley 24.766 llamada de confidencialidad de datos, que tutela la información que importe un secreto comercial. La ley 25.326, llamada de hábeas data, que tutela la información de carácter personal almacenada en archivos de datos”.

“La ley 11.723 (Propiedad Intelectual), con la modificación hecha por la ley 25.036 que amplía la tutela legal a las obras de computación fuente y objeto; la ley de Marcas 22.362 y la de patentes 24.481”.

- **ESTADOS UNIDOS MEXICANOS**

El Código Penal de México aprobó una reforma publicada en el Diario Oficial de la República Federal Hacker, atacando sistemas informáticos que pueden o no pertenecer al sector financiero mexicano. Esta agencia reguladora federal está sancionada. En esta agencia, los sujetos tienen derecho a acceder ilegalmente al sistema y cambiar, dañar, modificar o hacer que se pierda la información contenida en el sistema. Para ello se suelen utilizar los siguientes artículos:

Artículo 211 bis 1.- “Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa”.

- **COLOMBIA**

El “Reglamento” del país se publicó en la Ley Nº 599 de 2000 y no menciona explícitamente los delitos cibernéticos. Sin embargo, en algunas de sus normas, el comportamiento contenido en él puede entenderse como el concepto contenido en esta doctrina. De acuerdo a la Ley No. 679-2001 publicada en el Diario Oficial 44509 el 4 de agosto de 2001, "Disposiciones para Prevenir y Combatir la Explotación de Menores, Pornografía y Turismo Sexual". En el Capítulo 2

menciona la red global, cuyo propósito es dictar medidas de protección contra la explotación menor, la pornografía, el turismo sexual y otras formas de abuso sexual mediante el establecimiento de medidas preventivas y punitivas y la promulgación de otras disposiciones. Según el artículo 44 de la Constitución

- **VENEZUELA**

El 30 de octubre de 2001 se publicó en el Boletín Oficial de la República Bolivariana la Ley No. 48 "Ley Especial para Combatir Delitos Informáticos". Esta ley representa un gran avance en materia penal y permitirá que la protección de la tecnología de la información procese a todos los infractores. En el sitio

.

1.3. MARCO CONCEPTUAL

BIEN JURÍDICO.-

Es cualquier persona protegida por la ley, ya sea material o no material. Una persona que resulta lesionada por un delito informático y busca defensa.

CIBERNÉTICA.-

Es una ciencia interdisciplinaria que involucra sistemas de comunicación y control en organismos vivos, máquinas y organizaciones. El término cibernética se originó a partir de Kilney (timonel o gobernador) en Grecia. El desarrollo de la cibernética es el estudio de tecnologías que pueden cambiar la información de rendimiento requerida

COMPUTADORA.-

Es una máquina electrónica capaz de procesar información. Antes de la electrónica, eran mecánicos o electromecánicos.

COMPUTADORA U ORDENADOR.-

Es un dispositivo electrónico que puede recibir un conjunto de instrucciones y realizar cálculos sobre datos digitales, o ejecutar estas instrucciones compilando y correlacionando otros tipos de información.

CRACKING.-

Este es el propósito del acceso no autorizado al sistema con el propósito de destruir información; las personas que realizan estas operaciones se denominan "mentirosos", el término proviene del término "crack", que significa destruir algo o descifrar un código, que es un secreto.

CRIMINALIDAD INFORMÁTICA.-

Debido al desarrollo tecnológico y social, es un fenómeno en constante cambio en el campo nuclear manipular computadoras para obtener una propiedad heredada que sea beneficiosa para el autor o un tercero. (Tiedeman).

DELITO INFORMÁTICO.-

Son delitos cometidos en el ciberespacio, al igual que en el mundo virtual, los defectos humanos, el dolor y los malos hábitos son tan fáciles de replicar como las virtudes. El efecto aldea pública que genera la red y la proliferación de nodos en todo el planeta promueven la difusión instantánea de mensajes y permiten el acceso a cualquier información ingresada en la red.

DELITO COMPUTACIONAL.-

Existe una clara distinción entre el delito cibernético y el delito cibernético. Sin embargo, ambos forman parte del mismo fenómeno delictivo y el nombre correcto es "delito a través de una computadora".

DELITO CONTRA EL HONOR.-

El honor es parte de la ética personal de verse a uno mismo a través de los ojos de los demás.

DELITOS DE ESPIONAJE INFORMÁTICO.-

Se refieren principalmente a la obtención de resultados de investigación, direcciones de clientes, etc. Estas operaciones se pueden lograr mediante la introducción de un programa de copia u otros métodos (la radiación electrónica emitida por el terminal de la computadora se encuentra aproximadamente a un kilómetro del lugar de instalación).

DELITO INFORMÁTICO.-

Son la actitud ilegal de tratar la computadora como una herramienta o propósito (concepto atípico), o el comportamiento típico, ilegal y criminal de tratar la computadora como una herramienta o propósito (concepto típico).

ESPIONAJE INFORMÁTICO.-

Es cuestionable si el número de "robos" requiere la privación permanente de bienes o propiedad. La víctima cumplió con este procedimiento penal.

ESTAFAS INFORMÁTICAS.-

Son la actitud ilegal de tratar la computadora como una herramienta o propósito (concepto atípico), o el comportamiento típico, ilegal y criminal de tratar la computadora como una herramienta o propósito (concepto típico).

SABOTAJES INFORMÁTICOS.-

Tratándose de aquellas actividades dirigidas a inhabilitar temporal o permanentemente, parcial o totalmente a los medios informáticos, se pretende destruir la capacidad de producción de las empresas

propietarias de estos medios o instituciones públicas, que es el objeto de la presente investigación.

SISTEMAS INFORMÁTICOS.-

Es un grupo de dispositivos que colaboran para realizar tareas. En informática, los sistemas de escritura se utilizan en varios entornos

TECNOLOGÍAS.-

En términos generales, se aplican los procesos mediante los cuales las personas diseñan sus herramientas y sus máquinas

CAPITULO II

PLANTEAMIENTO DEL PROBLEMA

2.1. SITUACIÓN PROBLEMÁTICA

La "Ley de Delitos Informáticos" no es aplicable porque la autoridad judicial competente ha realizado el descifrado y verificación de calificación. El avance de la tecnología es vital para la ley. Con el profundo desarrollo de la informática jurídica en el mundo, varios campos que involucran a la sociedad y las relaciones legales se enfrentan a cambios tremendos en muchos aspectos, y estos cambios aumentan constantemente. En cuanto al tema del desarrollo adecuado, podemos referirnos a los campos del derecho, las relaciones comerciales y la administración pública. Ante tales incidentes, nadie sospecha que el fenómeno informático provocará confusión entre distintos departamentos, como derechos, litigio civil, civil y mercantil. Ante tales incidentes, nadie sospecha que el fenómeno de las tecnologías de la información generará confusión entre diferentes departamentos, como derechos, litigio civil, civil y mercantil.

Hoy en día, los problemas que genera este fenómeno hacen necesario recurrir al derecho penal para prevenir el mal uso de las computadoras, lo que se ha reflejado en una serie de leyes extranjeras. De hecho, "En la actualidad, la expansión de las tecnologías de la información y las redes (como Internet) ha llegado a la vida cotidiana de personas y organizaciones. La importancia de su progreso para el desarrollo del país pone a las personas en gran peligro. Porque están almacenados en múltiples sistemas informáticos, el crecimiento y diversificación de la información hace necesario tomar las medidas legales que se han tomado, pero hasta

ahora estas medidas están lejos de ser suficientes. Facebook, etc.) delitos derivados; considerar solo delitos informáticos, y en algunos casos, quiebra de medios.

2.2. FORMULACIÓN DEL PROBLEMA

"La Inaplicación De La Ley Sobre Delitos Informáticos, Mediante La No Calificación Y Tipificación Por Los Órgano Jurisdiccional Competentes Traen Consigo la Ineficiencia Para El Juzgamiento De Acuerdo A La Legislación que la Comprende".

PROBLEMA GENERAL

La inaplicación de la ley sobre delitos informáticos, mediante la no calificación y tipificación por el órgano jurisdiccional competentes trayendo como consecuencia el juzgamiento como delitos comunes.

PROBLEMA ESPECÍFICOS

De qué manera la inaplicación de la ley influye sobre los delitos informáticos, mediante la no calificación y tipificación por el órgano jurisdiccional competentes trayendo como consecuencia el juzgamiento como delitos comunes

DELIMITACIÓN DE PROBLEMA

Dentro de las limitaciones encontramos la escasa información en cuanto a nuestra investigación.

2.3. JUSTIFICACIÓN E IMPORTANCIA

2.3.1. JUSTIFICACIÓN

En nuestra investigación, esto es razonable, porque constituye un tema no revelado y muy importante para nuestro país, la relevancia no es alta. Por eso es importante saber aplicarlo de acuerdo con la normativa de nuestro país.

2.3.2. IMPORTANCIA

La aplicación de esta regla es importante porque este tipo de delitos deben ser juzgados en función de su naturaleza y no de los delitos ordinarios, por lo que estos delitos son minoritarios. La importancia de esta investigación radica principalmente en la verificación, existiendo una falta de vínculos estrechos entre la aplicabilidad de la teoría, el derecho, el ciberdelito y la verificación, y las posibles soluciones propuestas en las conclusiones de la investigación doctrinaria. Estos resultados nos ayudarán a lograr un trabajo conjunto presencial. En su caso, nos aseguraremos de que todas las partes relacionadas con las escuelas de posgrado, derecho, sociedad, empresas privadas e instituciones públicas conozcan e instalen redes informáticas, especialmente la primera porque corresponde a la jurisdicción de Ica, pero por su Importancia deben ser extenderse a otras partes de nuestra sociedad

2.4. OBJETIVOS DE LA INVESTIGACIÓN

2.4.1. OBJETIVOS GENERALES

En nuestro distrito judicial se de paso a la implementación, capacitación y ejecución en los diferentes órganos encargados

de la investigación y juzgamiento de los delitos informáticos en sus diferentes modalidades en la provincia de Ica

2.4.2. OBJETIVOS ESPECÍFICOS

En nuestro distrito judicial se de paso a la implementación, capacitación y ejecución a nivel policial, ministerio público y poder judicial sobre investigación y juzgamiento de los delitos informáticos en sus diferentes modalidades en la provincia de Ica.

2.5. HIPÓTESIS

2.5.1. HIPÓTESIS GENERAL

Existe una relación directa entre la inaplicación de la ley sobre delitos informáticos, mediante la no calificación y tipificación por los órgano jurisdiccional competentes traen consigo la ineficiencia para el juzgamiento de acuerdo a la legislación que la comprende

2.5.2. HIPÓTESIS ESPECÍFICAS

De que manera la inaplicación de la norma influye en los delitos informaticos.

2.6. VARIABLES

2.6.1. **Identificación de variables**

VARIABLE INDEPENDIENTE (Vx):

DELITOS INFORMÁTICOS

VARIABLE DEPENDIENTE (Vy):

INAPLICACIÓN DE LA NORMA

2.6.2. OPERACIONALIZACION DE VARIABLES

VARIABLES	TIPO	NATURALEZA	ESCALA	DIMENSIONES	INDICADORES	FUENTE
(X) **DELITOS INFORMÁTICOS**	Variable Indepen-diente	Variable Cualitativa	Nominal	Robos electrónicos Sabotaje Informático Criminalidad Informática. Terrorismo Informático.	Sistemas Informáticos Tecnologías Informáticas. Actividades Ilícitas.	- Encuesta. - Entrevista - Análisis Documental
(Y) **INAPLICACIÓN DE LA NORMA**	Variable Depen-diente.	Variable Cualitativa	Nominal	Manipulación Informática Comportamiento delictivo	Problemas Criminológicos. Problemas Penales	- Encuesta. - Entrevista. - Análisis Documental

CAPITULO III

METODOLÓGICA DE LA INVESTIGACIÓN

3.1. TIPO, NIVEL Y DISEÑO DE INVESTIGACIÓN

3.1.1. **Tipo**

Se utilizará una Investigación de tipo Básica, porque se incrementaran los conocimientos científicos y filosóficos, pero sin contrastarlos con ningún aspecto práctico las respectivas variables.

3.1.2 Nivel.-

Sera un trabajo con un Nivel Explicativa por que trataremos de poder dar respuesta sobre los objetivos objeto que se investigan.

3.1.3 Diseño.-

El diseño de la investigación corresponderá al Tipo no experimental – Explicativo Correlacional, porque la responsable no manipulara las Variables Independiente: Delitos Informáticos; pero si evaluó y explicó sus efectos en otra variable – Variable Dependiente: Legislación peruana.

3.2. POBLACIÓN – MUESTRA

La investigación estará compuesta por 184 de la población y universo los Actores Jurídicos con competencia para tener conocimiento sobre los delitos Informáticos, y la problemática que trae para la aplicación en el derecho penal peruano en los sistemas judiciales peruano.

