Universidad Nacional
Federico Villarreal

Vicerrectorado de
INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

"LOS DELITOS INFORMATICOS Y LA PROTECCIÓN PENAL DE LA INTIMIDAD EN EL DISTRITO JUDICIAL DE LIMA, PERIODO 2008 AL 2012"

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

MAESTRO EN DERECHO PENAL

AUTOR:

MORI QUIROZ, FRANCISCO

ASESOR:

DR. JIMENEZ HERRERA, JUAN CARLOS

JURADO:

DR. AHOMET CHAVEZ, OMAR ABRAHAN

DR. RIOJA VALLEJOS, JORGE LUIS

DR. CABREJO ORMACHEA, NAPOLEON

LIMA – PERÚ

2019

TESIS

"LOS DELITOS INFORMATICOS Y LA PROTECCIÓN PENAL DE LA INTIMIDAD EN EL DISTRITO JUDICIAL DE LIMA, PERIODO 2008 AL 2012"

DEDICATORIA

A Dios por concederme la sabiduría, a mi hija Katerine Guissell quien por ella soy lo que soy, por su apoyo, consejos, comprensión, amor, ayuda en los momentos difíciles. Me ha dado todo lo que soy como persona, mis valores, mis principios, mi carácter, mi empeño, mi perseverancia, mi coraje para seguir mis objetivos.

AGRADECIMIENTO

A la Escuela de Posgrado de la Universidad Nacional Federico Villarreal, por brindarme la oportunidad de realizar los estudios de Maestría, a mis compañeros de estudios por estar en todo momento en clases recibiendo los conocimientos, a mis profesores de maestría que me dieron sus conocimientos para culminar mis estudios de Maestría, y a los jurados examinadores de la tesis. Con sincera gratitud a las personas que contribuyeron y brindaron valiosos aportes, críticas, constructivas, apoyo moral y material para la materialización de la tesis.

INDICE

RESUMEN

Ahora se emplean computadoras tanto para organización y administración de empresas, publicas y privadas, posibilita que la informática sea indispensable y podrían ser utilizados ilícitamente para cometer delitos informáticos y de la violación de la intimidad, para ello se realizó esta investigación, , tiene por objetivo explicar la causa que influye en el desacierto del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en el Distrito Judicial de Lima. El tipo de investigación es descriptivo explicativo, porque se dará una medida correctiva para la satisfacción integral de los operadores de justicia y las personas involucradas, lográndose así la efectividad de las hipótesis y objetivos establecidos. En los resultados, la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad la ausencia de formación tecnológica en delitos informático los jueces están de acuerdo en 71%, los fiscales en 25%, la policía solo en 21%. Los jueces están en desacuerdo en 20% los fiscales en 39% y los policías en 31%. En las transgresiones las legislaciones vigentes, donde los jueces están de acuerdo en 74% y en desacuerdo el 9%, los fiscales en 19% y en desacuerdo el 29%, los policías en 16%, los que están en desacuerdo el 34%.

Palabras claves: Operadores de justicia, delitos informáticos, violación a la intimida

ABSTRACT

Now computers for both organization and business administration, public and private in technical and scientific research and even in leisure, entertainment used, enables the computer is essential and could be used illegally to commit computer crimes and rape of privacy, for elo this investigation "computer Crimes and criminal protection of privacy in the judicial district of Lima, period 2008 to 2012" was held, aims to explain the cause that influences the mistake the work of operators justice (police, prosecutors and judges) in the investigation and prosecution of computer crimes in the penal protection of privacy in the Judicial District of Lima. The research is explanatory descriptive, because you will find a remedy for the full satisfaction of justice operators and people involved, thus achieving the effectiveness of the assumptions and objectives. In the results, to know the status of the work of the operators of justice in the investigation and prosecution of computer crimes and criminal protection of privacy lack of technological training in computer crimes judges agree 71%, the 25% tax, police only 21%. The judges disagree 20% 39% prosecutors and police in 31%. In the transgressions existing laws, where judges agree 74% and disagree 9% tax on 19% and disagree 29%, police in 16%, those who disagree 34%.

Keywords: Operators of justice, cybercrime, privacy violation

INTRODUCCIÓN

Se orientó a explicar la causa que influye en el desacierto del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad, en el Distrito Judicial de Lima., esta problemática se presenta por que la informática y el uso de computadoras es indispensable y podrían ser utilizados ilícitamente para cometer delitos informáticos y de la violación de la intimidad. Para tal efecto, se puso a prueba la siguiente hipótesis. H1: “Las causas de desacierto de la labor de los operadores de justicia influyen en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el Distrito Judicial de Lima”. El cuestionario de encuesta fue dirigido a 50 personas para jueces, fiscales y policías. El diseño muestral escogido fue el no experimental, La investigación es de tipo descriptivo explicativo, porque se dará una medida correctiva para la satisfacción integral de los operadores de justicia y las personas involucradas, lográndose así la efectividad de las hipótesis y objetivos establecidos. La cual permitió recolectar los datos en un solo momento, en un tiempo único, según las características de las variables e indicadores propuestos en la hipótesis. Después de llevar a cabo el trabajo de campo el presente trabajo de investigación se ha estructurado en cinco capítulos. El primero, aborda Descripción del problema, donde se da a conocer la informática y el uso de

computadoras es indispensable y podrían ser utilizados ilícitamente para cometer delitos informáticos y de la violación de la intimidad. También se mencionan los objetivos generales, Hipótesis, la justificación Viabilidad y limitaciones. El segundo capítulo trata sobre los fundamentos teóricos. El tercero, presenta el marco metodológico donde se habla del tipo de investigación realizado en base a un referente bibliográfico, también de los instrumentos de recolección de datos donde se indica la validación del instrumento. El capítulo cuarto trata del análisis sobre el delito informático y de la violación de la intimidad, y el quinto capítulo se hacen las discusiones y las conclusiones de los resultados obtenidos en la investigación.

I. PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN DEL PROBLEMA

Actualmente puede comprobarse como el empleo de computadoras de todo tipo, marca, modelo y tamaño, esto es la informatización, tanto en la organización y administración de empresas, publicas y privadas en la, investigación técnica y científica e incluso en el ocio, el entretenimiento, posibilita que la informática sea indispensable y hasta conveniente sin embargo podrían ser utilizados por manos inescrupulosas para cometer diferentes Delitos Informáticos, circunstancia que no es más que consecuencia del continuo y progresivo desarrollo del campo de la informática, aplicada en la actualidad a todos los aspectos de la vida cotidiana.

Así, la utilización de computadoras en el ámbito multisectorial pero sobre todo en el sector de la banca y seguros, lleva también a la aparición de nuevas formas de delincuencia, representativas del ingenio y la habilidad de estos nuevos "delincuentes de computadoras". De esta manera el mundo, de la informática se convierte, por un lado, en un campo amplio y lleno de posibilidades para el futuro progreso, medio de avance en el desarrollo de la sociedad moderna; pero, por otro lado, se convierte en un factor de "riesgo", en cuanto fuentes de nuevas formas de criminalidad, citando la manipulación de computadoras, la destrucción o alteración de programas, etc.

Por estas razones, se constituyen en antecedente inmediato de la presente investigación, aquellos trabajos de investigación realizados teniendo como objeto de estudio aspectos relacionados con los delitos informáticos y la protección penal de la intimidad. Por ello alcanzaremos en la presente investigación un instrumento técnico científico de utilidad para los operadores de justicia que actúen sobre la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad (Jueces, Fiscales y Policías) en el Distrito Judicial de Lima y como un aporte para la comunidad científica para encontrar respuestas sobre la problemática actual de acuerdo al uso de tecnología emergente.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general:

¿Cuál es la causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, distrito Judicial de Lima?

1.2.1 Problemas Específicos

- Conocer la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima.
- Determinar la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima.

1.3. JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN

Justificación (Del Lat. Iustificatio - onis). Es la conformidad y lo justo en la vida de las personas y las cosas. Siendo así, el presente trabajo de investigación se pretende justificar teniendo en consideración, el factor determinante que contribuye a la eficiencia de la labor de los operadores de justicia (Policías, Fiscales y Jueces) comprometidos con la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad, lo cual posibilitará mejorar el tratamiento de la problemática en el Perú. Ya que tanto el derecho de la información como el derecho de la vida privada, forman parte de los llamados derechos humanos o fundamentales. Por tanto este trabajo de investigación se justifica porque:

- Es insuficiente la investigación sobre el tema en particular y con la presente investigación se llenaran esos vacíos de información.
- Con los resultados obtenidos de esta investigación se beneficiaran los operadores de justicia y la población en general.
- Con las escasas investigaciones que se realizaron en los niveles académicos que son solo a estudios superficiales descriptivos sobre el tema, con esta investigación se plantearan opciones de solución al problema de identificación y descripción.
- Se tendrán condiciones de hacer las recomendaciones tendientes a seguir adecuando el marco teórico de acuerdo a los cambios de modalidades de los delitos informáticos.

1.4. LIMITACIONES DE LA INVESTIGACIÓN

El presente trabajo está dirigido a los operadores del derecho dedicados a la investigación de este delito y profesionales del derecho, como una propuesta que sin duda coadyuve al despliegue de una labor eficiente en la investigación y juzgamiento de los delitos informáticos que afectan a la intimidad.

- Las limitaciones en esta investigación, son las referentes a trabajos anteriores de investigación, hay pocos libros, poco material de consulta, pocas publicaciones y bibliografía. Sin embargo hemos encontrado mucha colaboración para dilucidar este problema a nivel de los operadores jurídicos. Son escasos los especialistas al respecto, y las autoridades prestan nulo o escaso apoyo para este menester.
- Hay insuficiente la información virtual que nos haga pensar que a nivel internacional se haya visto este mismo problema.

- Es cierto que tradicionalmente se haya centrado este discurso en la pena, en sus funciones y fines, conviene no perder de vista que en la fase de individualización de la pena se despliegan series de consecuencias penales y eventualmente civiles que intentan responder al complejo de demandas sociales que se articulan frente al delito cometido, más aun cuando éste posee un carácter de dañino relevante.

1.5. OBJETIVOS

1.5.1. Objetivo General

Conocer la causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, distrito Judicial de Lima.

1.5.2. Objetivos Específicos

- Conocer la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima.
- Determinar la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima.

II. MARCO TEORICO

2.1. ANTECEDENTES

2.1.1. Antecedentes Internacionales

En España, Gonzáles (2013), dice que su trabajo de investigación centra su desarrollo en el ámbito jurídico penal de determinadas acciones cometidas contra sistemas informáticos. Parece adecuado, sin embargo, comenzar el mismo con una breve, pero importante introducción sobre la ciencia en la que se originan las conductas que más tarde van a ser estudiadas. Es sabido que el Derecho, como elemento regulador de las relaciones sociales, no puede prever en su totalidad los caminos que éstas siguen en el desarrollo de los diversos modelos de evolución. El caso de los delitos informáticos en general, que podríamos denominar como aquellos cometidos contra, o a través, de medios informáticos, no escapa a esta lógica, que se ha visto además agravada por el avance vertiginoso de la informática y las telecomunicaciones.

En el mismo Argentina, Novello (2010), dice que la sanción de la ley 26.388, mediante la cual el Congreso de la Nación modificó el Código Penal, constituye gran avance para en cuestión. Los legisladores acordaron un texto determinado y transformaron en ley el proyecto que se incorporó al digesto sustantivo. Es importante, las observaciones para resaltar los beneficios que apareja la decisión tomada por el cuerpo legislativo. Los desacuerdos parlamentarios habían constituido un obstáculo para la anhelada modernización de las normas penales en comparación con los desarrollos tecnológicos actuales. La cantidad de proyectos presentados, las diferencias que tenían unos de otros y el evidente tiempo insumido que le llevó al Parlamento construir consensos

suficientes para conseguir la mentada sanción legislativa demuestran que no se trata de una materia fácil de abordar y que permita, sin complicaciones, opiniones unánimes. Los desarrollos operados y las nuevas tecnologías exigen permanentes actualizaciones del ordenamiento jurídico. En general, la dinámica que exhibe el avance del plano tecnológico plantea diversas necesidades que reclaman respuestas. En particular, la evolución que denota el campo de las tecnologías de la información y de las comunicaciones presentan contornos de inimaginables dimensiones que imponen actuar sin demora con el objeto de silenciar los desajustes que puedan producirse en el universo legal o, cuanto menos, reducirlos a su ínfima expresión. Los perfiles criminológicos evolucionan simultáneo con el sinérgico progreso que propulsa la tecnología, adaptándose el comportamiento criminoso a los nuevos desarrollos e ideando inéditas modalidades de vulneración y menoscabo de las prósperas herramientas que suministra aquella disciplina.