CAPITULO IV

TÉCNICAS E INSTRUMENTOS DE INVESTIGACIÓN

4.1. TÉCNICAS DE RECOLECCIÓN DE DATOS

TÉCNICA DE LA ENCUESTA: Esta técnica se utilizó, mediante la recolección de información, de todos quienes se encuentran involucrados dentro del tema que se investiga.

- Cuestionario.

TÉCNICA DE LA OBSERVACIÓN: Realizada mediante la concurrencia del investigador al archivo central.

- Ficha de Registro.
- Grabaciones Fotografías.

TÉCNICA DOCUMENTAL: Recopilación de información a través de instrumentos.

- Recopilación de información a través de los instrumentos.

4.2. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Los instrumentos utilizados serán:

- Fichas de análisis de documental
- Ficha de recojo de información
- Formulario de entrevista
- Informes

4.3. TÉCNICAS DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Codificación y clasificación de datos: Nos permitió ordena y agrupar numéricamente los datos que se obtendrán.

Tabulación de datos: Procesamiento de la información.

Cuadros y representaciones estadísticas: Representación gráfica de los resultados.

CAPITULO V

CONTRASTACIÓN DE HIPÓTESIS

Prueba de hipótesis especifica 1:

Hi: Existe una relación directa entre los Delitos Informativos y la inaplicación de la norma.

Ho: No existe una relación directa entre los Delitos Informativos y la inaplicación de la norma.

Tabla cruzada Dimensión 1: Robos electrónicos*Variable dependiente: Inaplicación De La Norma						
			Variable dependiente: **INAPLICACIÓN DE LA NORMA**			Total
			Alto	Medio	Bajo	
Dimensión 1: Robos electrónicos	Alto	Recuento	0	2	0	2
		% del total	0,0%	1,1%	0,0%	1,1%
	Medio	Recuento	0	19	50	69
		% del total	0,0%	10,3%	27,2%	37,5%
	Bajo	Recuento	2	17	94	113
		% del total	1,1%	9,2%	51,1%	61,4%
Total		Recuento	2	38	144	184
		% del total	1,1%	20,7%	78,3%	100,0%

Pruebas de chi-cuadrado			
	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	12,870[a]	4	,012
Razón de verosimilitud	12,197	4	,016
Asociación lineal por lineal	4,201	1	,040
N de casos válidos	184		
a. 5 casillas (55,6%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,02.			

Decisión: Como X^2 12,970 mayor a Chi cuadrado tabla: 0,711, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes, es decir existe una relación directa entre los Delitos Informativos y la inaplicación de la norma.

Prueba de hipótesis especifica 2:

Hi: Existe una relación directa entre el sabotaje informático y la inaplicación de la norma.

Ho: No existe una relación directa entre el sabotaje informático y la inaplicación de la norma.

Tabla cruzada Dimensión 2: Sabotaje Informático*Variable dependiente: INAPLICACIÓN DE LA NORMA						
			Variable dependiente: INAPLICACIÓN DE LA NORMA			Total
			Alto	Medio	Bajo	
Dimensión 2:	Medio	Recuento	2	24	43	69

Sabotaje Informático		% del total	1,1%	13,0%	23,4%	37,5%
	Bajo	Recuento	0	14	101	115
		% del total	0,0%	7,6%	54,9%	62,5%
Total		Recuento	2	38	144	184
		% del total	1,1%	20,7%	78,3%	100,0%

Pruebas de chi-cuadrado			
	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	17,592[a]	2	,000
Razón de verosimilitud	17,850	2	,000
Asociación lineal por lineal	17,488	1	,000
N de casos válidos	184		
a. 2 casillas (33,3%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,75.			

Decisión: Como X^2 17,592 mayor a Chi cuadrado tabla: 0,103, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes, es decir existe una relación directa entre el sabotaje informático y la inaplicación de la norma.

Prueba de hipótesis especifica 3:

Hi: Existe una relación directa entre la criminalidad informática y la inaplicación de la norma.

Ho: No existe una relación directa entre la criminalidad informática y la inaplicación de la norma.

Tabla cruzada Dimensión 3: Criminalidad Informática*Variable dependiente: INAPLICACIÓN DE LA NORMA						
			Variable dependiente: INAPLICACIÓN DE LA NORMA			Total
			Alto	Medio	Bajo	
Dimensión 3: Criminalidad Informática	Alto	Recuento	2	2	1	5
		% del total	1,1%	1,1%	0,5%	2,7%
	Medio	Recuento	0	22	58	80
		% del total	0,0%	12,0%	31,5%	43,5%
	Bajo	Recuento	0	14	85	99
		% del total	0,0%	7,6%	46,2%	53,8%
Total		Recuento	2	38	144	184
		% del total	1,1%	20,7%	78,3%	100,0%

Pruebas de chi-cuadrado			
	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	79,593[a]	4	,000
Razón de verosimilitud	23,215	4	,000
Asociación lineal por lineal	16,257	1	,000

N de casos válidos	184		
a. 5 casillas (55,6%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,05.			

Decisión: Como X^2 79,593 mayor a Chi cuadrado tabla: 0,711, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes, es decir existe una relación directa entre la criminalidad informática y la inaplicación de la norma.

Prueba de hipótesis especifica 4:

Hi: Existe una relación directa entre el terrorismo informático y la inaplicación de la norma.

Ho: No existe una relación directa entre el terrorismo informático y la inaplicación de la norma.

Tabla cruzada Dimensión 4: Terrorismo Informático*Variable dependiente: INAPLICACIÓN DE LA NORMA

			Variable dependiente: INAPLICACIÓN DE LA NORMA			Total
			Alto	Medio	Bajo	
Dimensión 4: Terrorismo Informático	Medio	Recuento	2	29	55	86
		% del total	1,1%	15,8%	29,9%	46,7%
	Bajo	Recuento	0	9	89	98
		% del total	0,0%	4,9%	48,4%	53,3%
Total		Recuento	2	38	144	184
		% del total	1,1%	20,7%	78,3%	100,0%

Pruebas de chi-cuadrado			
	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	19,856[a]	2	,000
Razón de verosimilitud	21,169	2	,000
Asociación lineal por lineal	19,612	1	,000
N de casos válidos	184		
a. 2 casillas (33,3%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,93.			

Decisión: Como X^2 19,856 mayor a Chi cuadrado tabla: 0,103, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes, es decir existe una relación directa entre el terrorismo informático y la inaplicación de la norma.

Prueba de hipótesis general

Hi: Existe una relación directa entre los delitos informáticos y la inaplicación de la norma.

Ho: No existe una relación directa entre los delitos informáticos y la inaplicación de la norma.

Tabla cruzada Variable independiente: DELITOS INFORMÁTICOS*Variable dependiente: INAPLICACIÓN DE LA NORMA						
			Variable dependiente: INAPLICACIÓN DE LA NORMA			Total
			Alto	Medio	Bajo	
Variable independiente: DELITOS INFORMÁTICOS	Bajo	Recuento	2	23	18	43
		% del total	4,7%	53,5%	41,9%	100,0%
Total		Recuento	2	23	18	43
		% del total	4,7%	53,5%	41,9%	100,0%

Pruebas de chi-cuadrado			
	Valor	df	Significación asintótica (bilateral)
Chi-cuadrado de Pearson	21,866[a]	2	,000
Razón de verosimilitud	22,169	2	,000
Asociación lineal por lineal	21,612	1	,000
N de casos válidos	184		
a. 2 casillas (33,3%) han esperado un recuento menor que 5. El recuento mínimo esperado es ,93.			

Decisión: Como X^2 21,866 mayor a Chi cuadrado tabla: 0,103, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes, es decir existe una relación directa entre los delitos informáticos y la inaplicación de la norma

CAPITULO VI

PRESENTACIÓN, INTERPRETACIÓN Y DISCUSIÓN DE RESULTADOS

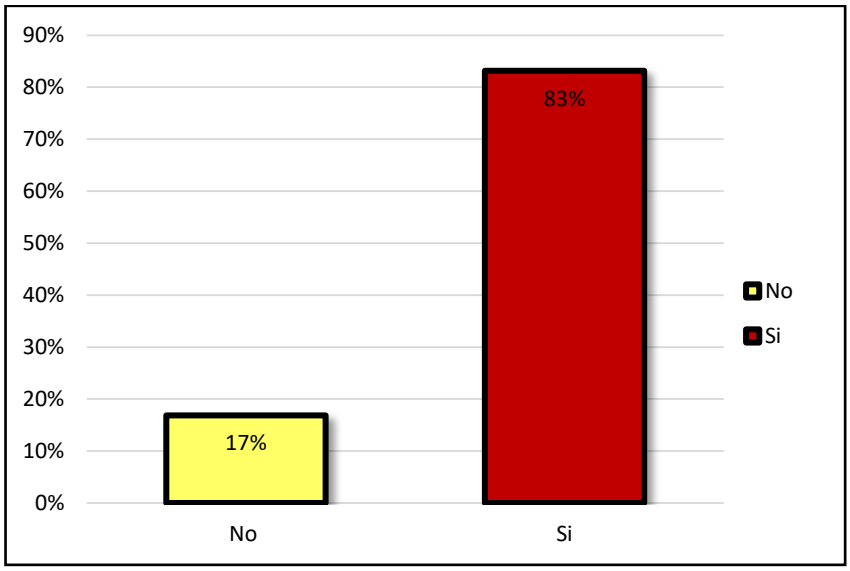
6.1 PRESENTACIÓN E INTERPRETACIÓN DE RESULTADOS

Cuadro 1: *¿Usted ha sido víctima de robo informático traducido en apropiación de su información que guarda en su correo o redes sociales?*

	f(i)	h(i)%
No	31	17%
Si	153	83%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 01



Interpretación:

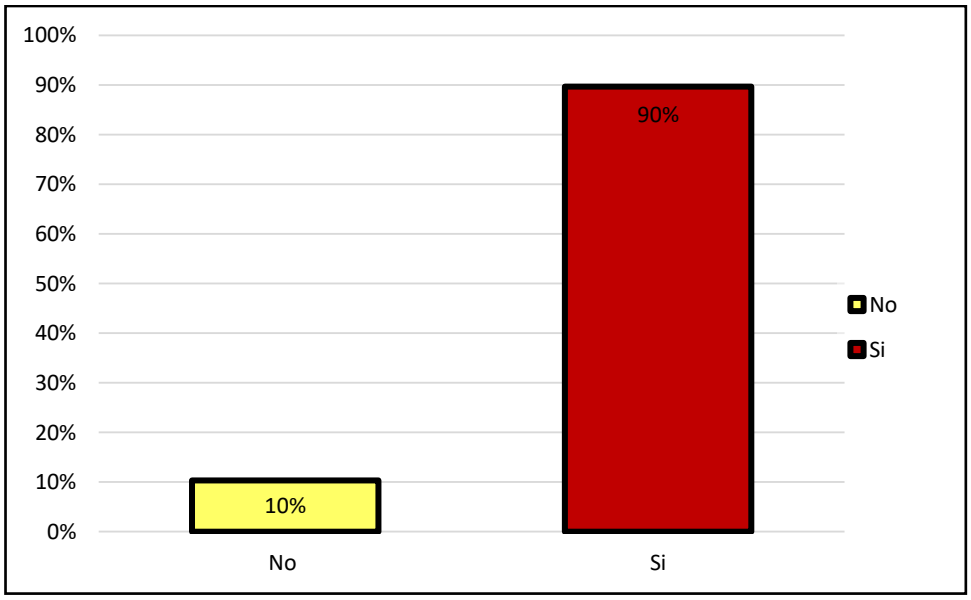
Observándose que el 17% de jueces penales, fiscales penales, docentes universitarios, policías y abogados no han sido víctima de robo informático y 83% manifiesta que han sufrido robo informático de información guardada en los correos o redes sociales.

Cuadro 2: *¿Considera Ud. que el robo de información por medio del internet es una violación a los derechos consignados en la constitución política del Perú?*

	f(i)	h(i)%
No	19	10%
Si	165	90%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 2



Interpretación:

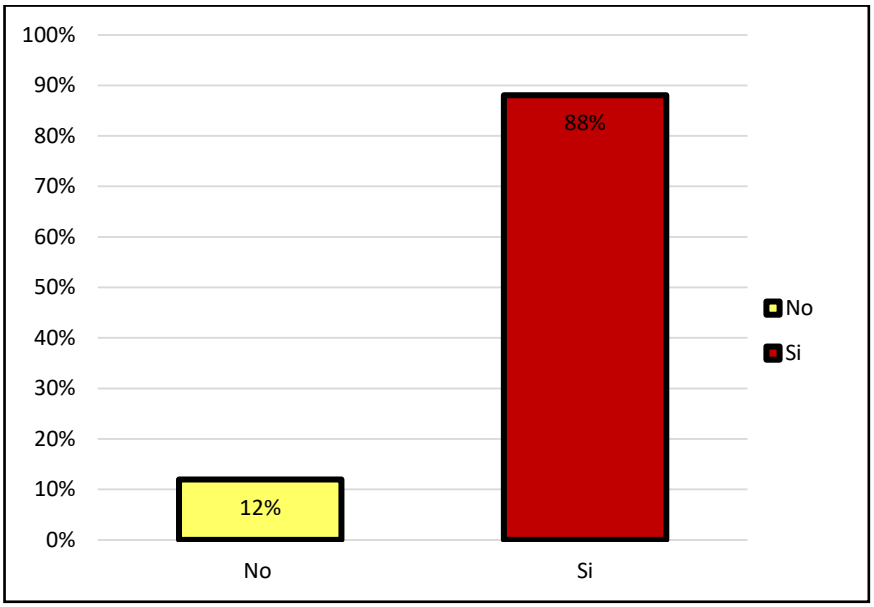
Observándose que el 10% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 90% manifiesta que el robo informático en el internet es violación a los derechos.

Cuadro 3: *¿Considera Ud. que la intimidad de las personas (vida familiar, amical, social, profesional) está siendo afectado por apropiación de información que se encuentra en las redes sociales para uso delictivo?*

	f(i)	h(i)%
No	22	12%
Si	162	88%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 3



Interpretación:

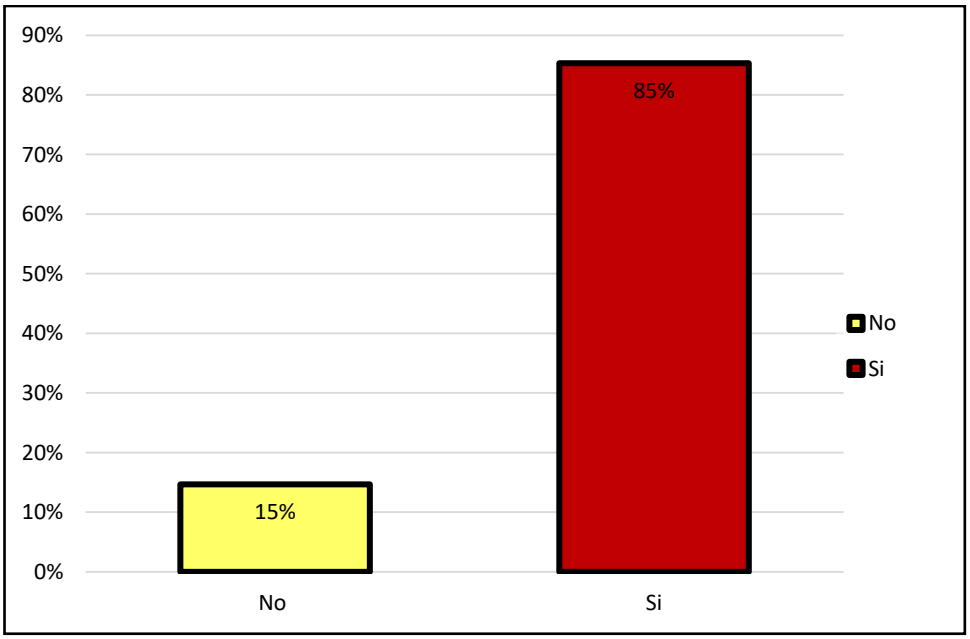
Observándose que el 12% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 88% manifiesta que la vida íntima es afectada por apropiación de información en las redes sociales.

Cuadro 4: *¿Considera Ud. que el robo de información (documentos, fotos y videos de correos, redes sociales) debe estar normado en la ley para su respectiva sanción?*

	f(i)	h(i)%
No	27	15%
Si	157	85%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 4



Interpretación:

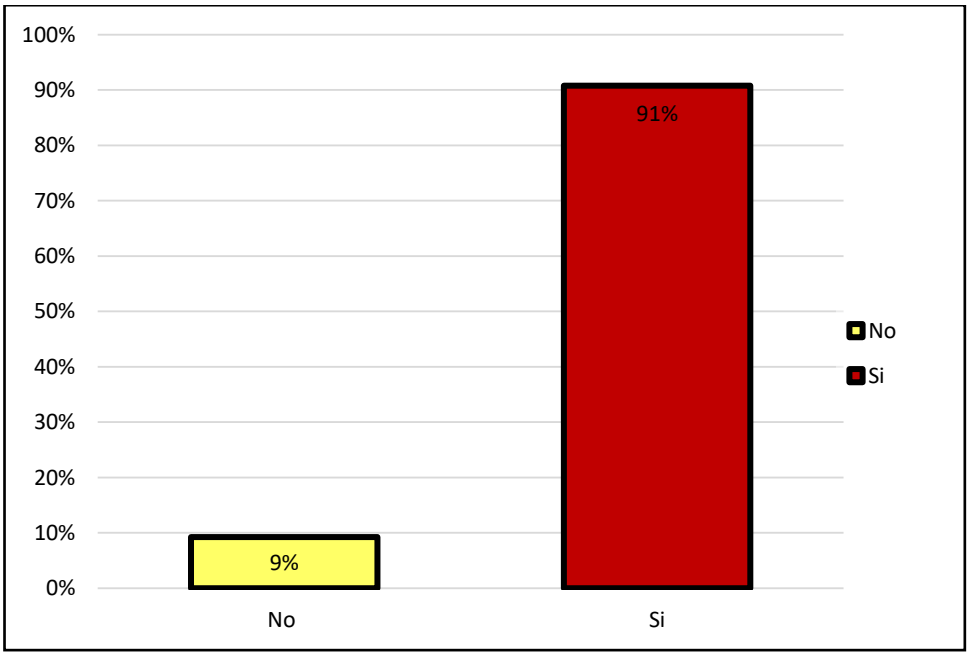
Observándose que el 15% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 85% manifiesta que el robo de información debe estar dentro de las leyes para ser sancionado.

Cuadro 5: *¿Conoce Ud. que la legislación penal peruana establece sanciones para el sabotaje informático?*

	f(i)	h(i)%
No	17	9%
Si	167	91%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 5



Interpretación:

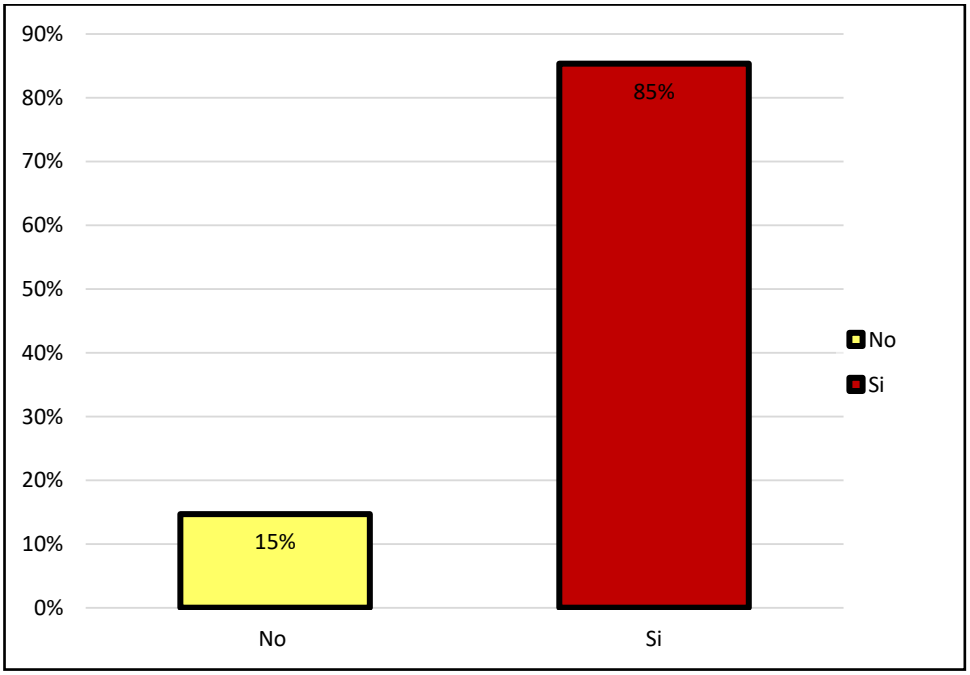
Según el 9% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 91% manifiesta que si conoce las sesiones que se le asigna los sabotajes informáticos.

Cuadro 6: *¿Conoce Ud. que el sabotaje informático se traduce mediante la destrucción o alteración de datos, programas, documentos electrónicos, contenido en redes sociales, robos de contraseñas?*

	f(i)	h(i)%
No	27	15%
Si	157	85%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 6



Interpretación:

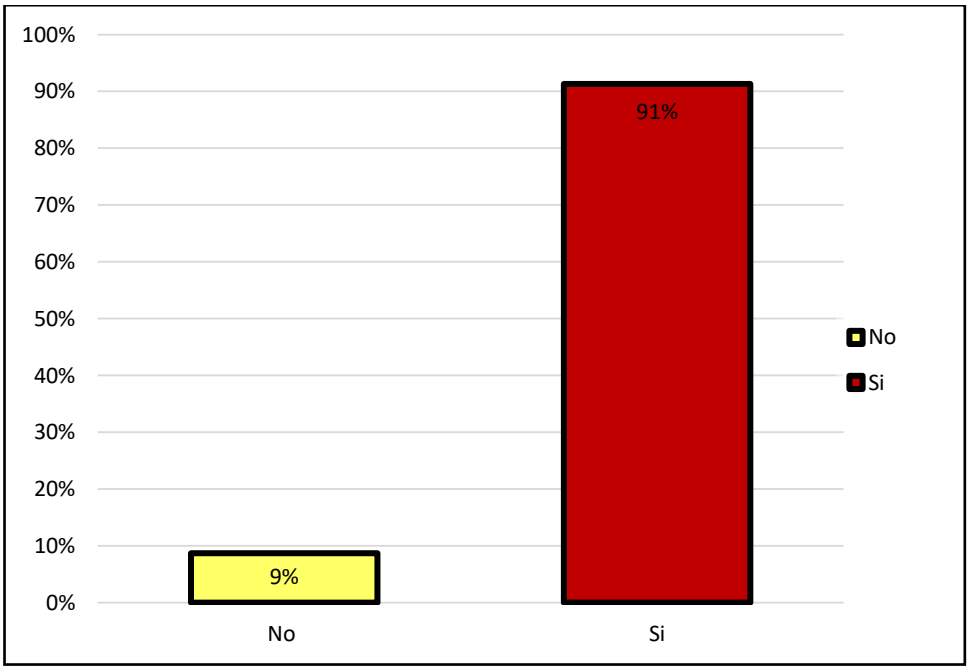
Observándose que el 15% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 85% manifiesta que conoce que el sabotaje es la destrucción o alteración de datos.

Cuadro 7: *¿Considera Ud. que las disposiciones legales que regulan el sabotaje electrónico en el Perú, son insuficientes y presentan vacíos?*

	f(i)	h(i)%
No	16	9%
Si	168	91%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 7



Interpretación:

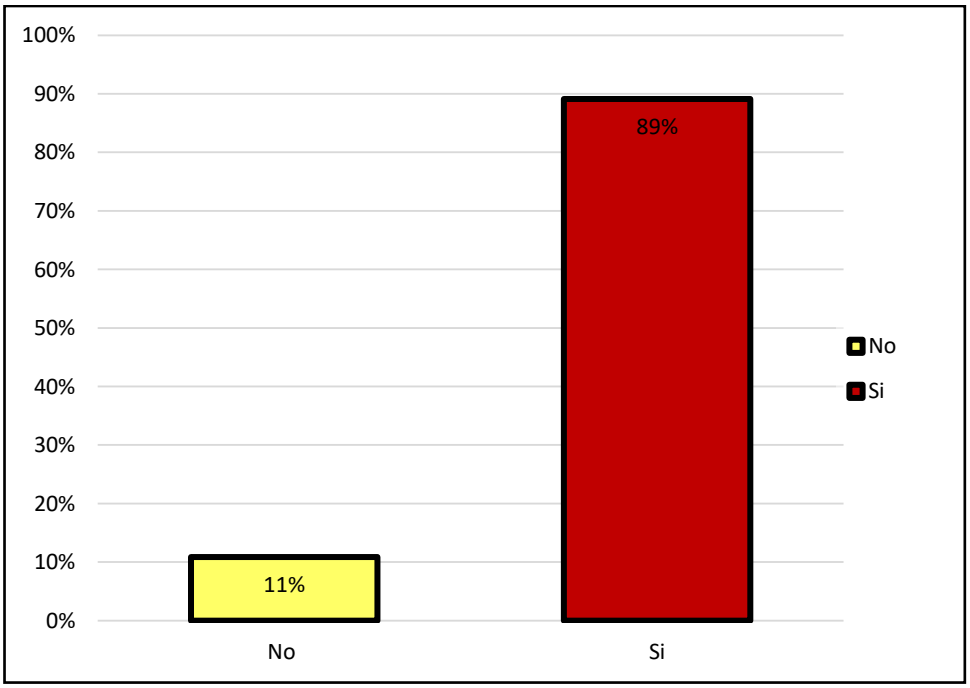
Observándose que el 9% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 91% manifiesta que las leyes en el Perú si son insuficientes en cuento al sabotaje informático.