En el mismo Chile, Toledo (2001), dice que a través del desarrollo del trabajo de la presente tesis, sobre los delitos informáticos, delitos considerados emergentes para el milenio que comienza y por ser de un carácter exploratorio y en base a todos los antecedentes recopilados, bibliografía recopilada y entrevistas realizadas, el alumno tesista logra llegar a las siguientes conclusiones sobre el tema tratado: Que desde el inicio del proyecto Arpa en el año 1967, el desarrollo de Internet en estos 33 años, ha permitido el surgimiento de una nueva era en las comunicaciones e interrelaciones humanas, comerciales y de gestión. Que este nuevo paradigma en las relaciones humanas, permite acercar distancias, eliminar barreras y deponer conflictos raciales, religiosos, culturales. Que, si bien existe una nueva forma

de comunicación social y humana, esto ha dado margen al surgimiento de nuevos hechos o delitos, que valiéndose de la red, de sus computadores como medio o como fin, logran transgredir y superar ampliamente las distintas figuras típicas penales. La Criminología, se ha abocado al estudio de los delitos informáticos, desde el punto de vista del delincuente, del delito, la norma y el control social. Del delincuente, ha determinado que los delincuentes informáticos, son de conductas llamados “delitos de cuello blanco”, catalogando al delincuente como persona de cierto status económico, la comisión del delito, no encuentra explicación en la pobreza, ni mala habitación, ni por carencia de recreación, etc.. Los problemas jurídicos relacionados con la Internet, se basan especialmente en los nombres de dominio y las marcas comerciales, al existir diferencias en su posesión y administración por parte de sus propietarios; de los derechos de autor, ante la imposibilidad de prohibir las reproducciones no autorizadas de trabajos y elementos de propiedad intelectual, la realización virtual de actividades altamente reguladas en los ámbitos financieros, de compra y venta de valores; al no existir fronteras ni el control adecuado sobre las incipientes instituciones mercantiles, que hacen uso de la red como sustento. El comercio electrónico desarrollo gracias a la proliferación de la Internet, los problemas más urgentes se basan en la formación del consentimiento, la seguridad acerca de las identidades de los contratantes y la prueba de las obligaciones; como también es sobre la legislación aplicable al acto o contrato específico, los tribunales competentes y la seguridad en los medios de pago; para ello las distintas legislaciones a nivel mundial y gracias a la promulgación de la Ley Modelo sobre el Comercio electrónico, de la Comisión de las Naciones Unidadas para el Derecho Comercial (UNCITRAL), que recomienda a los países integrantes de las Naciones Unidas, sobre la

legislación nacional en materia de las firmas y documentos electrónicos, con el objeto de dar seguridad a las relaciones jurídicas electrónicas. Chile, en parte adopta dicho criterio, mediante el establecimiento del Decreto Supremo N°. 81, de 1999, del Ministerio Secretaría General de la Presidencia, que regula el uso de la firma digital y los documentos electrónicos en la Administración del Estado, otorgando a la firma digital los mismos efectos que la firma manuscrita, eliminando de esta forma la necesidad de sellos, timbres y vistos buenos.

2.2.1. Antecedentes Nacionales

Fernández, Cabezudo, Arenas, Herrera, y Gastelu (2010), concluyen que el avance tecnológico, ha sido la causante de que nuestro estilo de vida haya cambiado por completo en las dos últimas décadas, estamos frente a nuevos tipos penales, debido a que antes no había un adelanto informático y electrónico de grandes magnitudes como ahora, lo cual nos lleva a dos conclusiones, la primera, que paralelamente al avance tecnológico, hay un avance más desarrollado en el delincuente, ya que este, tiene que tener un amplio conocimiento de dichos avances, los cuales, no los ocupan en realizar el bien sino a delinquir; y la segunda, que debido a la falta de una completa tipificación de los delitos cometidos con ayuda de la tecnología, estos delincuentes pueden seguir cometiendo este tipo de actos ilícitos, sin temor a recibir alguna sanción o privación de su libertad, es así que la población debe ser orientada en las medidas de seguridad para evitar ser víctimas de delitos informáticos. Los delitos informáticos constituyen una gran laguna en nuestras leyes penales, y basados en la diversa información existente en el medio virtual, podemos hacer una lista de los delitos que no están contemplados en

nuestro Código Penal y que requieren análisis por parte de académicos, penalistas y legisladores; toda vez, que nuestro ordenamiento jurídico, específicamente la Ley 27309, dada el 26 de junio del 2000, incorpora la figura de “Delitos Informáticos” al Código Penal, en sus artículos 207-A.- Interferencia, acceso o copia ilícita contenido en base de datos, el Art. 207-B Sabotaje Informático y el Art. 207-C.- que detalla las circunstancias. Agravantes de los anteriores artículos. Tipificación que es insuficiente, con palabras muy técnicas que son poco entendidas; la ley debe ponerse adelante con la tecnología. Es necesario establecer que no existe una herramienta de control que abarque todas las necesidades y sea infalible, aunque el único plan de seguridad eficaz es el que utiliza muchas capas de seguridad. Ejemplo, los firewall, no puede protegerla frente a muchos tipos de brechas de seguridad, como las internas, las físicas o las intrusiones causadas por la divulgación de contraseñas de los usuarios, siendo esta la principal medida de seguridad para evitar ser víctima de delitos informáticos. La Policía Nacional del Perú, representada por la DIVINDAT, tiene responsabilidad de dar solución a delitos informáticos e implementar cambios en verificación de la utilización de herramientas de control, evaluación de riesgos, así como medidas de protección que ayuden a minimizar las amenazas que presentan los delitos informáticos.

Recientemente, como consecuencia del crecimiento de las tecnologías de la información y comunicación, un nuevo tipo de delito denominado delito informático se ha ido desarrollando. En esa línea en nuestro país, se han emitido leyes penales con el propósito de sancionar acciones delictivas que involucren los sistemas informáticos, información denominada como secreta, el patrimonio, la fe pública y la libertad sexual (Villavicencio, 2014)

2.2. MARCO CONCEPTUAL

2.2.1. Delitos informáticos.

Sobre el significado de delito informático se anotan tres definiciones de gran valor:

- Es cualquier acción ilegal en la que el ordenador sea el instrumento o el objeto del delito y, más concretamente, cualquier delito ligado al tratamiento automático concretamente de datos;
- Cualquier acto criminoso relacionado con la tecnología informática, por el cual una víctima ha sufrido una pérdida y un autor ha obtenido intencionalmente una ganancia.
- Cualquier conducta ilegal, no ética o no autorizada, que involucra el procesamiento automático de datos y/o la transmisión de datos.

2.2.2. Teorías generales relacionadas con el tema : Los Delincuentes Informáticos.- El sujeto Activo

Según Vera (1996), éstas son las características del delincuente informático:

- Adolescentes con un coeficiente intelectual alto, y ausentes de toda consciencia de estar obrando mal (síndrome de Robin Hood).
- Mito ya que una gran cantidad de casos, son cometidos por sujetos que trabajan en el mundo de la informática, de edad superior y no necesariamente muy inteligentes.
- Empleados de confianza por la actividad que realizan o por el tiempo que llevan en la empresa.
- Además, existen los delincuentes a distancia.

Magliona (2003) opina que “se ha venido realizando una caracterización casi mítica respecto del perfil del delincuente informático, basándose en los primeros casos de estudiantes americanos que fueron dados a conocer, en que se trataba de adolescentes con un coeficiente intelectual alto ausentes de toda consciencia de estar obrando mal”.

El prototipo de delincuentes informáticos descritos por la mayoría de los autores, caracterizaba al sujeto activo de estos delitos como jóvenes cuyas edades fluctuaban entre los 18 y los 30 años de edad, en su mayoría varones solteros sin antecedentes penales, inteligentes motivados por su profesión y por el desafío técnico. Esto no constituye más que un mito por cuanto una gran cantidad de casos de gran gravedad, son cometidos por sujetos que trabajan en el mundo de la informática, y ni la mitad de inteligentes. (Aniyar de Castro, 1980)

Actualmente de acuerdo a Artega (1987)las conductas informáticas delictivas se llevan a cabo por personas vinculadas de algún modo a las empresas, como empleados de confianza, técnicos especialistas en programación y en general, todo tipo de personas con acceso material a las instalaciones de procesamiento de datos. Suelen ser empleados de confianza por el tiempo que llevan en la empresa o por el tipo de trabajo que desempeñan en ella, y conocen debilidades del sistema. Sin perjuicio de lo anterior, Internet permite que hoy concurran como sujetos activos de los delitos informáticos, los delincuentes a distancia, quienes desde cualquier país del mundo pueden atentar contra un sistema de tratamiento de información. Con el aporte de la

obra criminológica del sociólogo norteamericano Sutherland en las corrientes estructuralistas, se pone de manifiesto la relación clase social delito en términos de características según el estatus social, de comisión delictiva y de reacción social.

Callegari (1985)afirma que los criminales informáticos en su generalidad son de sexo masculino de 18 a 30 años de edad, con características de ser un empleado de confianza en la empresa en la que desenvuelve sus funciones, posee necesariamente conocimientos técnicos de computación. Estos agentes responden a motivaciones dispares generalmente el “animus delicti” es motivado por razones de carácter lucrativo. Por la popularidad que representa este actuar en la sociedad moderna o por simple diversión “hackers” o por intención de que su actuar puede responder al deseo de destruir o dañar un sistema informático, lo que varía es la intencionalidad en su comisión. Estos delincuentes poseen varias características semejantes a los delincuentes de cuello blanco ya que ambos sujetos activos poseen un status socioeconómico, no pudiendo explicarse su comisión por mala situación o pobreza, ni por carencia de recreación o por baja educación, ni por poca inteligencia.

2.2.3. Los Usuarios Agraviados.- El Sujeto Pasivo

Vera (1996) sostiene que las características de las víctimas de los delitos son: Personas Jurídicas, Bancos, Compañías de Seguros Empresas públicas y privadas. No denuncian los delitos por temor a pérdida de imagen corporativa (Seriedad, solvencia y seguridad) Solución mediante medidas internas (despidos o aumentos de medidas de seguridad). Situación favorece a

delincuentes (generalmente no se denuncian los delitos, se llega a un acuerdo con el delincuente).

Según Magliona (2003), las víctimas de estos delitos son generalmente personas jurídicas. Se trata, usualmente de bancos compañías de seguros, empresas públicas y privadas, sin importar si cuentan o no con medidas técnicas de protección. Una vez que estas asociaciones detectan las conductas ilícitas de las cuales han sido objeto, suelen no denunciar los delitos por temor a sufrir una pérdida de su imagen corporativa. No están dispuestas a perder la imagen de seriedad, solvencia y seguridad y antes de ver sus debilidades expuestas, prefieren solucionar su problemas mediante la aplicación de medidas internas, como despidos o aumentos de seguridad. Por supuesto esa actitud no hace sino favorecer a los delincuentes, quienes continuaran con sus conductas con la mayor impunidad.

2.2.4. El bien jurídico tutelado

En un principio, el legislador del Código Penal de 1991 consideró que con la inclusión del delito de hurto telemático sería suficiente para reprimir el fenómeno comentado (Silva, 2006).

Sin embargo, al advertirse que la mencionada disposición impuesta a manera de agravante solo contenía a un grupo reducido de comportamientos, dejando sin sanción a otro gran número, es que, vía la promulgación de la Ley n.° 27309, el legislador incorporó al Código Penal los delitos informáticos (arts. 207-A, 207-B Y 207-C). Tal adición se realizó bajo el marco de los ilícitos que

atentan contra el bien jurídico patrimonio, por lo que, desde cierto sector, se llegó a sostener que el bien jurídico protegido era aquel y no un nuevo interés social que de manera autónoma a la afectación del daño patrimonial, pueda también ser objeto de tutela en atención a su importancia para el mantenimiento de las relaciones normales de interacción (Salf, 1994)

Gálvez, Delgado y Rojas, (2011) afirman quehoy en día, si bien existe consenso en aceptar a la categoría de los delitosinformáticos como el reflejo de una nueva forma de criminalidad, que se relaciona directamente con el uso o la intermediación de un elemento o dato informatizado, existen dos distintos caminos para encarar el citado fenómeno desde un punto de vista propiamente penal.

Uno de estos, que se acerca a la posición asumida por el legislador del Código Penal de 1991, así como las posteriores reformas, niega que el avance tecnológico y los problemas presentados por el uso generalizado de los sistemas informáticos configuren un nuevo interés digno de protección, de manera que, en realidad, subyacería una nueva forma de criminalidad aun carente de adecuada tutela, pero que versaría sobre bienes jurídicos ya conocidos por todos (entendemos, por ejemplo, el patrimonio, la intimidad, entre otros) (Salinas, 2006).