Cuadro 8: *¿Conoce Ud. que aquel que realiza sabotaje informático será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setena a noventa días-multa?*

	f(i)	h(i)%
No	20	11%
Si	164	89%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 8



Interpretación:

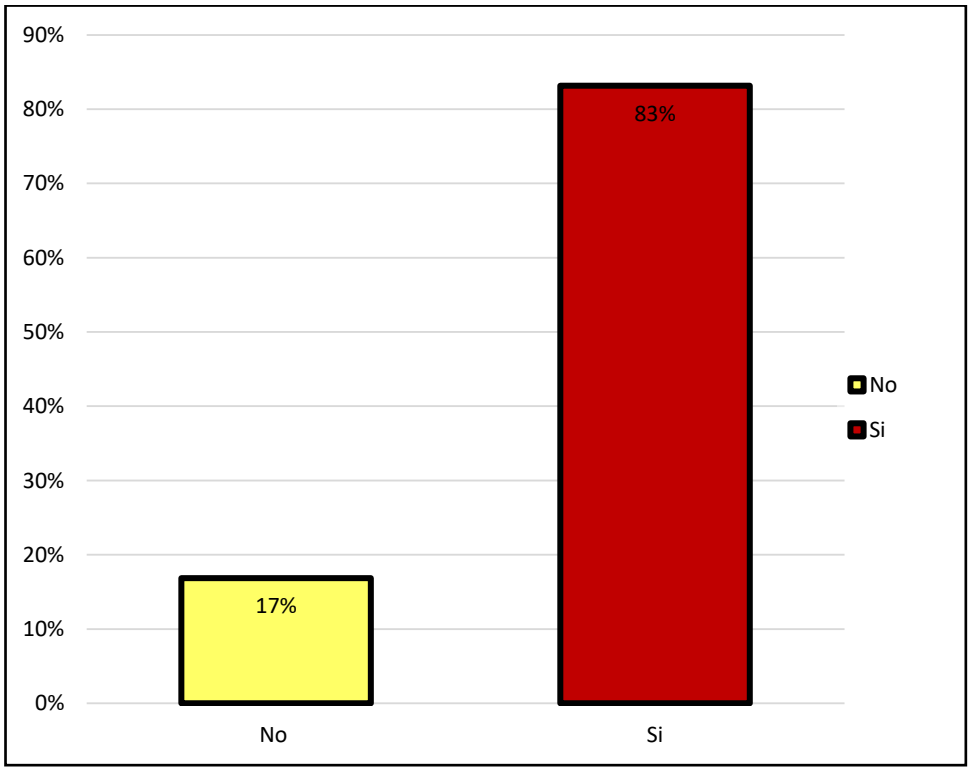
Observándose que el 11% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 89% manifiesta que las penas contra el sabotaje se castigan con pena privativa de la libertad.

Cuadro 9: *¿Conoce Ud. que los cibercriminales y ciberdelitos necesitan de una gran habilidad de los operadores jurídicos para encontrar el encaje procesal y penal de una presunta conducta criminal?*

	f(i)	h(i)%
No	31	17%
Si	153	83%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 9



Interpretación:

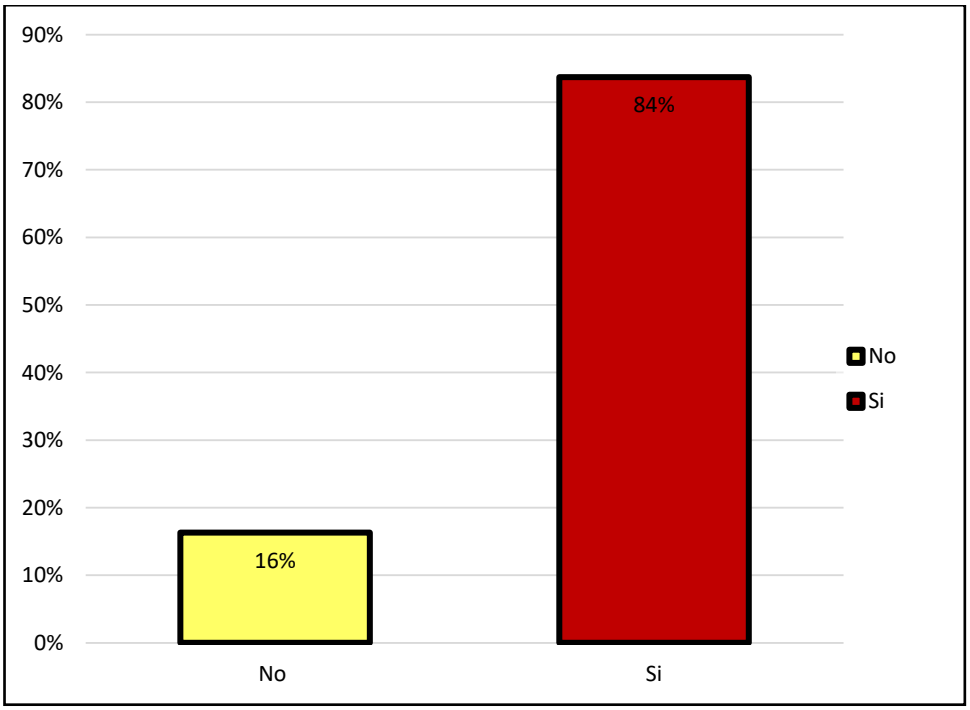
De acuerdo al 17% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 83% manifiesta que es necesaria una gran habilidad de los operadores judíos para sancionar los criminales cibernéticos.

Cuadro 10: *¿Conoce Ud. que los cibercriminales y ciberdelitos son personales especializadas en sistemas de computadoras?*

	f(i)	h(i)%
No	30	16%
Si	154	84%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 10



Interpretación:

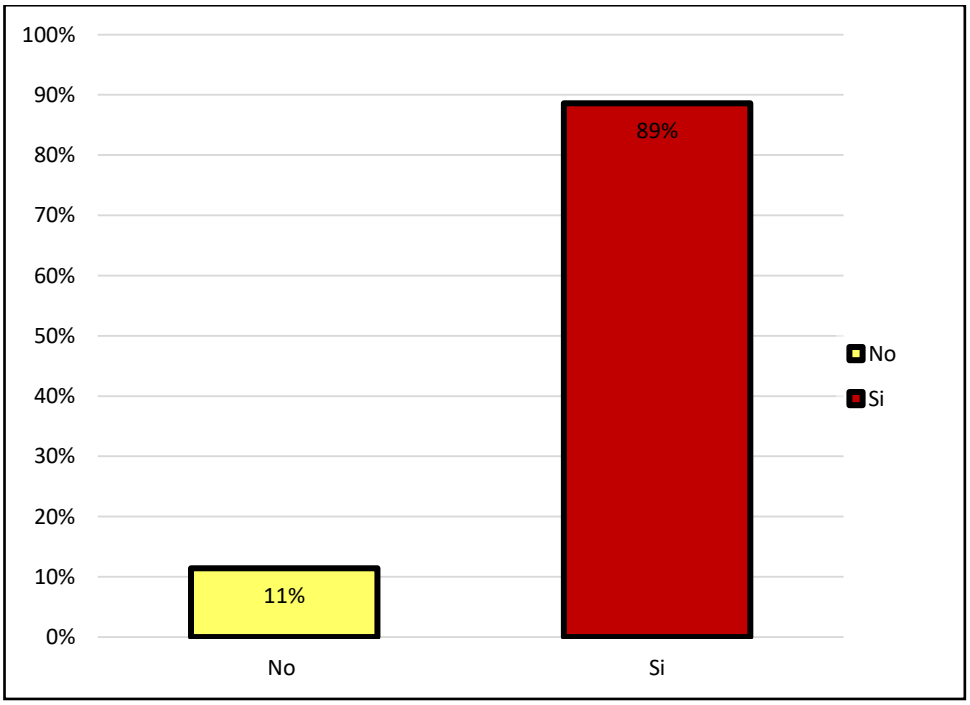
Observándose que el 16% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 84% manifiesta que los delincuentes son personales especializadas en sistemas de computadoras.

Cuadro 11: *¿Considera Ud. que el anonimato de los ciberdelincuentes dificulta la persecución para sentenciar delitos de criminalidad informática?*

	f(i)	h(i)%
No	21	11%
Si	163	89%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 11



Interpretación:

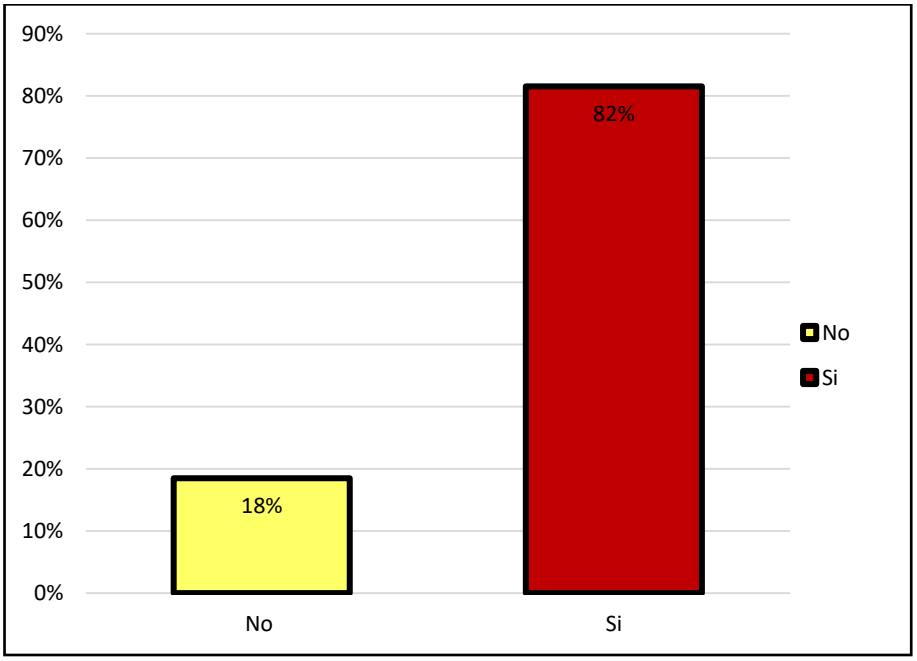
En la tabla se observan que el 11% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 89% manifiesta que el anonimato de los delincuentes en la red, dificulta las sentencias.

Cuadro 12: *¿Conoce Ud. que las organizaciones criminales cada vez están empleando la tecnología informática como instrumento de realización de sus actividades delictivas (estafa, robo de dinero informático, chantajes, etc.)?*

	f(i)	h(i)%
No	34	18%
Si	150	82%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 12



Interpretación:

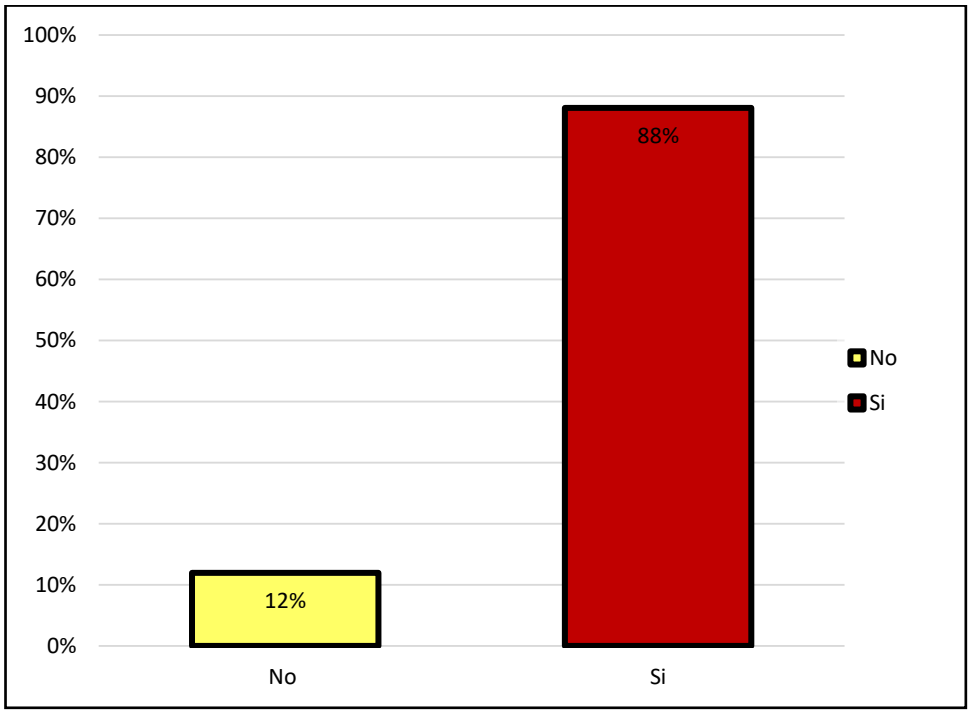
En la tabla se evidencia que el 18% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 82% manifiesta que las organizaciones criminales emplean cada día mejor tecnología informática.

Cuadro 13: *¿Conoce Ud. que un terrorista informático es una persona que causa pánico y terror con la finalidad de debilitar y desacreditar gobiernos, a la sociedad, una creencia, etc.?*

	f(i)	h(i)%
No	22	12%
Si	162	88%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 13



Interpretación:

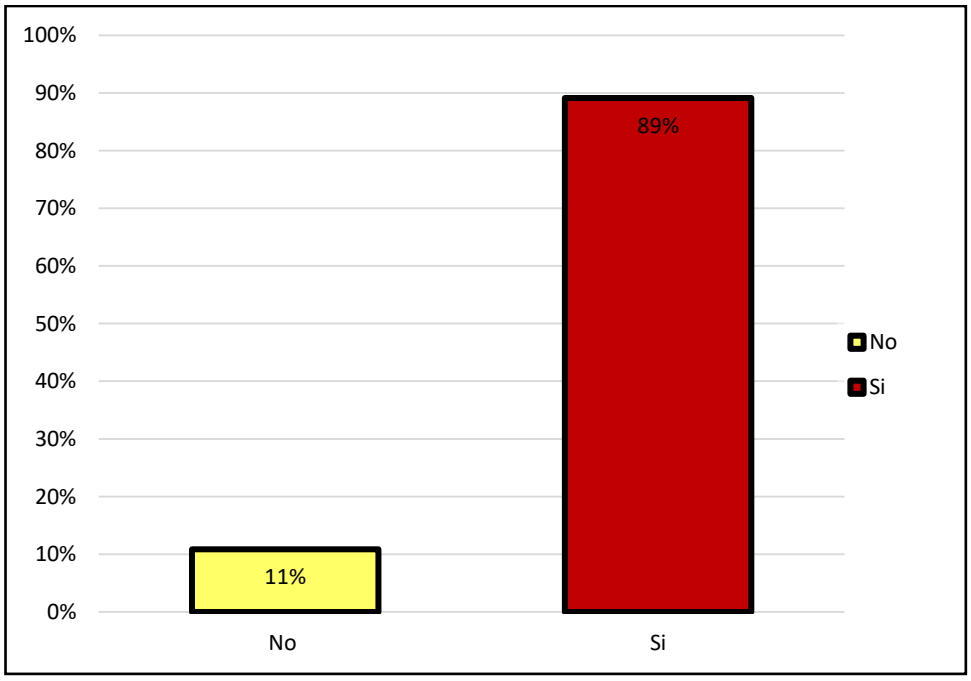
En la tabla se observan que el 12% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 88% manifiesta que los terroristas buscan fines de destrucción del país o entidades importantes.

Cuadro 14: *¿Conoce Ud. que el ciberterrorismo es el ataque masivo que sufre los sistemas de ordenadores de una entidad o sistema gubernamental para provocar inestabilidad?*

	f(i)	h(i)%
No	20	11%
Si	164	89%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 14



Interpretación:

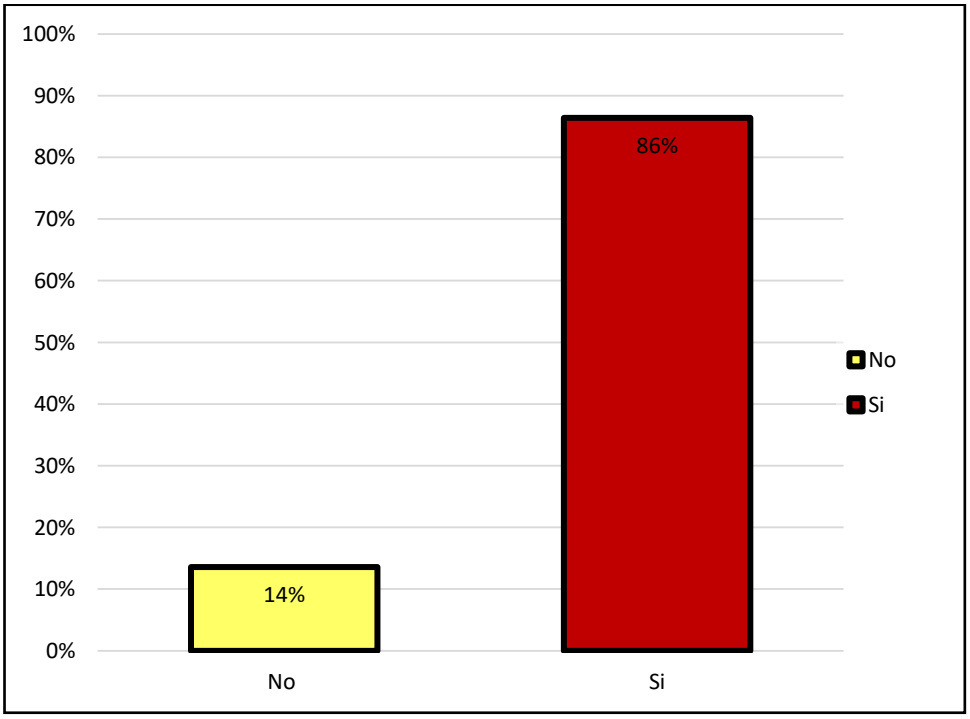
En la tabla se observan el 11% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 89% manifiesta que el ciberterrorismo está haciendo daño a los sistemas y estados gubernamentales.

Cuadro 15: *¿Conoce Ud. que el ciberterrorismo tiene como objetivo el control generalmente político, religioso o ideológico?*

	f(i)	h(i)%
No	25	14%
Si	159	86%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 15



Interpretación:

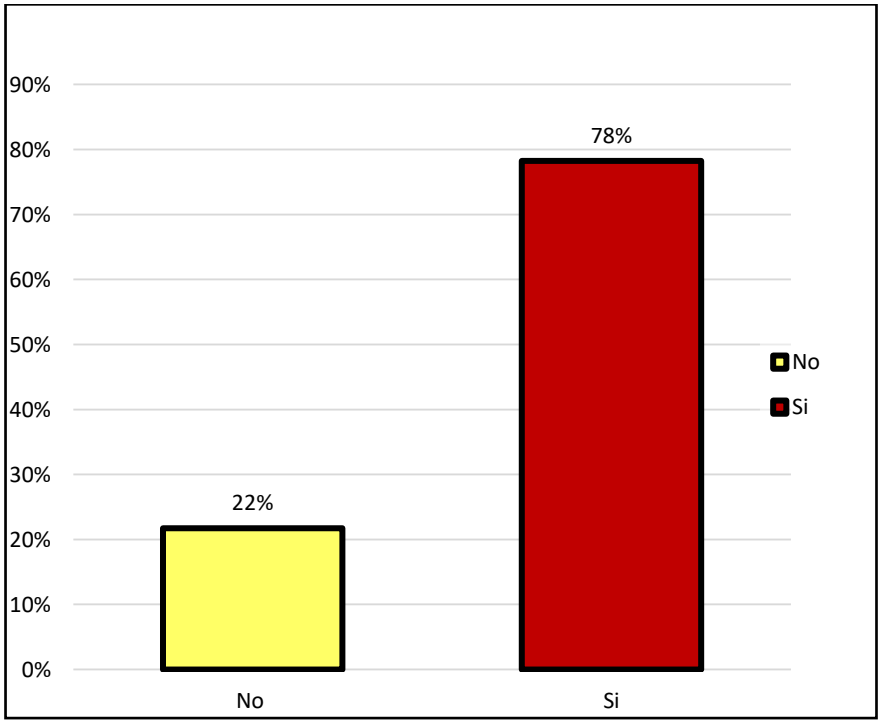
Observándose que el 14% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 86% manifiesta que los terroristas desean ter e control de organizaciones.

Cuadro 16: *¿Conoce Ud. que el uso de las tecnologías de la información por parte de grupos terroristas o individuos con el fin de desarrollar y promover su agenda. Se incluyen los ataques contra redes, el intercambio de información y la organización de actividades terroristas?*

	f(i)	h(i)%
No	40	22%
Si	144	78%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 16



Interpretación:

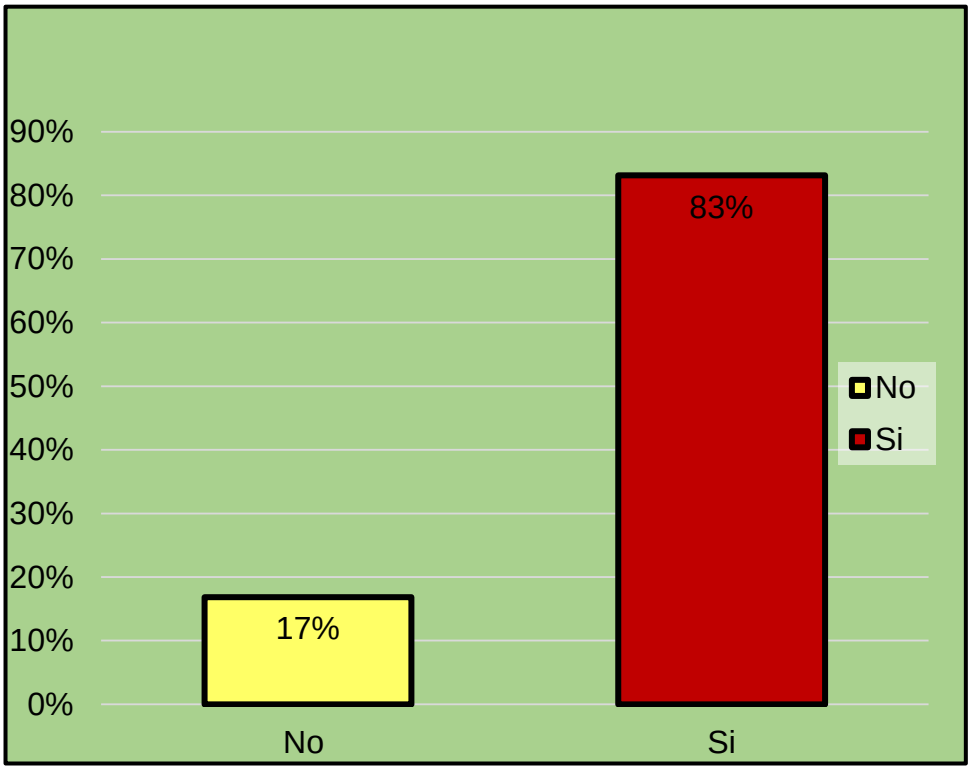
Observándose que el 22% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 78% manifiesta que los terroristas desarrollan agentas a través del ciberespacio.

Cuadro 17: *¿Considera que la manipulación informática trabaja bajo diferentes técnicas como la Salami que consiste en extraer dinero en cantidades pequeñas hasta y de manera rápida de una cuanta y transferirla hacia otra?*

	f(i)	h(i)%
No	31	17%
Si	153	83%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 17



Interpretación:

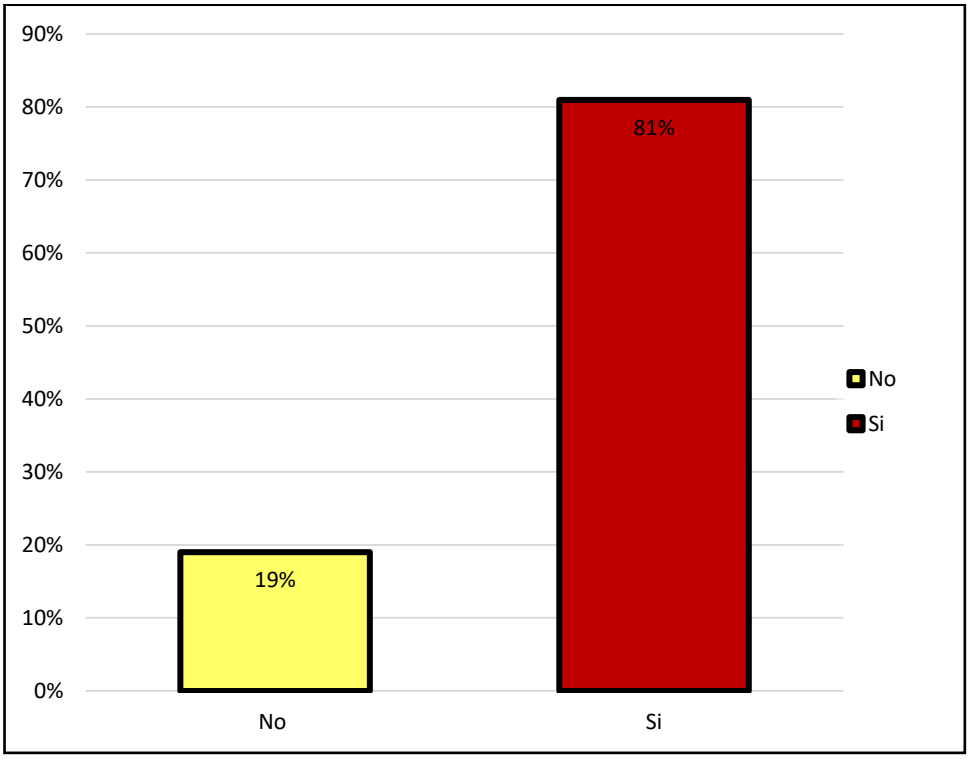
En la tabla podemos evidenciar que el 17% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 83% manifiesta que conoce técnicas para extraer dinero.