Romeo(2012) sostiene que de acuerdo a esta primera posición, en sintonía con un sector de la doctrina, se puede elaborar una clasificación tripartita de los delitos informáticos: i) delitos económico-patrimoniales vinculados a la informática (ciberdelincuencia económica), ii) atentados por medios

informáticos contra la intimidad y la privacidad (ciberdelincuencia intrusiva), iii) ataques por medios informáticos contra intereses supraindividuales (ciberespionaje y ciberterrorismo).

Los delitos económico-patrimoniales vinculados a la informática tratarían sobre ataques al bien jurídico patrimonio, realizados a través de la informática y siempre llevados a cabo con la "intención" de consumar apoderamientos o beneficios económicamente evaluables sobre el patrimonio de terceras personas (estafa informática y espionaje informático de secretos de empresa, por ejemplo). En relación con los atentados por medios informáticos contra la intimidad y la privacidad, cabe indicar que, para dicho sector de opinión, constituyen ataques al bien jurídico privacidad, pero "como un concepto que incluyendo el de intimidad, va más allá, pues abarca todas las modalidades protegidas en el art. 18 CE [Constitución española] (el honor, la intimidad personal, la familiar, la propia imagen, el domicilio, el secreto de las comunicaciones o el uso correcto de la informática)" (Gálvez, Delgado, & Rojas, 2011)

Asimismo, los ataques por medios informáticos contra intereses supraindividuales hacen referencia a los atentados más graves, que afectan indiscriminadamente a intereses generales de la población con la intención de crear pánico y terror para subvertir el sistema político o de convivencia generalmente aceptado. Visto aquello, cabe examinar la otra perspectiva que, a diferencia de la que acabamos de exponer, defiende la existencia de un nuevo interés social, cuya importancia amerita urgente protección, toda vez que, de la mano con el avance tecnológico, se impone una nueva constatación de la

realidad, cuya principal característica es la necesidad de regular los procedimientos consistentes en el almacenamiento, transmisión y empleo de mecanismos automatizados dada su repercusión en la vida moderna y en el tráfico mercantil (Peña, 2010).

En esa línea, a partir de una rápida revisión del estado actual del debate en la doctrina nacional, es posible indicar que se resguarda de manera específica la información contenida en los sistemas de tratamiento automatizado de datos o, quizá de manera aún más precisa, la seguridad de la información contenida en las bases de datos, sistema o red de computadoras. Brevemente, si bien los delitos informáticos involucran el delito de hurto; hoy en día, se entiende que el uso de las TIC genera serios riesgos de cara a la tutela de un nuevo interés social, gestado al interior de la sociedad de la información, cuya importancia propicia la necesidad de tutela por parte del Derecho penal: la seguridad de la información contenida en las bases de datos, sistema o red de computadoras (Reyna, 2002).

2.2.5. La Policía Nacional del Perú, respecto a los delitos informáticos.

Tienen funciones preventivas, respetuosas de los DDHH, tratando de evitar en lo posible estigmas sociales, abierta a organismos de socialización primaria y secundaria y, ser una institución racionalmente profesional. El artículo 166° de la Constitución Política dice: “La policía tiene por finalidad fundamental garantizar, mantener y restablecer el orden interno. Prestar ayuda y protección a las personas y a la comunidad. Garantiza el cumplimiento de las leyes y la

seguridad del patrimonio público y del privado. Previene investiga y combate la delincuencia. Vigila y controla las fronteras" (Landa & Velazco, 2007).

Nuestra policía cuenta con la División de Investigaciones de Delitos de Alta Tecnología DIVINDAD de la DIRINCRI, departamento integrado por 45 policías, encargados de patrullar el ciberespacio de los peruanos de la posible comisión de delitos tales como: Hurto de fondos, pornografía infantil, delitos informáticos, piratería de software y otras investigaciones especiales. "No se trata de cualquier trabajo policial, hablamos de un patrullaje virtual en el ciberespacio que demanda estar en las mismas y de ser posible, en mejores condiciones tecnológicas que los delincuentes informáticos. También implica una gran dedicación y paciencia para detectarlos a través de minuciosos trabajos de inteligencia" dice el coronel Alejandro Díaz Changanaki, Jefe de la DIVINDAD-PNP, El Coronel Díaz manifiesta que se tiene conocimiento de múltiples delitos cometidos contra grandes firmas bancarias, quienes se abstienen de denunciar estos hechos por temor a no ver mellada su imagen o provocar el llamado pánico financiero. Ante esta situación, no queda más que estar alertas e informados", señala el Coronel Díaz Changanaki (Fernández, Cabezudo, Arenas, Herrera, & Gastelu, 2010).

De otro lado un aspecto a considerar en los delitos informáticos es lo referente a la cifra negra de impunidad, la misma que gira en torno a la capacidad tecnológica que mantienen los agentes delictivos que contrastada con la debilidad de los órganos encargados del control penal otorgan prerrogativas los delincuentes en clara vulneración del principio de igualdad ante la ley. Privilegios que adquiere mayor contundencia con la coexistencia de una

limitada legislación vigente que no permite a la PNP garantizar, mantener y restablecer el orden interno, a ello se suma la abulia de algunos efectivos de la PNP, un sistema laboral inadecuado, la supervivencia en la Institución Policial de un sistema de corrupción, bajas remuneraciones; inexistencia de policías especializados en informática para determinar en un parte policial, o en un atestado en la comisión de un delito informático; y la difusión en la colectividad de que los delitos informáticos no entrañan connotación ni reacción social en contra (Fernández, Cabezudo, Arenas, Herrera, & Gastelu, 2010).

2.2.6. El Ministerio Publico respecto a los delitos Informáticos

(Blossiers, 2003) Afirma quecon el Nuevo Código Procesal, el Ministerio Público conduce y controla jurídicamente los actos de investigación que realiza la Policía Nacional. Es el Fiscal del caso quien decidirá si la Policía Nacional realiza o no algún acto de investigación el cual se realizará bajo su conducción y control directo.Es importante resaltar entonces, que en el Nuevo Código Procesal Penal quién dirige y conduce las investigaciones policiales en su calidad de persecutor penal, es el Ministerio Públicoy sobre esa base, la Policía siempre debe supeditar su actuar a esa premisa.

En el Distrito Judicial de Lima se cuenta con 47 Fiscales provinciales penales. Defensores de la legalidad a quienes se les presenta una realidad impostergable, la lucha contra la criminalidad informática, situación que la legislación debe tener en cuenta, conincontrolable avance en los últimos años, el Estado no toma conciencia de tal amenaza, inoperanciaEstatal que bien podría ser explicado en lo siguiente: presencia de muy pocos trabajos

científicos sobre el tema analizado (derecho informático); limitada legislación que no permite una adecuada persecución del delito; poco profesionalismo en los miembros del Ministerio Publico para el cumplimento de sus labores; presencia de un sistema corrupto; ausencia de peritos adscritos y especializados en delitos informáticos que contribuyan a formular adecuadas denuncias, ausencia de fiscales especializados en delitos informáticos, e inexistencia de tratados o convenios sobre criminalidad informática, entre otros factores (Blossiers, 2003).

2.2.7. El Poder Judicial respecto al Delito Informático

Según Espinoza (2000) la Constitución Política del Estado señala en su artículo 138 que “la potestad de administrar justicia emana del pueblo y se ejerce por el poder judicial a través de sus órganos jerárquicos con arreglo a la Constitución y a las leyes”. Así el poder judicial es autónomo en su ejercicio, en lo político, administrativo, económico, disciplinario e independiente en lo jurisdiccional, con sujeción a la ley y a su ley orgánica. Pues la Constitución Política, garantiza en su artículo 146, la independencia de los magistrados, debiendo estos estar sólo sometidos a la Constitución y a las Leyes.

Sin embargo, el escenario actual nos muestra una marcada desconfianza popular respecto a la justicia, la que podría ser reducida en el temor de los ciudadanos para acudir al órgano jurisdiccional. El mismo que se relaciona con varios elementos; de una parte la confusión a que da lugar el ropaje legal en los no iniciados, así como en la imprevisibilidad, incluso los abogados lo contagian, como ocurre en al pie del acantilado de Ribeiro, cuando el asesor

legal de los ocupantes precario de un terreno estatal les dice a modo de explicación del desalojo que ya está en curso: “los juicios se ganan o se pierden”, yo no tengo nada que ver. Y por supuesto en la tajante discrepancia entre la verdad real y la razón de la ley desconfianza en el órgano jurisdiccional que, que en realidad no solo puede ser explicado subjetivamente, sino quizás mejor enfocada contrastándola con la realidad, empecemos nombrando a un personal no calificado en informática jurídica. Pero la ineficacia del sistema judicial no puede ser resuelta solo mediante medios tecnológicos, sino que urge la provisión de mayores recursos materiales y humanos, ciertamente despejará algunos de los obstáculos que, a la hora de resolver la problemática judicial, hoy adquiere el peso de cuestiones previas. Locales adecuados, vehículos, agilización y descongestión de los despachos judiciales atiborrados de interminables volúmenes de casos, personal capacitado y bien pagados (Magistrados y personal de bajo nivel profesional que no participan en capacitaciones serias y que siguen maestrías y doctoras en Universidad poco serias, solo para la obtención de un certificado que les permita mantener sus cargos) (Peña, 2010).

2.2.8. Las tecnologías de la información y la comunicación

Según Faraldo (2009) en las dos últimas décadas han surgido distintos fenómenos (sociales, tecnológicos, etc.) que, pese a no originarse en el entorno criminal, han sido aprovechados por este para la realización de comportamientos prohibidos. El principal, sin lugar a dudas, es el fenómeno de la globalización y el portentoso desarrollo y generalización de su principal instrumento: las tecnologías de la información y de la comunicación (TIC).

Gálvez, Delgado y Rojas(2011)sostienen que con dicha expresión se busca, hacer referencia al conjunto de instrumentos desarrollados en las últimas décadas para la comunicación y la transmisión de la información. Conviene indicar que aquello puede adquirir un mayor o menor alcance si es que se la entiende o dota de un sentido amplio o restringido.

Desde una perspectiva amplia, se hace referencia tanto a las tecnologías de la comunicación (principalmente la radio, la televisión y la telefonía en todas sus formas) como a las tecnologías de la información, vinculadas principalmente con la informática, los ordenadores y las redes que permiten el rápido flujo de esa información, principalmente la Internet. La segunda perspectiva, en cambio, adquiere un significado solo centrado en aquello último (Internet) o alude a la digitalización de los datos como elemento esencial de estas nuevas tecnologías (Gálvez, Delgado, & Rojas, 2011).

De acuerdo a Díaz (2009), es preferible optar por una perspectiva amplia, que incluya tanto a las tecnologías de la comunicación (principalmente la radio, la televisión y la telefonía en todas sus formas) como a las tecnologías de la información, vinculadas principalmente con la informática, los ordenadores y las redes que permiten el rápido flujo de esa información, principalmente, la Internet; por lo que, resultaría más acertado utilizar la expresión TIC para referirse a ellas.

Según Gálvez, Delgado y Rojas (2011)en nuestro ordenamiento jurídico, la Ley n.° 30096 no se ha decantado por una u otra alternativa, posibilitando así que se le atribuya unos alcances muy amplios (la telefonía fija, el móvil, la radio y la televisión, la informática y los ordenadores, la videoconferencia, los SMS, la

Internet, entre otros). No obstante, toda vez que se emplea de manera reiterada tanto para el tipo penal de atentado contra la integridad de datos informáticos (art. 3) como también para el de atentado contra la integridad de sistema informáticos (art. 4), consideramos que hubiese sido preferible que la mencionada Ley ofrezca algunos alcances sobre lo que ha de entenderse por tecnologías de la información o de la comunicación.

Con relación a esto último, el presente trabajo buscará brindar algunos alcances sobre la nueva regulación que la Ley N° 30096 ofrece para los delitos informáticos. A fin de realizar tal tarea, se darán algunos alcances sobre el concepto de TIC y, seguidamente, se identificará el bien jurídico que al interior de la sociedad de la información puede afectarse a través de su empleo (Peña, 2010).

Finalmente, se analizarán los ilícitos previstos en los arts. 2, 3 y 4 de la nueva Ley de delitos informáticos, haciéndose especial incidencia en el de acceso ilícito o también llamado “mero” intrusismo (Suárez, 2009).

Bases teóricas especializadas sobre el tema

2.2.9. Intimidad

De las diversas definiciones se incluye la de Casabona que entiende por intimidad "aquellas manifestaciones de la personalidad individual o familiar, cuyo conocimiento o desarrollo quedan reservadas a su titular o sobre las que ejerce alguna forma de control cuando se ven implicados terceros, entendiendo por tales, tanto los particulares como los poderes públicos (Casabona, 2006).