Cuadro 18: *¿Considera que usurpar la identidad de otro en transacciones electrónicas se consideraría únicamente delito de falsedad?*

	f(i)	h(i)%
No	35	19%
Si	149	81%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 18



Interpretación:

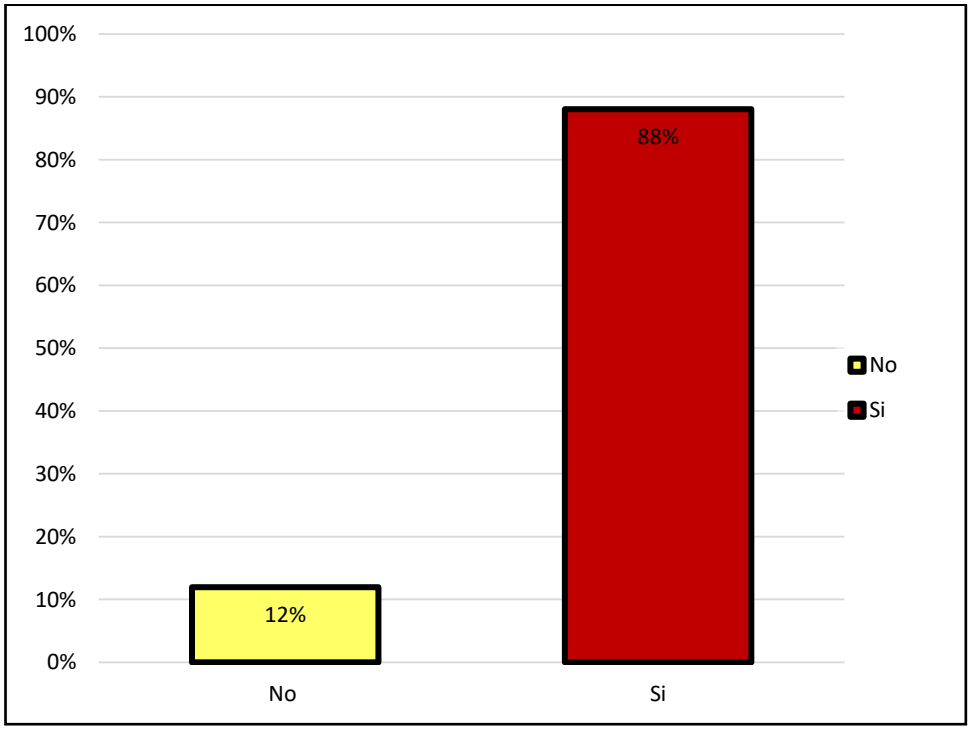
Podemos observar que el 19% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 81% manifiesta que usurpar identidad se considera como delito de falsedad.

Cuadro 19: *¿Considera que la manipulación informática no debe de ser tipificado solamente como un delito de falsedad?*

	f(i)	h(i)%
No	22	12%
Si	162	88%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 19



Interpretación:

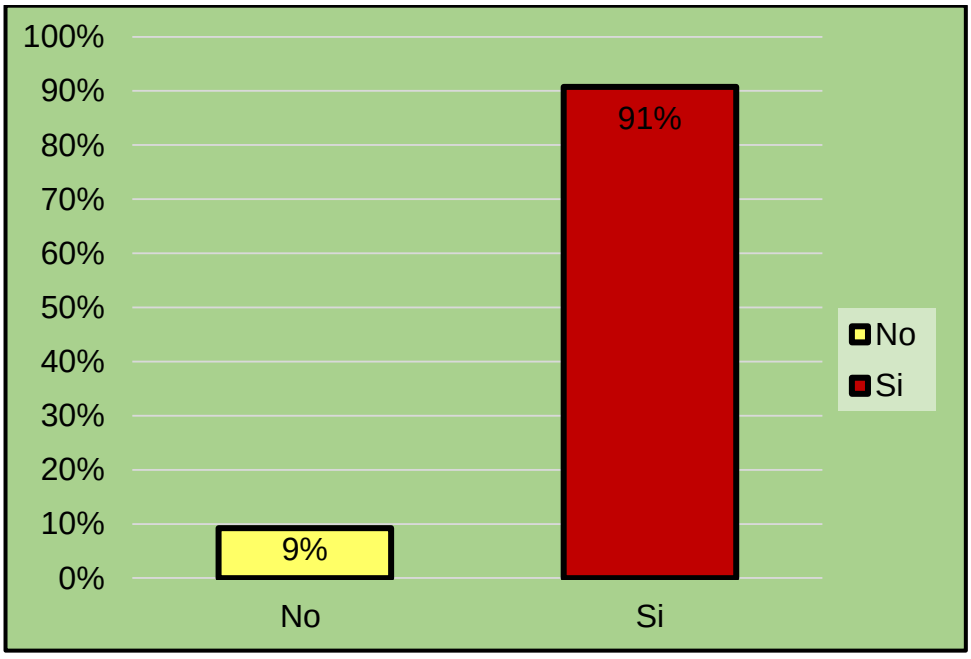
Observándose que el 12% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 88% manifiesta que la manipulación informática no solamente debe ser considerada como un delito de falsedad.

Cuadro 20: *¿Ha escuchado hablar de programas informáticos maliciosos como los spyware?*

	f(i)	h(i)%
No	17	9%
Si	167	91%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 20



Interpretación:

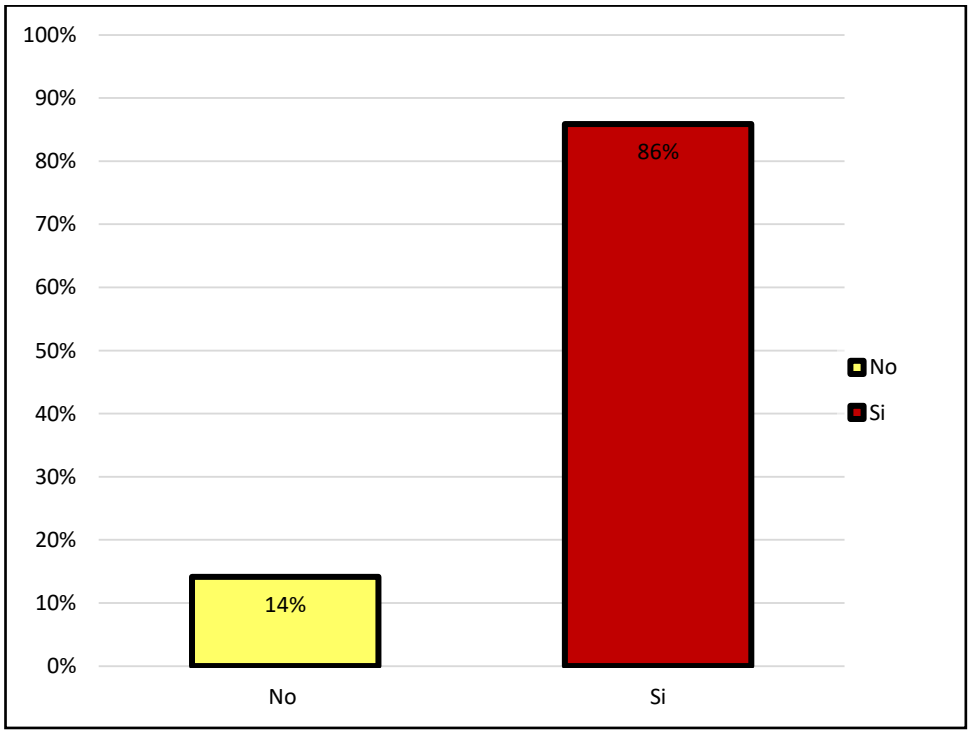
En la tabla se observan los resultados que el 9% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 91% manifiesta que conocen programas maliciosos.

Cuadro 21: *¿Considera que los delitos de "cuello blanco" (delito informático) es un tema controversial porque es difícil identificar dentro de las organizaciones a los delincuentes?*

	f(i)	h(i)%
No	26	14%
Si	158	86%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 21



Interpretación:

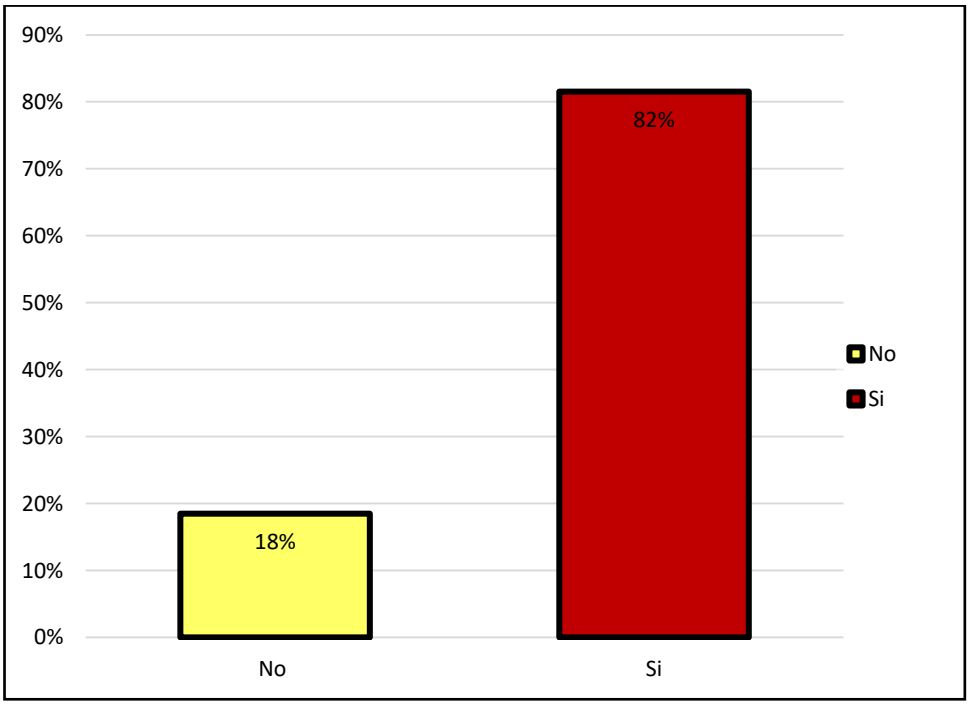
En la tabla se observan los resultados de la aplicación del cuestionario que el 14% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 86% manifiesta que los delitos de cuellos blancos son controversiales.

Cuadro 22: *¿Considera que el comportamiento delictivo es consecuencia de la impulsividad y ansiedad, sin percepción del daño a ocasionar; siendo una degradación a las leyes peruanas?*

	f(i)	h(i)%	F(i)	H(i)%
No	34	18%	34	18%
Si	150	82%	184	100%
TOTAL	184	100%		

Fuente: Data de resultados.

Gráfico Nº 22



Interpretación:

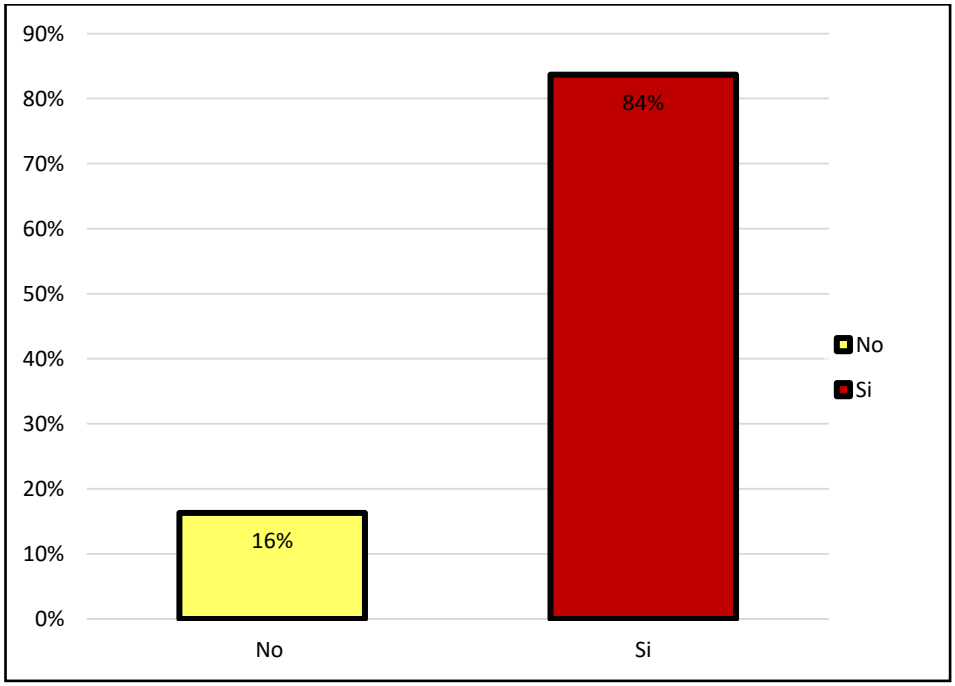
En la tabla el 18% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 82% manifiesta que si considera que el comportamiento delictivo tiene varias causales como la impulsividad y ansiedad.