2.2.10. Derecho a la Intimidad

Ribagorna(1996) sostiene:

El derecho a la intimidad no aparece enunciado de forma expresa y como categoría independiente en los textos constitucionales hasta fechas muy recientes. El primer texto constitucional en Europa que recogió de forma expresa el derecho a la intimidad fue la Constitución portuguesa de 1986 (art. 33.1) y posteriormente lo hizo la Constitución española de 1978 (art. 18). Anteriormente, tan sólo existieron formulaciones filosóficas y doctrinales. La elaboración doctrinal que sirve de precedente a la constitucionalización del derecho a la intimidad, concebido como "therightto be letalone" por el Juez Cooley, es decir, el derecho a ser dejado en paz, o a ser dejado solo, se originó en 1.890 cuando Warren y Brandeis publicaron un artículo sobre "TheRighttoPrivacy". Entre las formulaciones filosóficas podemos destacar la de Jeremy Bentham.

2.2.11. Defensa de la Intimidad

“Se ha tratado de defender la intimidad como un valor en sí, es decir, con independencia de la finalidad perseguida por las conductas criminales” (Ribagorna, 1996).

2.2.12. Escuelas Técnico Jurídicas Vinculantes a la Investigación

a) Escuela Técnico Jurídica

La dirección técnico penal de carácter jurídico queda expresada en América con la tendencia jurídico penal que tiene su asentamiento en Italia, y que los

alemanes también han prestado gran atención a la tendencia dogmática - jurídica. En Italia, Carnelutti aparece como un eminente técnico-jurista, que escribió con agudeza temas alusivos a los filósofos. El señalaba con énfasis que el jurista debe pretender resolver sus asuntos del Derecho con su propia técnica, obviando todo lo extraño que tiende a la alienación sociocultural de cada una de las personas (Alcalá, 1985).

Por otra parte, señalamos la urgente necesidad de separar hoy la tendencia meramente técnica, respecto a la ciencia del deber ser del Derecho, que obviamente se llama dogmática y por tanto no está debidamente desvinculada de la Filosofía, que es un aporte especializado para lograr entender con sapiencia las ciencias penales. Mejor aun cuando hoy en día es relevante e importante destacar la vinculación de la tecnología y la filosofía al enriquecimiento de la doctrina penal, que además contribuye a la humanización y sensibilización de los artículos de nuestro ordenamiento jurídico penal (Amoroso, 1991).

b) Escuela de la Antropología Criminal.

Escuela Antropológica social y/o Lyon. El fundador recae en el medico y psicólogo francés Alexander Lacassgne fue uno de los opositores de la teoría Lombrosiana. Señala, que la sociedad es el factor preponderante o la causa de la criminalidad, considera, que a mayor desorganización y esta situación tiene estrecha relación con el problema, los objetivos y las hipótesis en cuanto a la personalidad formada, mayor criminalidad. Esto hace, que los estados desorganizados sea más alta la criminalidad (Toniatti, 1991).

Según Garbarino, Curbelo, Pernovich yWonsiak(1990), en cambio los estudios sociológicos y jurídicos nos conducen a pensar que en las sociedades mejor organizadas, existe menos criminalidad. Esto implica que las sociedades tienen los criminales que se merecen, de esta manera se reafirma el carácter eminentemente social. Mayor cuando la sociedad es tolerante, frente a las insinuaciones exógenas que realizan. La sociedad desorganizada, es debida entre otros factores, a la carencia de la planificación social y económica. Recordemos que la familia puede hacer mucho entre la primera y segunda infancia y en la niñez en cambio es difícil pero no imposible. Que una deficiente conducta se logra corregir en la adolescencia, se da señala Lacassgne pero con bastante o suma dificultad.

El medico biólogo Lois Paster señalaba, que un microbio solo prolifera en un medio adecuado, haciendo énfasis al trabajo de Lacasgne, donde el delincuente venía siendo un microbio, y actúa solamente teniendo a su disposición el medio social, ese medio ambiente propio para cometer el ilícito. Si el sujeto activo, hubiese sido preparado adecuadamente en el seno de su hogar paterno-materno y con determinado estimulo emocional y afectivo, probablemente no entraría tan fácil en la senda del mal. Y la sociedad se ahorraría el tiempo necesario para no procesar a estas gentes, que en la práctica tenga conductas ilícitas, como consecuencia a la formación de su personalidad (Garbarino, Curbelo, Pernovich, & Wonsiak, 1990).

c) Teoría de la sociedad de riesgos

De acuerdo a Velasco(2010) en la dogmática penal actual hay un nuevo paradigma el de la “sociedad de riesgos” Se dice que la sociedad actual es una sociedad de riesgos, en la que se admiten evidentemente dentro de ciertos límites los riesgos que se derivan del tráfico rodado, ferroviario y aéreo, dela utilización de gases de la existencia de centrales nucleares, necesarias para facilitar energía eléctrica, pero que amenazan parte de la civilización, la producción y comercialización de productos de carácter alimenticio en grandes cantidades, con grave riesgo para los consumidores, la manipulación genética con peligro de selección de razas, a través de la creación de seres humanos por clonación, etc..

Baratta (1985) afirma que esta innegable realidad exige la comprensión de la sociedad. Son riesgos exigidos por la modernización e industrialización de la sociedad, que sin duda plantean y seguirán planteando nuevas necesidades al derecho penal a lo largo de los próximos años. Pues bien como un claro fenómeno asociado a estos “nuevos riesgos” de la sociedad se encuentra la informática. No cabe duda que la informática proporcione muchos beneficios pero al mismo tiempo origina no pocos riesgos, porque al generar una abundante información, en poco tiempo y en un espacio muy reducido, puede afectar a la esfera privada del individuo.

En este sentido la existencia de bancos de datos personales y su posible manipulación puede afectar a la intimidad de las personas.

En España, afortunadamente la Ley orgánica de regulación del tratamiento automático de datos de Carácter personal, de 29 de octubre de 1992, proporciona la protección administrativa de esta información, cuidando el uso de dichos datos personales (Mir Puig, 1992).

d) Teorías en relación al derecho a la intimidad

Son múltiples las teorías y posiciones doctrinales que se han esgrimido para delimitar el contenido del derecho a la intimidad. Pérez Luño (1984), parte del planteamiento de delimitar conceptualmente la intimidad, con la que llama "noción actual de la privacy", porque considera que la intimidad y la vida privada, contienen una carga emotiva que las hace equívocas, ambiguas y dificulta la precisión de su significado, e incluso se llega a sostener que tiene una "definición introuvable" (Vitalis, 1981).

Entre las varias doctrinas referentes al tema, entre otras, se citan:

1. La Alemana de Hubmann, que reconoce tres esferas: la intimsphäre (secreto), la Privatsphäre (lo íntimo) e Individual sphäre (individualidad de la persona. Vg. nombre).
2. La Italiana de Frosini, que distingue cuatro fases de aislamiento: soledad, intimidad, anonimato y la reserva.
3. La Norteamericana de Jhon H. Shattuck, sostiene que la privacy abarca cuatro aspectos, a saber:

    a) FreedomFromunreasablesearch, libertad o seguridad frente a cualquier tipo de intromisión indebida en la esfera privada.

b) Privacyofassociation and belief, garantía del respeto a las opciones personales en materia de asociación o creencias.
c) Privacy and autonomy, tutela de la libertad de elección sin interferencias.
d) Information control, posibilidad de los individuos y grupos de acceder y controlar las informaciones que les atañen. La posición de Shattuck, estuvo precedida por Alain Westin,

Charles Fried y L. Lusky, al menos en lo referente al control de la información que tiene toda persona sobre sí misma. Westin, lo llamó derecho al control de la información referente a uno mismo (TheRightto control information aboutoneself); Lusky, posibilidad de controlar la circulación de informaciones relevantes para cada sujeto y Fried, control sobre las informaciones que nos conciernen (Fried & Lusky, 1968).

e) Teoría de los delitos contra la honestidad.

Honestidad (Del Latín*honestitas, átis*) implica en la práctica, docencia y moderación en el desempeño de las funciones que realizan las personas, así como en sus palabras y en las múltiples funciones que efectúa cotidianamente, incluyendo su hogar. La persona decente es sinónimo de modesto y decoroso (Peña, 2010).

Velasco (2010)Afirma que según el derecho babilónico de la época de Hamurabi, al que besaba a una mujer casada se le debía cortar el labio inferior.

Según el derecho indio, se hacía culpable de adulterio el que no se conducía decentemente con una mujer ajena o le hacía indicaciones equivocas.

Según Peña (2010) en la sociedad alemana de la época en que se escribió esa información, la figura jurídica honestidad estaba referida, exclusivamente, al honor, disciplina, lealtad y honestidad, que se esperaba de los varones a favor de este género. Con el transcurrir del tiempo, esta figura jurídica se hizo extensivo a otros delitos como es, el de comportarse bien, tener ética, valores morales, etc., en cualquier actividad que la persona realiza.

f) Teoría de las subculturas criminales

De acuerdo a Baratta y Silverrnagl(1985) existe una relación de reciprocidad y compatibilidad entre la teoría funcionalista y la teoría de las subculturas criminales. La primera estudia la relación funcional del comportamiento desviado con la estructura social, el plano sobre el que se desarrolla la teoría de las subculturas criminales “tal como se presenta desde sus primeras formulaciones por obra de Clifford R. Shaw y de Frederic M. Thasher hasta Sutherrland, se preocupan sobre todo de estudiar el modo como la subcultura delictiva se comunica a los delincuentes y deja por tanto sin resolver el problema estructural del origen de los modelos subculturales del comportamiento y la comunican que se comunican.

Pero desde el momento en que, con la obra de Albert K. Cohen, el alcance de las teorías de las subculturas criminales se amplía desde el plano de los fenómenos del aprendizaje subsiste entre las dos teorías un terreno de

encuentro, que ha llevado generalmente más de una integración que a una mera compatibilidad" (Peña, 2010).

Existe una integración entre la teoría funcionalista y la teoría de las subculturas criminales. Así lo sostiene Pavarini, cuando afirma que "si se asume que la estructura social de una determinada sociedad ofrecen oportunidades diversas para la consecución de las metas culturales y que esta desigual distribución de los chances de servirse de medios legítimos está en función de la estratificación social, por lo que existen algunos que están siempre y objetivamente excluidos de ella, entonces el método funcionalista de la anomia puede abastecerse de una base explicativa y teórica para la formación de subculturas criminales". La estructura de la sociedad ofrece situaciones importantes, también desaciertos (Paravarini, 1993).

Velasco(2010) sostiene que el concepto de subcultura nace en la sociología criminal para explicar la conducta desviada de ciertas minorías; criminalidad de jóvenes y adolescentes de clases bajas organizados en bandas. Respecto a las organizaciones de banda, esta, pues carece de pretensiones generalizadoras.

Además, su surgimiento a partir de la década de los cuarenta es tardío, siendo identificado a partir de la obra de Cohen. El presupuesto común de las teorías subculturales es que la delincuencia es una respuesta solución cultural compartida, a los problemas creados por la estructura social (Peña, 2010).

Según Baratta y Silverrnagl (1985) es opinión dominante que a las subculturas corresponden las siguientes características: a) la subcultura es un grupo de

rasgos diferentes en relación a la sociedad oficial porque institucionaliza especiales formas de ver el mundo o cosmovisiones; b) su código axiológico o sistema de valores cuenta con cierta autonomía sin llegar a independizarse de la cultura dominante; c) la subcultura tiene una organización interna que regula las relaciones de sus miembros; d) las subculturas surgen en un modelo de sociedad plural y heterogénea.

De acuerdo a Garcia(1988) el proceso de interacción con otras personas que padecen semejante problemas de adaptación social genera un sentimiento de solidaridad de grupo y determinados estándares comunes. Es un mecanismo sustitutivo de participación social y prepara al joven para una carrera criminal de adulto, razón por la cual que todas estas teorías relacionan adolescencia de los delincuentes de clase baja, las bandas y subculturas y carreras delictivas. Estas subculturas también son de aplicación en nuestra realidad nacional.

Bases Legales.

Marco Jurídico Nacional

Según (Ley Nº 30096, 2013, art. 6):

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

Artículo 7. Interceptación de datos informáticos

Según (Ley Nº 30096, 2013, art. 7):

> El que, a través de las tecnologías de información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.
>
> La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.
>
> La pena privativa de libertad será no menor de ocho años ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales

Otras figuras delictivas del Código Penal Peruano

Artículo 181-A.- Explotación sexual comercial infantil y adolescente en ámbito del turismo.

Según (Ley Nº 29408, 2009, art. 181):

> El que promueve, publicita, favorece o facilita el turismo sexual, a través de cualquier medio (…) electrónico, magnético o a través de internet,

con el objeto de ofrecer relaciones sexuales de carácter comercial de personas de 14 y menos de 18 años de edad.

Artículo 183-A.- Pornografía infantil

Según (Ley Nº 28251, 2004, art. 183-A):

> El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o pública, importa o exporta por cualquier medio incluido el internet, (…) escritos, imágenes visuales o auditivas, (…) de carácter pornográfico, en los cuales se utilice a personas de 14 y menos de 18 años de edad.