Cuadro 23: *¿Está de acuerdo que el comportamiento delictivo es el resultado de procesos ambientales, grupales y cognitivo-perceptuales a través de los cuales los hechos de violencia, crimen o delictivos inciden en el comportamiento humano?*

	f(i)	h(i)%
No	30	16%
Si	154	84%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 23



Interpretación:

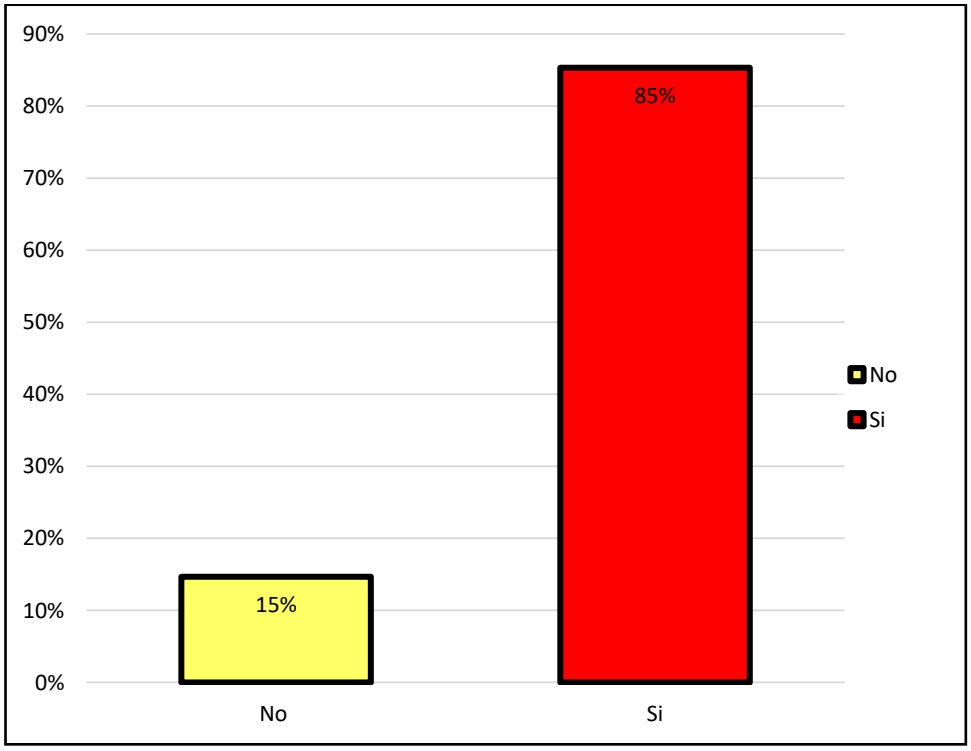
En la tabla del total de encuestados tenemos que el 16% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 84% manifiesta que si considera que el comportamiento delictivo es resultado de varias causales.

Cuadro 24: *¿Considera que el entorno familiar, contexto social y los medios de comunicación influyen en el comportamiento delictivo?*

	f(i)	h(i)%
No	27	15%
Si	157	85%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 24



Interpretación:

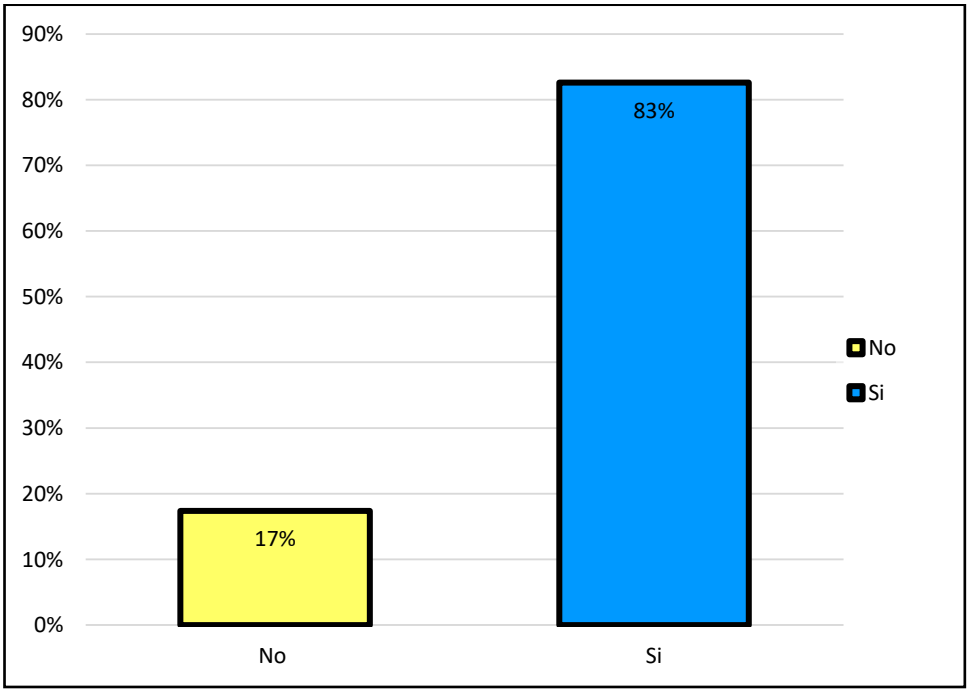
Observándose que el 15% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 85% manifiesta que los entornos familiares, sociales y medos influyen en el comportamiento delictivo.

Cuadro 25: *¿Considera que las leyes deberían de castigar con penas más severas?*

	f(i)	h(i)%
No	32	17%
Si	152	83%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 25



Interpretación:

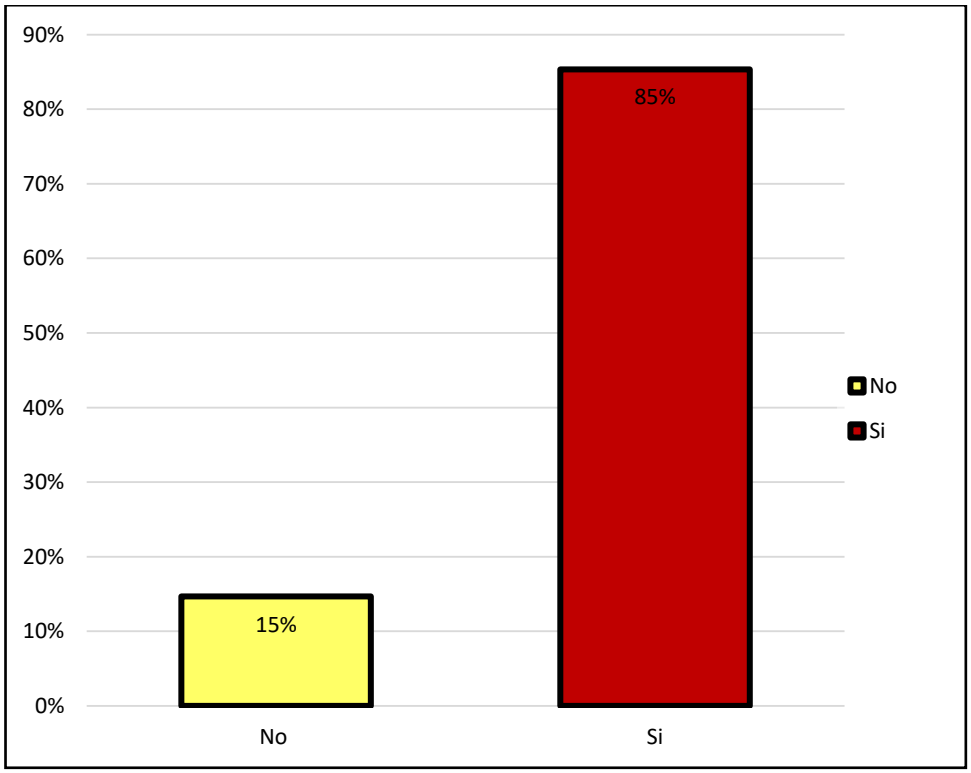
Observándose que el 17% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 83% manifiesta que las penas deberías ser más severas.

Cuadro 26: *¿Considera que los delincuentes formados en la niñez, están predispuestos a delinquir con mayor facilidad?*

	f(i)	h(i)%
No	27	15%
Si	157	85%
TOTAL	184	100%

Fuente: Data de resultados.

Gráfico Nº 26



Interpretación:

Según el 15% de jueces penales, fiscales penales, docentes universitarios, policías y abogados responden que sí y 85% manifiesta que los delincuentes formados en la niñez pueden accionar negativamente con facilidad.

6.2 DISCUSIÓN DE RESULTADOS

En la presente investigación se indago sobre como las variables delitos informáticos y dimensión problematice; para lo cual se aplicó como instrumentos de recolección de datos como el cuestionario que fueron debidamente construidos en función de sus dimensiones que permitieron a través de interrogantes conocer la percepción de los sujetos muéstrales.

Los resultados obtenidos se puede observar existe una relación directa entre los delitos informáticos y la inaplicación de la norma debido a que se obtuvo un X^2 21,866 mayor a Chi cuadrado tabla: 0,103, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes, es decir existe una relación significativa entre ellas. Dicho resultados se contrastan con la investigación de la Universidad Complutense de Madrid que sostiene que no cabe duda de que en la actualidad tanto las instituciones, sean públicas o privadas, como los particulares, y toda clase de asociaciones, tomen la forma que sea, se ven abocados irremediablemente a la utilización de equipos informáticos y sistemas de información.

Con respecto a las hipótesis específicas plateadas se puede sostener que:

Hipótesis especifica 1: Existe una relación directa entre los robos electrónicos y la inaplicación de la norma. Debido a que se obtuvo un X^2 4,026 mayor a Chi cuadrado tabla: 0,711, X^2 12,970 mayor a Chi cuadrado tabla: 0,711, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes. Dicho resultados se contrastan con la investigación de la “Universidad Nacional Mayor de San Marcos se concluye que La finalidad de la Ley de Delitos Informáticos es prevenir y sancionar las conductas ilícitas que afectan los sistemas y datas informáticos, secreto de comunicaciones, contra el patrimonio, la fe pública y la libertad sexual cometidos mediante la utilización de las TIC.

Hipótesis especifica 2: Existe una relación directa entre el sabotaje informático y la inaplicación de la norma. Debido a que se obtuvo un X^2 17,592 mayor a Chi cuadrado tabla: 0,711, entonces se procede a rechazar

la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes. Dicho resultados se contrastan con la investigación de la Universidad Nacional Autónoma de México se concluye que La influencia de la Informática en el Derecho ha originado la existencia del denominado Derecho Informático enfocado a la protección de datos informáticos o la información concentrada en medios magnéticos o digitales, teniendo una gran relación con el Derecho a la Información, en el que se pretende regular el acceso a la libre información; siendo el Derecho Informático definido por Julio Téllez Valdez como "una rama de las ciencias jurídicas que consideran a la Informática como instrumento y objeto de estudio"; siendo el análisis de ambas de suma importancia para la regulación de los Delitos Informáticos

Hipótesis especifica 3: Existe una relación directa entre la criminalidad informática y la inaplicación de la norma. Debido a que se obtuvo un X^2 79,593 mayor a Chi cuadrado tabla: 0,711, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes. Dicho resultados se contrastan con la investigación de la Universidad Internacional del Ecuador concluye que Pese a que se discute si los delitos informáticos son estrictamente tales, o solo nuevas formas de perpetración del delito, la mayor parte de legislaciones, han incluido reformas al Código Penal que contienen delitos en donde, son los medios de información son el objeto del delito, ya que responden a la necesidad social y procesal en donde los administradores de justicia dejaban en la impunidad ciertas conductas, porque el medio de su comisión era poco tradicional, diluía la responsabilidad del autor, e impedía un ajuste irrestricto al tipo, lo que a su parecer impedía la subsunción del acto al hecho considerado antijurídico, quedando el mismo en la impunidad

Hipótesis especifica 4: Existe una relación directa entre el terrorismo informático y la inaplicación de la norma. Debido a que se obtuvo un X^2 19,856 mayor a Chi cuadrado tabla: 0,103, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes. Dicho resultados se contrastan con la investigación de la Universidad de San Carlos de Guatemala se concluye que en la actualidad existe una gran variedad de

conductas delictivas que medios informáticos, que en Guatemala no se encuentran tipificadas como delitos, esto acarrea la existencia de un vacío legal en nuestro ordenamiento jurídico.

CONCLUSIONES

Primera: Se ha logrado determinar que existe una relación directa entre los delitos informáticos y la inaplicación de la norma debido a que se obtuvo un X^2 21,866 mayor a Chi cuadrado tabla: 0,103, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes.

Segunda: Se ha logrado determinar que Existe una relación directa entre los robos electrónicos y la inaplicación de la norma. Debido a que se obtuvo un X^2 4,026 mayor a Chi cuadrado tabla: 0,711, X^2 12,970 mayor a Chi cuadrado tabla: 0,711, entonces se procede a rechazar la hipótesis nula de independencia

Tercera: Se ha logrado determinar que Existe una relación directa entre el sabotaje informático y la inaplicación de la norma. Debido a que se obtuvo un X^2 17,592 mayor a Chi cuadrado tabla: 0,711, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes.

Cuarta: Se ha logrado determinar que Existe una relación directa entre la criminalidad informática y la inaplicación de la norma. Debido a que se obtuvo un X^2 79,593 mayor a Chi cuadrado tabla: 0,711, entonces se

procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes.

Quinta: Se ha logrado determinar que Existe una relación directa entre el terrorismo informático y la inaplicación de la norma. Debido a que se obtuvo un X^2 19,856 mayor a Chi cuadrado tabla: 0,103, entonces se procede a rechazar la hipótesis nula de independencia, por consecuencia se puede sostener que las variables estudiadas no son independientes.

RECOMENDACIONES

1. Es preciso recomendar que el estado debe, reconocer puntualmente la problemática de donde surgen estos delitos informáticos y proveer políticas de seguridad informáticos en los sectores más vulnerables de la población, empezando desde sus instituciones que salvaguardan información valiosa de distintos índoles, los cual al ser vulnerada podrían ocasionar un gran daño al interés público y a la defensa nacional.

2. Así también en vista de que la sociedad Peruana no se encuentra suficientemente preparada para afrontar este tipo de criminalidad, es recomendable que se fortalezcan las instituciones policiales especialidades en crímenes informáticos, no sin dejar de educar constantemente a la población y de capacitar a los funcionarios públicos que manejan información privilegiada sobre el estado, asegurando así la seguridad de esta frente a posibles ataques.

3. Así también es recomendable crear plenos jurisdiccionales con la finalidad de dar unidad a los criterios que han sido desarrollados tanto en la esfera nacional como internacional, para así dar una certera utilización de la normativa vigente.

4. Recomendamos no dejar de avanzar progresivamente el desarrollo de la normativa respecto a los delitos informáticos, puesto que con el rápido avance de la tecnología, se requiera también una legislación acorde que pueda regularla en pos de la seguridad informática de los usuarios.

VII. FUENTES DE INFORMACIÓN

American Bar Association. (1984). “Informe sobre delitos informáticos: junio de 1984. Chicago: Grupo de Trabajo sobre delitos informáticos, la Sección de Justicia Criminal”.

Banda, S., Cappelli, D., Fischer, L., Moore, A., Shaw, E., y Trzeciak, R. (2006). “La comparación de información privilegiada TI sabotaje y espionaje: un análisis basado en modelos”. Informe técnico CMU / SEI-2006-TR-026, de la Universidad Carnegie Mellon Software Engineering Institute.

Bermay, FP, y Godlove, N. (2012). “El ciberdelito siglo 21 de la víctima 'común''. Materia de justicia penal”, 89 (1), 4-5.

BERMEJO G, M. Tesis: “Tipificación del Delito Informático de Robo de identidad”, pág. 1

Brenner, SW (2008). “Ciberamenazas: la aparición de fallos Líneas del Estado-nación”. Nueva York: Oxford University Press

Casey, E. (2002). “Error La incertidumbre y la pérdida de evidencia digital. Revista Internacional de Evidencia Digital”, 1 (2). Consultado el 2 de noviembre 2014, frente https://utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

Castro O. “Delitos Virtuales: Problemas Jurídicos de las Nuevas Tecnologías”, pág. 1.

Collier, P.A, y Spaul, BJ (1992, junio). “Problemas en la policía delitos informáticos. Policial y sociedad”, 2 (4), 307-320.

Cornish, DB, y Clarke, RV (1986). “Razonando criminales - Elección Racional Perspectivas sobre infractor”.

Crozier, B. (1974), “A teoría del conflicto. Hamish Macmillan”, Londres

Furnell, S. (2002). “La delincuencia informática: Destrozar la sociedad de la información”. Londres: Pearson Education Ltd

Goodno, NH (2007). “Ciberacoso, un nuevo crimen: Evaluación de la efectividad del estado actual y las leyes federales”. Missouri Law Review, 72, 125-196.

Gordon S., y Ford, R. (2006). “En la definición y clasificación de los delitos cibernéticos. *Diario de Virología del ordenador”*, 2 (1), 13-20.

Grabosky, P. (2000). “El delito informático: Una visión general criminológica. Taller sobre delitos relacionados con la red informática, Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y el Tratamiento del Delincuente”. Viena: Citeseer.

Kshetri, N. (2013). “La delincuencia informática en la Unión Soviética y ex Europa central y oriental: Estado actual y factores clave. Ley de la delincuencia y el cambio social”, 60 (1), 39-65.
La ley Informática e informe de seguridad. volumen 21, Pp. 408-414.

Lupsha, P.A (1996). “La delincuencia organizada transnacional Versus Estado-nación. El crimen organizado transnacional”, 2 (1), 21-48.

Nykodym, N., Ariss, S., y Kurtz, K. (2008). “Adicción computadoras y los delitos. Diario de Liderazgo, Responsabilidad y Ética”.

Nykodym, N., Taylor, R., y Vilela, J. (2005). “Perfiles criminales y el crimen cibernético de información privilegiada”.

Oficina Federal de Investigación Instituto de Seguridad / ordenador. Crime Survey ordenador (2002):http://www.gocsi.com/pdfs/fbi/FBI2002.pdf

Parker, DB (1983). “La lucha contra la delincuencia informática. Nueva York, Nueva York: Hijos de Charles Scribner”.

Pocar, F. (2004). “La definición de los delitos cibernéticos en la legislación internacional. Revista Europea de Política Criminal e Investigación”, 10, 27-37.

Rogers, M. (2003). “El papel de los perfiles criminales en el proceso de la informática forense. Computadoras y Seguridad”, pp. 292-298.

Savona, U.E, y Mignone, M. (2004). “El Fox y The Hunters: ¿Cómo IC tecnologías cambian la carrera del crimen. Revista Europea de Política Criminal e Investigación”, 10, 2-26.

Schultz, E. (2002). “Un marco para entender y predecir los ataques internos. Computadoras y Seguridad”, pp. 526-531.

Spitzberg, B.H, y Hoobler, G. (2002). “Ciberacoso y las tecnologías de terrorismo interpersonal. Nuevos medios y sociedad”, 4 (1), 71-92.

Walden, I. (2005). “La delincuencia y la seguridad en el ciberespacio. Cambridge Revista de Asuntos Internacionales”, 18 (1), 51-68.

Zhigang, Y. (2011). “Cibernéticos Las variantes de los delitos tradicionales y respuestas de la ley penal”.

X. ANEXO

CUESTIONARIO SOBRE DELITOS INFORMÁTICOS

Estimados participantes, a través de este cuestionario, podrán participar sinceramente con sus opiniones sobre los delitos informáticos. Apreciado de antemano.

DIMENSIÓN 1: ROBOS ELECTRÓNICOS

1. **¿**Usted ha sido víctima de robo informático traducido en apropiación de su información que guarda en su correo o redes sociales?
   Si ( )
   Si ( )
2. ¿Considera Ud. que el robo de información por medio del internet es una violación a los derechos consignados en la constitución política del Perú?
   Si ( )
   Si ( )
3. ¿Considera Ud. que la intimidad de las personas (vida familiar, amical, social, profesional) está siendo afectado por apropiación de información que se encuentra en las redes sociales para uso delictivo?
   Si ( )
   Si ( )
4. ¿Considera Ud. que el robo de información (documentos, fotos y videos de correos, redes sociales) debe estar normado en la ley para su respectiva sanción?
   Si ( )
   Si ( )

DIMENSIÓN 2: SABOTAJE INFORMÁTICO

5. ¿Conoce Ud. que la legislación penal peruana establece sanciones para el sabotaje informático?

   Si ( )

   Si ( )

6. ¿Conoce Ud. que el sabotaje informático se traduce mediante la destrucción o alteración de datos, programas, documentos electrónicos, contenido en redes sociales, robos de contraseñas?

   Si ( )

   Si ( )

7. ¿Considera Ud. que las disposiciones legales que regulan el sabotaje electrónico en el Perú, son insuficientes y presentan vacíos?

   Si ( )

   Si ( )

8. ¿Conoce Ud. que aquel que realiza sabotaje informático será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setena a noventa días-multa?

   Si ( )

   Si ( )

DIMENSIÓN 3: CRIMINALIDAD INFORMÁTICA.

9. ¿Conoce Ud. que los cibercriminales y ciberdelitos necesitan de una gran habilidad de los operadores jurídicos para encontrar el encaje procesal y penal de una presunta conducta criminal?

   Si ( )

   Si ( )

10. ¿Conoce Ud. que los cibercriminales y ciberdelitos son personales especializadas en sistemas de computadoras?

    Si ( )

    Si ( )

11. ¿Considera Ud. que el anonimato de los ciberdelincuentes dificulta la persecución para sentenciar delitos de criminalidad informática?

    Si ( )

Si ( )

12. ¿Conoce Ud. que las organizaciones criminales cada vez están empleando la tecnología informática como instrumento de realización de sus actividades delictivas (estafa, robo de dinero informático, chantajes, etc.)?

    Si ( )

    Si ( )

DIMENSIÓN 4: TERRORISMO INFORMÁTICO.

13. ¿Conoce Ud. que un terrorista informático es una persona que causa pánico y terror con la finalidad de debilitar y desacreditar gobiernos, a la sociedad, una creencia, etc.?

    Si ( )

    Si ( )

14. ¿Conoce Ud. que el ciberterrorismo es el ataque masivo que sufre los sistemas de ordenadores de una entidad o sistema gubernamental para provocar inestabilidad?

    Si ( )

    Si ( )

15. ¿Conoce Ud. que el ciberterrorismo tiene como objetivo el control generalmente político, religioso o ideológico?

    Si ( )

    Si ( )

16. ¿Conoce Ud. que el uso de las tecnologías de la información por parte de grupos terroristas o individuos con el fin de desarrollar y promover su agenda. Se incluyen los ataques contra redes, el intercambio de información y la organización de actividades terroristas?

    Si ( )

    Si ( )

CUESTIONARIO SOBRE INAPLICACIÓN DE LA NORMA

Estimado participante, mediante el presente cuestionario se solicita su participación sincera sobre la percepción que tiene sobre la inaplicación de la norma.

Se agradece por anticipado por anticipado.

DIMENSIÓN 1: MANIPULACIÓN INFORMÁTICA.

1. ¿Considera que la manipulación informática trabaja bajo diferentes técnicas como la Salami que consiste en extraer dinero en cantidades pequeñas hasta y de manera rápida de una cuanta y transferirla hacia otra?
   Si ( )
   Si ( )
2. ¿Considera que usurpar la identidad de otro en transacciones electrónicas se consideraría únicamente delito de falsedad?
   Si ( )
   Si ( )
3. ¿Considera que la manipulación informática no debe de ser tipificado solamente como un delito de falsedad?
   Si ( )
   Si ( )
4. ¿Ha escuchado hablar de programas informáticos maliciosos como los spyware?
   Si ( )
   Si ( )
5. ¿Considera que los delitos de “cuello blanco” (delito informático) es un tema controversial porque es difícil identificar dentro de las organizaciones a los delincuentes?
   Si ( )
   Si ( )

DIMENSIÓN 2: COMPORTAMIENTO DELICTIVO

6. ¿Considera que el comportamiento delictivo es consecuencia de la impulsividad y ansiedad, sin percepción del daño a ocasionar; siendo una degradación a las leyes peruanas?

   Si ( )

   Si ( )

7. ¿Está de acuerdo que el comportamiento delictivo es el resultado de procesos ambientales, grupales y cognitivo-perceptuales a través de los cuales los hechos de violencia, crimen o delictivos inciden en el comportamiento humano?

   Si ( )

   Si ( )

8. ¿Considera que el entorno familiar, contexto social y los medios de comunicación influyen en el comportamiento delictivo?

   Si ( )

   Si ( )

9. ¿Considera que las leyes deberían de castigar con penas más severas?

   Si ( )

   Si ( )

10. ¿Considera que los delincuentes formados en la niñez, están predispuestos a delinquir con mayor facilidad?

    Si ( )

    Si ( )