(MINJUS, 2016):

> **Falsificación de documentos**
>
> **Artículo 247.-** El que hace uso de un documento falso o falsificado, como si fuese legítimo, siempre que de su uso pueda resultar algún perjuicio. El que viola la intimidad de la vida personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios.

(MINJUS, 2016):

> **Uso indebido de archivos computarizados.**
>
> **Artículo 157.-** El que, indebidamente, organiza, proporciona o emplea cualquier archivo que tenga datos referentes a las convicciones políticas o religiosas y otros aspectos de la vida íntima de una o más personas,

será reprimido con pena privativa de libertad no menor de 1 ni mayor de 4 años.

(MINJUS, 2016):

Artículo 217.- Reproducción, difusión, distribución y circulación de obra sin autorización del autor

(…) el que con respecto a una obra, (...) realiza alguno de los siguientes actos sin la autorización previa y escrita del autor o titular de los derechos:

a. La modifique total o parcialmente.
b. La distribuya mediante venta, alquiler o préstamo público.
c. La comunique o difunda públicamente por cualquiera de los medios o procedimientos reservados al titular del respectivo derecho.
d. La reproduzca, distribuya o comunique en mayor número que el autorizado por escrito.

La pena será no menor de cuatro años ni mayor de ocho y con sesenta a ciento veinte días multa, cuando el agente la reproduzca total o parcialmente, por cualquier medio o procedimiento y si la distribución se realiza mediante venta, alquiler o préstamo al público u otra forma de transferencia de la posesión del soporte que contiene la obra o producción que supere las dos (2) Unidades Impositivas Tributarias, en forma fraccionada, en un solo acto o en diferentes actos de inferior importe cada uno.

Marco Jurídico Internacional

Estados Unidos.

La legislación destinada a reprimir el delito informático se encuentra bastante dispersa, aunque son dignas de mención el Acta Federal de Abuso informático, de 1994 que modifico el Acta de Fraude y Abuso informático de 1986, “Communications DecrecyAct”, declarada inconstitucional por la Corte Suprema y la “Child Online ProtectionAct”.

España.

Se ha optado por intermedio del proceso de reforma del Código Penal de 1995, hacer frente a las emergentes formas de criminalidad a través de referencias expresas en figuras tradicionales. Así tenemos menciones exprofeso a cuestiones informáticas en los delitos de descubrimientos o revelación de secretos, Robo, Estafa, contra los derechos intelectuales y descubrimiento de secreto empresarial.

En el ámbito extrapenal es la LOPD la normativa que regula el tratamiento automatizado de datos y pretende garantizar el honor la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos.

Alemania.

El fenómeno informático se inscribe en la legislación penal germana a través de la Segunda Ley contra la Criminalidad económica que incorporo una serie de delitos relacionados al uso indebido de los sistemas informáticos, así aparecen a) el espionaje informático (art. 202 C.P.), fraude informático (art.263 C.P.), falsedad informática (art.269 C.P.), alteración de datos (art.303-A C.P.),

sabotaje informático (art.303-B C.P.) y la utilización indebida de tarjetas de crédito (art. 266-B C.P.)

Portugal.

La criminalidad informática en el país luso h a sido abordad a través de la Ley 109/92. Esta norma contiene 19 artículos que se aplican subsidiariamente al Código Penal.

El legislador portugués no solo ha tipificado los delitos de falsedad informática (art. 4), daños informáticos (art. 5) sabotaje informático (art.6), intrusismo informático (art. 7), intercepción ilegal (art. 8), sino que establece un glosario de términos (art. 2), una clausula sobre responsabilidad penal de las personas jurídicas (art. 3 y 10) y un conjunto de consecuencias jurídicas y medidas accesorias (art. 11 al 19).

Francia.

En Enero de 1998 se promulgo en Francia la ley N°88-19 sobre Fraude Informático que reprime el intrusismo informático (462-3 y 462-4 C.P.) y falsificación informática (art.462-5 y 462-6 C.P.).

Canadá.

En Canadá existen una serie de preceptos relacionados a la criminalidad informática: La sección 342.1 del código Penal reprime el acceso no autorizado de ordenadores (unathorizad use of a computer), las sección 430 sanciona el daño a datos informáticos (mischiefto data), asimismo, tenemos la sección 326 que sanciona la sustracción de servicios de telecomunicaciones

(theftoftelecommunicationsrrvice), todas estas conductas se encuentran sancionadas con pena de prisión no mayor de 10 años.

Austria.

A partir de Diciembre de 1987, mediante una ley de reforma del Código Penal, se incorporó en dicho país dos tipos penales relacionados a la cuestión informática: el sabotaje informático (art. 126 C.P.) y el fraude informático (art.148 C.P.).

Chile.

La vecina nación chilena ha sido una de las pioneras en la regulación de los delitos informáticos en nuestra región, ya desde 1993, por medio de la Ley 19,223 se introdujo en el ordenamiento de Chile una serie de delitos cometidos a través de computadoras.

Las conductas punibles son dos básicamente el sabotaje informático (art. 1 y 3 de la Ley N°19,223) y el espionaje informático (art. 2 y 4 de la Ley N°19,223). La figura de intrusismo informático se encuentra subsumida dentro de la definición del delito de espionaje informático. Las penas previstas para dichos delitos será de presidio menos en su grado medio a |máximo – en delito de sabotaje informático – y de presidio menor en su grado mínimo a medio – en el delito de espionaje informático.

Paraguay.

El código Penal de Paraguay incluye algunas importantes prescripciones referidas al ámbito informático, así tenemos que se reprimen los delitos de

alteración de datos, el sabotaje informático, el fraude por medio de ordenadores y la destrucción o daño de documentos.

En otros Países

Aunque es unánime el interés por la problemática de los delitos informáticos, no obstante a lo afirmado, actualmente se vienen planteando una serie de propuestas siendo las de mayor interés en nuestro país la de México, Colombia, y la Unión Europea.

2.2.13. Marco Histórico

La Internet y su influencia en las sociedades contemporáneas trajo consigo la llamada “Sociedad de la Información”; En nuestro país Internet es representada por la Red Científica Peruana, organismo que funciona de manera autónoma, sin ningún tipo de aporte económico foráneo, su objetivo es el intercambio de información y desarrollo de las telecomunicaciones; esta institución en pocos años, ha difundido enormemente su contenido. Internet no es sino un conjunto de redes que se conectan a través de un protocolo común de comunicación que es el TCP/IP (Transfer Control Protocol/Internet Protocol). Dentro de Internet se comprende a la World Wide Web (www o web) que permite que la información de cualquier red interconectada a Internet pueda ser localizada sin importar su ubicación física. El punto de inicio de funcionamiento del Internet radica en que cada computadora resulta identificada a través del numero IP. Los protocolos se expresan a través de números binarios por conveniencia expresados en forma decimal, sin embargo, esta forma de expresión solo resulta adecuada para los técnicos, mas no para el usuario, creándose así los nombres de dominio “domainnames” (Barriuso, 2000).

Los nombres de dominio no son otra cosa que la dirección de Internet consignada en palabras, de forma tal que resulta fácilmente comprensible para el usuario de Internet. El funcionamiento de este sistema de nombres de dominio (“domainnamessystem” DNS) es a través de bases de datos con listas de los nombres de dominio y susrespectivas direcciones IP. El “domainname” se compone de dos elementos uno identificador (ejemplos conocidos “yahoo”, “terra”, etc) y otro que sirve para hacer referencia al nivel al que pertenecen (“com”, “edu”, “gob”, etc.). La asignación de los nombres de dominio corresponde hoy en dia a “Internet CorporationforAssignedNames and Numbres” o ICANN, entidad que se encarga de la administración del sistema de nombres de dominio (Barriuso, 2000).

Los dominios se clasifican en: dominio de nivel superior (“Top LevelDomains” o TLD) y dominios de segundo, tercer o cuarto nivel. Los TLD comerciales, “org” para organizaciones, etc.), dominios especiales para entidades que cumplen con ciertos requerimientos (“edu” para entidades educativas, “gov-int” para internacionales, etc.) y dominios internacionales o territoriales (“pe” para Perú, “es” para España, “ar” para Argentina, entre otros). La administración de estos ha recaído sobre las entidades que resultaron ser las primeras en cada país en conectarse a Internet (Lara, 1996).

En paralelo, la informática, Derecho y Derecho Informático, no fueron ajenos a este desarrollo, ya en el año 1962, Philippe Dreyfus emplea el término “Informatique” para unificar dos conceptos: “información” “automática”, con lo que se nace una nueva disciplina, esto es, la Informática se convertiría en el

método que iba a servir para afrontar las cuestiones propias del Derecho (Rondinel, 1995).

Al respecto es acertada la definición planteada por PerezLuño (1984), para quien la Informática Jurídica; “estudia el tratamiento automatizado de las fuentes de conocimiento jurídico, por lo que su objeto será “la aplicación de la tecnología de la información al derecho”. Sin embargo, la tecnología informática tiene implicancias que van más allá de la mera aplicación en el derecho y que se encontraban relacionadas a su propia regulación, es así como surge el Derecho Informático como la materia jurídica que comprende al conjunto de disposiciones que regulan las nuevas tecnologías de la información y la comunicación, esto es la informática y la telemática.

De acuerdo a Calderón (2000) en este contexto la actual “Sociedad de la Información” y la “desmaterialización” del Derecho, aparecen nuevas tecnologías que propiciaron un verdadero “cambio de paradigmas”, el antiguo paradigma de la escritura sobre papel se ha transformado en paradigma de la información digital. Esta información, que antes de la aparición de la informática y las redes de interconexión se encontraba confinada en bibliotecas, con la aparición del fenómeno informático ha sido trasladada, de las bibliotecas oscuras y húmedas, a las computadoras y luego a las redes y el internet, generándose un fenómeno tan impresionante. Tal ha sido la repercusión que ha provocado el fenómeno cibernético en el manejo de la información de nuestras sociedades que se ha optado por denominar a nuestra era como la “era de la información” y a nuestra moderna sociedad como la “Sociedad de la Información”.

Esto, en el Derecho, tiene repercusiones bastante evidentes y que se relacionan con la denominada “desmaterialización del Derecho”Trazegnies (1998). La aparición de las redes de interconexión y el Internet han acelerado dicha desmaterialización, lo que guarda íntima relación con la propia naturaleza del entorno digital, citemos, por ejemplo, el caso de Internet, que sin ser un “lugar” es un “lugar. Y es que por ella circulan grandes cantidades de información digitalizada, de allí que se le conozca como “súper carretera de información”, “aldea global” “red de redes”, “red de cobertura geográfica mundial”, “ciberespacio” acuñado originalmente por William Gibson (Rowland, 1998).

Dentro de este fenómeno de nueva incriminación aparecen conductas que vulneran bienes jurídicos no convencionales y a su vez comportamientos que se realizan empleando medios no convencionales para lesionar bienes jurídicos convencionales. Ambos, por lo general, tienen intrínsecos connotaciones tecnológicas, debido a la incidencia que la evolución tecnológica a tenido en el cambio social, tal como hemos afirmado. El uso generalizado de la red Internet se debe a sus propias características, las mismas que Christine Mayewski ha descrito de manera didáctica, estas son: la facilidad de su uso, su bajo costo, su velocidad, sus capacidades y la ausencia de límites geográficos (Zaffaroni, 1981).

Tal necesidad, generada desde comienzos de década en sociedades altamente informatizadas, se ha trasladado a sociedades como la nuestra, el reflejo de los avances tecnológicos ha tenido gran influjo en el campo de la criminalidad en tanto este nuevo “modus operandi” permite captar vacíos en el Derecho Penal

tradicional, quedando indefensos “los contenidos inmateriales del sistema informático, su integridad, su disponibilidad o su exclusividad (Cafure de Battistelle, 1995).

III. METODO

3.1. TIPO DE INVESTIGACIÓN

El tipo de investigación es descriptivo explicativo, porque se dará una medida correctiva para la satisfacción integral de los operadores de justicia y las personas involucradas, lográndose así la efectividad de las hipótesis y objetivos establecidos. Descriptivo porque incluye un análisis y su relación, se aplicara la metodología positivista con el uso de las técnicas cuantitativas de investigación; Por ello se utilizara de manera combinada, los métodos inductivo-deductivo, analítico-sintético.

Prospectivo. Porque nuestro estudio pretende utilizar información en el tiempo que no ha sido utilizada para datos de estudio.

Nivel de Investigación

El nivel de investigación es de corte transversal del tipo prospectivo, que nos permitió ir a la búsqueda de la explicación científica y su aplicación al Derecho en general y al Derecho penal de manera específica.

3.2. POBLACIÓN Y MUESTRA

Población

La población es de 40 policías, 59 jueces y 59 fiscales adscritos a los juzgados y fiscalías del distrito Judicial de Lima siendo un total de 158 entrevistados.

Muestra

Proporcionalidad de la Muestra

Para el cálculo del tamaño muestral se consideró un nivel de confianza de 95 % y un error de 5 %.

Datos: N = 158

Z = 95%

p = 50%

q = 1-p

e = 5%

Se calculó haciendo uso de la siguiente fórmula.

0.3173628	X	59	=	18.72 Jueces
0.3173628	X	59	=	18.72 Fiscales
0.3173628	X	40	=	12.69 Policías

Por lo tanto la muestra fue conformada por 50 entrevistados, de las cuales 19 fueron jueces, 19 fiscales y 12 policías e ser entrevistados en total.

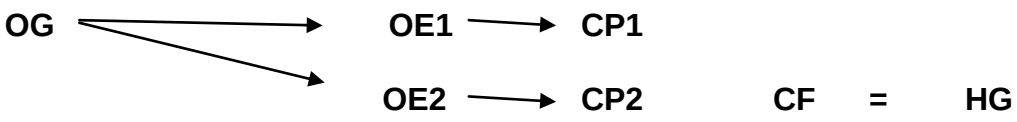
3.3. HIPÓTESIS

H1: “La causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) es el desacierto en la tipificación de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, en el Distrito Judicial de Lima”

Ho: “La causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) es el acierto en la tipificación de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, en el Distrito Judicial de Lima”

Diseño de investigación

La investigación por su diseño será por “Objetivos”, conforme a los resultados que se obtendrán de acuerdo al esquema que se acompaña:



Dónde:

OG = Objetivo General.

OE = Objetivo Específico.

CP = Conclusión Parcial.

CF = Conclusión Final.

HG = Hipótesis General

Estrategia de prueba de hipótesis

La utilidad de este estudio de los delitos informáticos y la protección penal de la intimidad no se limita a la creación de nuevas teorías, porque existe un amplio reconocimiento de su utilidad en la exploración y descripción de aspectos novedosos o poco conocidos de la justicia peruana, cuyos resultados representan avances significativos, con un alto potencial de utilidad en la práctica penal. Pese a ello, en los circuitos académicos, la mayor parte de la atención que se presta a la valoración de la investigación mediante estudio de casos está asociada a determinar su capacidad para realizar prueba de

hipótesis, que es el ámbito donde debe competir con las metodologías cuantitativas, y donde éstas presentan sus máximas fortalezas.

En este diseño para responder y explicitar en términos académicos como en los adecuados para el trabajo de campo cual es la evidencia necesaria para aceptar o rechazar las hipótesis, en qué fuentes se debe obtener dicha evidencia, como debe ser triangulada para garantizar su objetividad, cuáles son sus escalas de medición, etc. Esto conduce a la formalización de un protocolo que además de evidenciar la lógica que une hipótesis y datos colectados, constituye la base de la tesis que resultará de la investigación y para ello se hizo uso de la regresión y correlación r de Pearson para determinar qué tan intensa es la relación entre las dos variables.

3.4. OPERACIONES DE VARIABLES

Variable Independiente

X= Operadores de justicia.

Indicadores:

- Ausencia de formación tecnológica en delincuencia informática.
- Desconocimiento de la Deontología Tecnológica.
- Transgresiones de las legislaciones vigentes.

Variable Dependiente

Y= Investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad

Indicadores

- Impropia determinación del tipo penal.
- Inadecuada determinación del daño causado.
- Insuficiente cálculo del monto indemnizatorio.

Técnicas de investigación

Para el recojo de estas informaciones, fue necesario utilizar, entre otras las siguientes técnicas: la entrevista, el análisis de contenidos, observación de la realidad problemática en relación a lo que propusimos en el universo, sesiones académicas con asesoría técnica especializada. Los cuales nos permitió obtener información, confiable y segura para la demostración de las hipótesis y cumplimiento de los objetivos del presente trabajo.

Se realizó de la siguiente manera:

- Se ha puesto en conocimiento de las personas objetivo de la investigación a realizarse para la autorización.
- La entrevista fue personal y anónimo; con la finalidad de evitar sesgos y mantener confidencialidad en cuanto a la información recogida.
- Se procesó la información recogida para el desarrollo de la investigación.

Técnica.

Se utilizó como técnica una encuesta para evaluar los delitos informáticos y la protección penal de la intimidad.

a. Encuestas a operadores de justicia como. Jueces y Fiscales

b. Encuesta a Policías

3.5. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El instrumento empleado fue una encuesta de 25 preguntas a responder para evaluar los delitos informáticos y la protección penal de la intimidad previa determinación de rubros, que comprenden personas e instituciones: a Jueces, Fiscales y miembros de la Policías.

3.6. PROCESAMIENTOS

Los datos fueron procesados haciendo uso del paquete estadístico SAS versión 8.1 para Windows y los resultados se presentan en tablas y gráficos haciendo uso de la estadística descriptiva e inferencial.

Se procedió a elaborar las encuestas a base de preguntas con respuestas alternativas referente al problema de investigación, se mandó a reproducir los mismos para el uso o rellenado adecuado de éstos. Una vez, preparados todos los materiales y los instrumentos a utilizar se procedió a realizar la entrevista a las personas seleccionadas.

3.7. ANÁLISIS DE DATOS

Encuesta. La encuesta fue aplicado previamente mediante una prueba piloto del 10 % y fue validado mediante la prueba de alfa de crombach, que es una media ponderada de las correlaciones entre las variables que forman parte de la escala y valides con R de Pearson; Puede calcularse de dos formas: a partir de las varianzas (alpha de Cronbach) o de las correlaciones de los ítems (Alpha de Cronbach estandarizado).

Cuadro 1. Estadístico de fiabilidad, Alpha de Cronbach del instrumento.

Alfa de Cronbach	N de elementos
0.9001877	24

Fuente: Base de datos de la encuesta.

IV. RESULTADOS

4.1. CONTRASTACIÓN DE HIPÓTESIS

Tabla 1. Análisis de correlación de los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012.

Operadores de justicia en la protección penal de la intimidad	**Delitos informáticos**				**TOTAL**
	Desacierto		**Acierto**		
	O	**E**	**O**	**E**	
Favorable	7	6.8	4	4.1	11
Regular	5	5	3	3.3	8
Desfavorable	3	3.1	2	1.8	5
TOTAL	**15**		**9**		**24**

Fuente: Instrumento para evaluar los delitos informáticos y la protección penal de la intimidad

Cálculo de la Chi-Cuadrado:

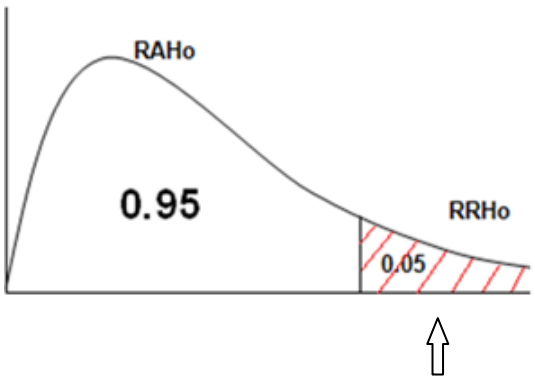
$$X^2 = \frac{\sum(O-E)^2}{E} = \frac{(7-6.8)^2}{6.6} + \frac{(5-5)^2}{5} + \frac{(3-3.1)^2}{3.1} + \frac{(4-4.1)^2}{4.1} + \frac{(3-3.3)^2}{3.3} + \frac{(2-1.8)^2}{1.8} = X^2 = 0.061042133$$

Hipótesis Estadística:

H1: "Las causas de desacierto de la labor de los operadores de justicia influyen en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el Distrito Judicial de Lima"

H0: "Las causas de desacierto de la labor de los operadores de justicia no influyen en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el Distrito Judicial de Lima"

Región Crítica:



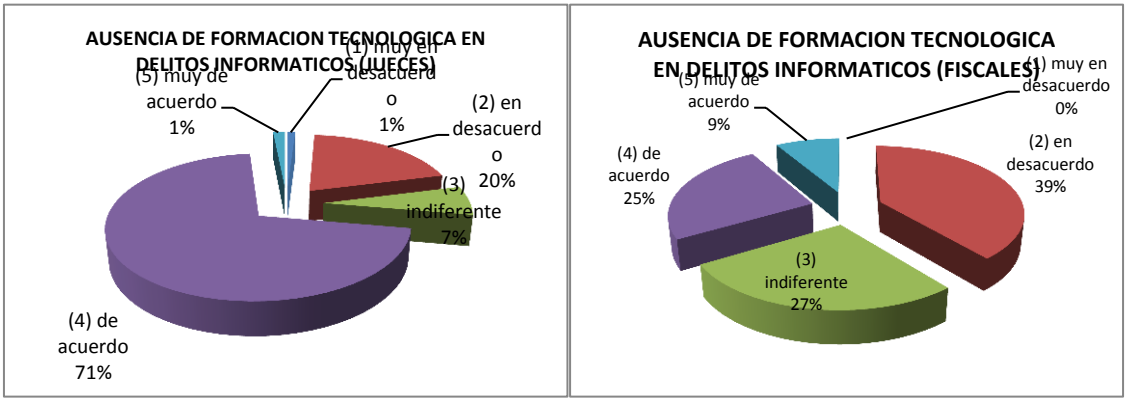
X^2= 0.061042133

Descripción: En la región crítica se observa que el valor de la Chi-cuadrado es 0.061042133, la cual cae en la región de rechazo de la hipótesis nula (RRHo); es decir, se demuestra que las causas de desacierto de la labor de los operadores de justicia influyen en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el Distrito Judicial de Lima.

4.2. ANÁLISIS E INTERPRETACIÓN

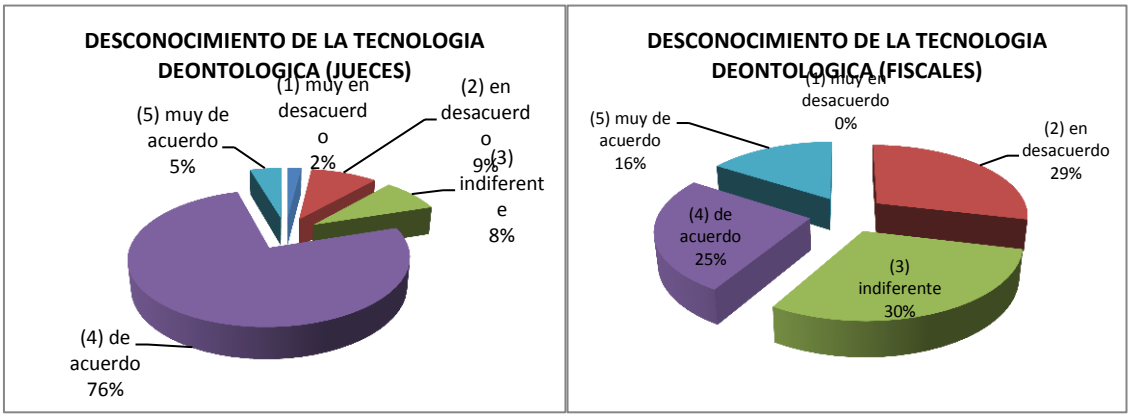
Al analizar el primer objetivo para conocer la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima, se tiene que en la ausencia de formación tecnológica en delitos informático los jueces están de acuerdo en 71%, los fiscales en 25%, (ver figura 1), y la policía solo en 21%. Ahora se encontró también que los jueces están en desacuerdo en 20% los fiscales en 39% y los policías en 31%(ver anexo 4).

Figura 1. Opinión de jueces, fiscales y policía en ausencia de formación tecnológica en delitos informático.



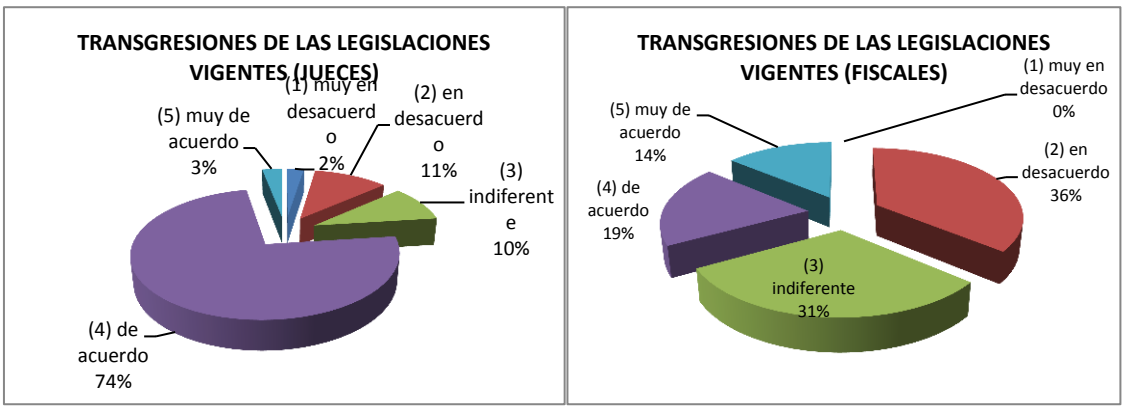
En la figura 2, se analiza el desconocimiento de la tecnología deontológica, donde los jueces están de acuerdo en 76%, los fiscales en 25% y los policías en 40%. Los que están en descuerdo se tiene que los jueces en 9%, para los fiscales en 29% y para los policías en 25% (ver anexo 5).

Figura 2. Opinión de jueces, fiscales y policía en desconocimiento de la tecnología deontológica.



En la figura 3, se analiza transgresiones las legislaciones vigentes, donde los jueces estan de acuerdo en 74% y en desacuerdo el 9%, los fiscales en 19% y en desacuerdo el 29%, los policias en 16%, los que estan en desacuerdo el 34% (ver anexo 6).

Figura 3. Opinión de jueces, fiscales y policía en transgresiones de las legislaciones vigentes.



En la figura 4, se analiza la impropia determinación del tipo penal, donde los jueces están de acuerdo en 72% y en desacuerdo en 11%, los fiscales de acuerdo en 20% y en desacuerdo en 34%, los policías de acuerdo en 53%, los que están en desacuerdo el 30% (ver anexo 7).

Figura 4. Opinión de jueces, fiscales y policía en la impropia determinación del tipo penal.

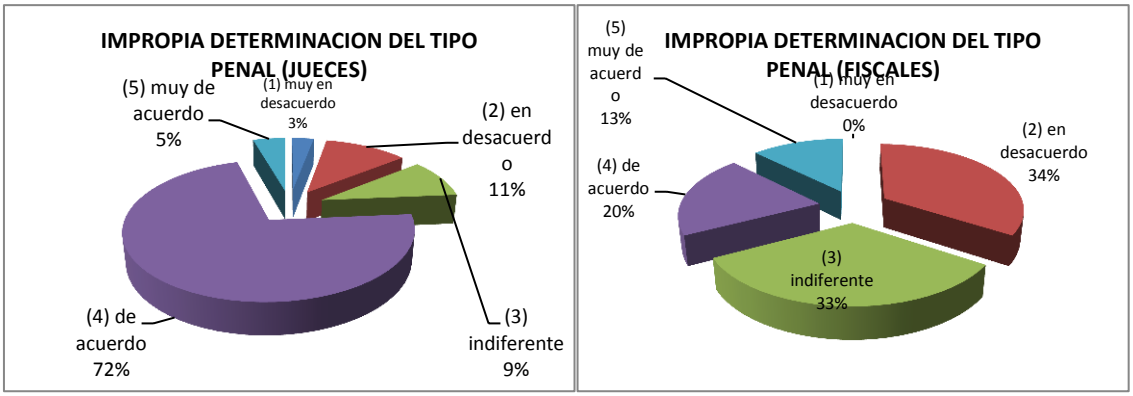
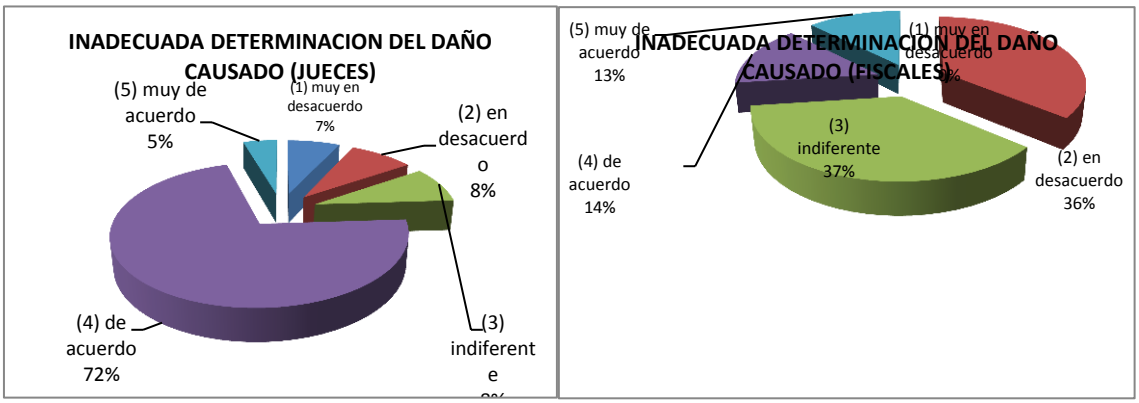
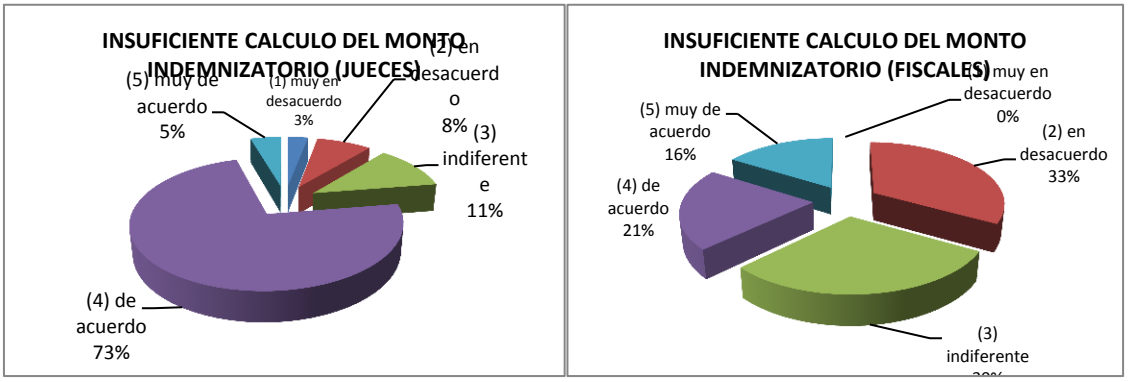


Figura 5. Opinión de jueces, fiscales y policía en la inadecuada determinación del daño causado.



En la figura 5, se analiza la inadecuada determinación del daño causado, donde los jueces están de acuerdo en 72% y en desacuerdo e indiferente en 8%, los fiscales de acuerdo en 14%, indiferente en 37% y en desacuerdo en 36%, los policías de acuerdo en 36%, los que están en desacuerdo el 39% (ver anexo 8).

Figura 6 Opinión de jueces, fiscales y policía en el insuficiente cálculo del monto indemnizatorio.



En la figura 6, se analiza el insuficiente cálculo del monto indemnizatorio, donde los jueces están de acuerdo en 73%, indiferente en 11% y en desacuerdo en 8%, los fiscales de acuerdo en 21%, en desacuerdo en 33% e indiferente en 30%, los policías de acuerdo en 13%, los indiferentes en 32% y en desacuerdo el 30% (ver anexo 9).

Al analizar el segundo objetivo para determinar la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima, se hizo un análisis de regresión de la base de datos obtenidos de los encuestados tanto de jueces, fiscales y policías, donde se encontró que si los jueces están de acuerdo que el desconocimiento de la deontología tecnológica afecta la competitividad de los operadores de justicia, de su institución que está, bien reconocida influye en 58% sobre si esta de acuerdo, que la impropia determinación del tipo penal, afecta la competitividad

en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad a un nivel de significancia de 0.001.

Si los jueces están de acuerdo, que con mayores facilidades del estado, en términos de una especialización, de los operadores de justicia sobre delitos informáticos podría favorecer el desarrollo, e su institución influye en 30% sobre el acuerdo que la inadecuada determinación del daño causado, afecta a la víctima en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad.

Al preguntar a los jueces y policías están de acuerdo, que los operadores de justicia de su institución se encuentra preparado para pronunciarse eficazmente sobre la responsabilidad civil en sede penal como lo está para pronunciarse sobre la responsabilidad criminal, sin que se produzcan transgresiones a las legislaciones vigentes influye en 29% sobre la impropia determinación del tipo penal, afecta la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad, ver Tabla 2.

Tabla 2.

Análisis de regresión múltiple de los operadores de justicia sobre investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad.

Variable Independiente: Operadores de justicia	**Variable Dependiente: Investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad**	**R-Square**	**P value**
X6: (Jueces) Desconocimiento de deontología tecnológica afecta la competitividad de los operadores de justicia, de su institución que está, bien reconocida?	X13: (Jueces) Impropia determinación penal, afecta investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	58	<.0001
X3: (Jueces) Mayor facilidad del estado, en especialización, de operadores de justicia en delitos informáticos que favorece desarrollo de institución.	X18: (Jueces) Inadecuada del daño causado, afecta en investigación y juzgamiento de delitos informáticos en protección penal de intimidad.	30	<.0001
X11: (Jueces) (Policías) Operadores de justicia preparado en responsabilidad civil como está pronunciarse sobre responsabilidad criminal, sin transgresiones a legislaciones vigentes	X13: (Jueces) (Policías) Impropia determinación penal, afecta investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad	29	<.0001
X1: (Fiscales) Ausencia de tecnología en delitos informáticos, de operadores de justicia, es obstáculo para un ejercicio eficiente y eficaz	X20: (Fiscales) Cambios para escases de procesal judicial de investigación y juzgamiento de delitos informáticos	10	0.0207
X12: (Policías) Sería útil contar con marco teórico actualizado de los delitos informáticos, para los operadores no transgredan las legislaciones vigentes	X13: (Policías) Impropia determinación penal, afecta investigación y juzgamiento de los delitos informáticos en protección penal de la intimidad	49	<.0001
X12: (Policías) Sería útil contar con marco teórico actualizado de los delitos informáticos, para los operadores no transgredan las legislaciones vigentes	X14: (Policías) Fiscal con tecnología informática y jurídica, puede combatir la impropia penal, en investigación de los delitos informáticos.	49	<.0001
X12: (Policías) Sería útil contar con marco teórico actualizado de los delitos informáticos, para los operadores no transgredan las legislaciones vigentes	X15: (Policías) La impropia penal, en perjuicio del agraviado en investigación y juzgamiento de delitos informáticos en protección de la intimidad	47	<.0001
X12: (Policías) Sería útil contar con marco teórico actualizado de los delitos informáticos, para los operadores no transgredan las legislaciones vigentes	X16: (Policías) La impropia penal, representa desconocimiento de informática en investigación y juzgamiento de los delitos informáticos	37	<.0001

Al preguntar a los fiscales si está de acuerdo que la ausencia de formación tecnológica en delitos informáticos, de los operadores de justicia, es un obstáculo para un ejercicio eficiente y eficaz de su función influye en 10% sobre algunos cambios en su ámbito para poder atender la escases de la celeridad procesal judicial de la investigación y juzgamiento de los delitos informáticos en la protección de la intimidad.

Al preguntar a los policías si está de acuerdo, que sería útil contar con marco teórico actualizado de los delitos informáticos, para los operadores no transgredan las legislaciones vigentes, vemos que influye en 49% sobre la impropia determinación del tipo penal, afecta la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad y si el fiscal, contara con el auxilio de la tecnología informática y jurídica, se podría combatir la impropia determinación del tipo penal, en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad, también en ?, en 47% sobre la impropia determinación del tipo penal, redunda en perjuicio del agraviado en la investigación y juzgamiento de los delitos informáticos en la protección de la intimidad y en 37% sobre la impropia determinación del tipo penal, representa un desconocimiento de la informática jurídica actualizada en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad, ver Tabla 2.

V. DISCUSION DE RESULTADOS

5.1. DISCUSIÓN

En nuestro análisis para conocer la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad la ausencia de formación tecnológica en delitos informático los jueces están de acuerdo en 71%, los fiscales en 25%, la policía solo en 21%. Los jueces están en desacuerdo en 20% los fiscales en 39% y los policías en 31%.

Al analizar las transgresiones las legislaciones vigentes, donde los jueces están de acuerdo en 74% y en desacuerdo el 9%, los fiscales en 19% y en desacuerdo el 29%, los policías en 16%, los que están en desacuerdo el 34%. Al analizar el la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima, los jueces están de acuerdo que el desconocimiento de la deontología tecnológica afecta la competitividad de los operadores de justicia, de su institución que está, bien reconocida influye en 58% sobre si está de acuerdo, que la impropia determinación del tipo penal, afecta la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad

En Ecuador, Acosta (2012), dice que en su mayoría los Jueces de la Sala Especializada de lo Penal, Miembros del Tribunal y Jueces de Garantías

Penales de Cotopaxi, así como los Fiscales y profesionales del derecho en libre ejercicio investigados; conocen sobre lo que es el delito informático y desconocen el procedimiento que hay que seguir en los mismos por no existir la presencia de estas causas en nuestro medio, en su esencia se lo realizó como ayuda para solucionar los problemas de administración de Justicia Penal, que existe para sancionar este tipo de delitos. Se ha determinado que los en cargados de la administración de justicia y profesionales en libre ejercicio, tienen la necesidad de conocer la normativa penal vigente en materia referente a delitos informáticos, para acceder a los beneficios y saber cuáles son las limitantes que la ley impone a los ciudadanos sobre el tema de los delitos informáticos.

Si los jueces están de acuerdo que, con mayores facilidades del estado, en términos de una especialización, de los operadores de justicia sobre delitos informáticos podría favorecer el desarrollo, de su institución influye en 30% sobre el acuerdo que la inadecuada determinación del daño causado, afecta a la víctima en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad.

Los jueces y policías están de acuerdo, que los operadores de justicia de su institución se encuentra preparado para pronunciarse eficazmente sobre la responsabilidad civil en sede penal como lo está para pronunciarse sobre la responsabilidad criminal, sin que se produzcan transgresiones a las legislaciones vigentes influye en 29% sobre la impropia determinación del tipo penal, afecta la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad.

5.2. CONCLUSIONES

- Para conocer la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad, se encontró que los jueces aceptan que existe ausencia de formación tecnológica en delitos informáticos, pero los fiscales y policías dicen estar en desacuerdo. También los jueces aceptan que existen desconocimiento de la tecnología, para los fiscales son indiferentes.
- Los jueces y fiscales aceptan que hay transgresiones de las legislaciones vigentes. Los jueces están de acuerdo con la impropia determinación del tipo penal, los fiscales en desacuerdo al igual que los policías.
- Los jueces están de acuerdo con la inadecuada determinación del daño causado, los fiscales indiferentes y los policías en desacuerdo. Los jueces están de acuerdo con el insuficiente cálculo del monto indemnizatorio, los fiscales en desacuerdo y los policías indiferentes.
- Se advierte que dentro de este cumulo de desaciertos o inexactitudes, en el trabajo de los operadores de justicias, se trata de defender la intimidad como un valor en sí, es decir con independencia de la finalidad perseguida por las conductas criminales.
- Para determinar la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad, se encontró que la deontología tecnológica que afecta la competitividad de los operadores de justicia influye en la impropia determinación del tipo penal

y en la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad.

- Los jueces están de acuerdo, en términos de una especialización, de los operadores de justicia sobre delitos informáticos podría favorecer el desarrollo, e su institución influye sobre el acuerdo de la inadecuada determinación del daño causado.
- Los jueces y policías están de acuerdo, que los operadores de justicia de su institución se encuentran preparado para pronunciarse eficazmente sobre la responsabilidad civil en sede penal como lo está para pronunciarse sobre la responsabilidad criminal.

5.3. RECOMENDACIONES

- Continuar con este estudio, por ejemplo, respecto a la prevención social para reducir los delitos informáticos con una adecuada comprensión de este tipo de conductas.
- Que el Estado implemente medidas que posibiliten la disminución de las situaciones carenciales básicas, de las instituciones formales como el Poder Judicial, Ministerio Publico y Policía Nacional, que conlleven a reducir las desigualdades y concilien conflictos no resueltos.

5.4. REFERENCIAS

Acosta, B. (2012). *Los delitos informáticos y su perjuicio en la sociedad.* Latacunga, Ecuador: Universidad Técnica de Cotopaxi Unidad Académica de Ciencias Administrativas y humanísticas. Recuperado de http://repositorio.utc.edu.ec/bitstream/27000/197/1/T-UTC-0224.pdf.

Alcalá, N. (1985). *Derecho procesal mexicano. S.N.E.* México: Porrúa.

Amoroso, Y. (1991). La informática como objeto de derecho. Algunas consideraciones acerca de la protección jurídica en Cuba de los Datos Automatizados. *Revista Cubana de Derecho*(1).

Aniyar de Castro, L. (1980). El delito de cuello blanco en América Latina, una investigación necesaria. *Revista ILANUD al día, 3*(8), 79-81.

Artega, A. (1987). El delito informático: algunas consideraciones jurídico penales. *Revista de la Facultad de Ciencias Jurídicas y Políticas, 33*(68), 125-133.

Baratta, A., & Silverrnagl, M. (1985). La Legislación de Emergencia y el Pensamiento Jurídico Garantista. *Revista Doctrina Penal*, 559-595.

Barriuso, C. (2000). Nombres de Dominio (DNS), en Internet. En *Libro de ponencias del VII Congreso Iberoamericano de Derecho e Informática* (págs. 31-47). Lima: Editora Perú.

Blossiers, J. (2003). *Criminalidad informática.* Lima: Editorial Portocarrero.

Cafure de Battistelle, M. (1995). *El Delito Informático en la agenda internacional, en cuadernos del departamento del Derecho Penal y Criminología* . Córdoba: Universidad Nacional de Córdoba.

Calderón, C. (2000). Perú. El impacto de la era digital en el derecho. *REDI Revista Electrónica de Derecho Informático*(21).

Callegari, L. (1985). Delitos Informáticos y Legislación. *Revista de la Facultad de Derecho y Ciencias Políticas de la Universidad Pontificia Bolivariana*, 113-118.

Casabona, C. (2006). De los delitos informáticos al cibercrimen. Una aproximación conceptual y político-criminal. En *El cibercrimen: Nuevos retos jurídico-penales, nuevas respuestas político-criminales.* Granada.

Díaz, F. (2009). *Los derechos humanos ante los nuevos avances científicos y tecnológicos. Genética e internet ante la Constitución.* Valencia: Tirant lo Blanch.

Elías, R. (2014). *Luces y sombras en la lucha contra la delincuencia informática en el Perú.* Lima: Hiperderecho. Recuperado de http://www.hiperderecho.org/wp-content/uploads/2014/07/01_delitos_informaticos_elias.pdf

Espinoza, J. (2000). La firma digital en el Perú a propósito del reglamento de la Ley 27269 - Ley de firmas y certificados digitales. *Derecho informático y comercio electrónico.*

Faraldo, P. (2009). *Las nuevas tecnólogias en los delitos contra el patrimonio y orden socioeconómico.* Valencia: Tirant Io Blanch.

Fernández, L., Cabezudo, J., Arenas, M., Herrera, R., & Gastelu, J. (2010). Diseño de herramientas de control y medidas de prevención para evitar ser víctimas de Delitos Informáticos. *Fernández, L,. Cabezudo, J. Arenas , M. Herrera, R. Gastelu , J.* Perú: Policía Nacional del Perú. Recuperado de http://www.buenastareas.com/ensayos/Dise%C3%B1o-De-Herramientas-De-Control-Inform%C3%A1tico/1245461.html

Fried, C., & Lusky, L. (1968). Privacy. *Yale Law Journal, 77*, 475-493.

Gálvez, T., Delgado, W., & Rojas, R. (2011). *Derecho penal: parte especial, Volumen 1.* Instituto Derecho y Justicia - Jurista Editores.

Garbarino, A., Curbelo, C., Pernovich, M., & Wonsiak, M. (1990). Nuevas normas jurídicas en materia informática. *Revista de la Asociación de Escribanos del Uruguay, 76*(1), 68-78.

Garcia, A. (1988). *Manual de Criminologia, Introduccion y teorías de la criminalidad.* Madrid: Espasa Calpe.

Gonzáles, J. (2013). *Delincuencia Informática: Daños Informáticos del Artículo 264 del Código Penal y Propuesta de Reforma*. (tesis de doctorado), Madrid, España: Univesidad Complutense de Madrid. Recuperado de http://eprints.ucm.es/23826/1/T34976.pdf.

Landa, C., & Velazco, A. (2007). *Constitución Política del Perú.* Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú.

Lara, J. (1996). *Manueal de Informática y Derecho.* Barcelona: Editorial Ariel.

Ley General de Turismo. Ley Nº 29408. Diario Oficial El Peruano, Lima, Perú. (18 de septiembre de 2009).

Ley de Delitos Informáticos. Ley Nº 30096. Diario Oficial El Peruano, Lima, Perú. (22 de octubre de 2013).

Ley que Modifica e incorpora artículos referidos a la Violación sexual, explotación sexual comercial y pornografía infantil. Ley Nº 28251. Diario Oficial El Peruano, Lima, Perú. (7 de junio de 2004).

Magliona, C., & López, M. (2003). *Delincuencia y Fraude Informático. Derecho Comparado y Ley 19233.* Santiago: Editorial Jurídica de Chile.

Ministerio de Justicia y Derechos Humanos. (2016). *Código Penal.* Lima: Ministerio de Justicia y Derechos Humanos.

Mir Puig, S. (1992). *Delincuencia informática.* Barcelona: Editorial PPU.

Novello, F. (2010). *Delitos informáticos y algunas de sus implicancias procesales.* Recuperado el 13 de Abril de 2016, de Ministerio de Seguridad de Argentina: www.minseg.gob.ar/download/file/fid/892

Paravarini, M. (1993). *Control y dominación.* Mexico: Siglo XXI Editores.

Peña, A. (2010). *Derecho penal: parte especial* (2da ed.). Lima: Idemsa.

Pérez, A. (1984). *Derechos Humanos, Estado de Derecho y Constitución.* Madrid: Tecnos.

Reyna, L. (2002). *Manual de Derecho penal económico: parte general y especial.* Lima: Gaceta jurídica.

Ribagorna, A. (1996). *Seguridad de las tecnologías de información. Ámbito jurídico de las tecnologías de la información.* Consejo General del Poder Judicial.

Romeo, C. (2012). La penetración del Derecho penal económico en el marco jurídico europeo: los delitos contra los sistemas de información. En Romeo Casabona , & Flores Mendoza, *Nuevos instrumentos jurñidicos en la lucha contra la delincuencia económica y tecnológica.* Granada: Editorial Comares.

Rondinel, R. (1995). *Informática Jurídica. De la Teoría a la Práctica.* Lima.

Rowland, D. (1998). Cyberspace: A World Apart? En *Ponencias dela 13º Conferencia de la British & Irish Legal Education Technology Association: "The Changing Jurisdiction".* Dublin.

Salf, M. (1994). *Delitos Informáticos de carácter económico.* Buenos Aires: Editores del Puerto.

Salinas, R. (2006). *Delitos contra el patrimonio.* Lima: Jurista Editores.

Silva, J. (2006). *a. La expansión del Derecho penal. Aspectos de la Política criminal en las sociedades postindustriales* (2da ed.). Montevideo-Buenos Aires.

Suárez, A. (2009). *La estafa informática.* Bogotá: UNAB – Grupo Editorial Ibañez.

Toledo, J. (2001). *Delitos emergentes en internet y el desafío de Carabineros de Chile en la prevención y control en la era informática*. (tesis de pregrado), Chile: Carabineros de Chile - Academia de Ciencias Policiales.

Toniatti, R. (1991). Libertad Informática y Derecho a la Protección De Los Datos Personales: Principios de Legislación Comparada. *Revista Vasca de Administración Pública*(29), 139 -162.

Trazegnies, F. (1998). La Desmaterialización del derecho. Del derecho de pernada al Internet. *Themis*, 7-14.

Velasco, E. (2010). *Delitos cometidos a través de Internet. Cuestiones procesales.* Madrid: La Ley – Grupo Wolters Kluwer.

Vera, A. (1996). *Delito e informática: la informática como fuente de delito.* Santiago: Editorial La Ley .

Villavicencio, F. (2014). Delitos Informáticos. *IUS ET VERITAS*(49), 284-304.

Vitalis, A. (1981). *Informática, poder y libertades.* París: Economica.

Zaffaroni, E. (1981). Reflexiones político-criminales sobre la tutela penal de los derechos de autor . En *Conferencia Continental de derecho de autor.* Buenos Aires: Instituto Interamericano de Derecho de Autor (IIDA).

VI. ANEXOS

Anexo 1. Matriz de consistencia

TITULO: "Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012"

Problema	**Objetivos**	**Hipótesis**	**Variables**	**Indicadores.**	**Metodología**
Problema general: ¿Cuál es la causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, distrito Judicial de Lima? **Problemas específicos:** • Se puede conocer la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima. • Se puede determinar la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima.	**Objetivo general:** Conocer la causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, distrito Judicial de Lima **Objetivos específicos:** •Conocer la situación de la labor de los operadores de justicia en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima. •Determinar la opción factible que influye en el desacierto de la labor de los operadores de justicia, en la investigación y juzgamiento de los delitos informáticos y la protección penal de la intimidad en el Distrito Judicial de Lima.	**Hipótesis general:** H1: "La causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) es el desacierto en la tipificación de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, en el Distrito Judicial de Lima" Ho: "La causa que influye en la inexactitud del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) es el acierto en la tipificación de los delitos informáticos en la protección penal de la intimidad en el periodo 2008 al 2012, en el Distrito Judicial de Lima"	**Variable independiente:** X= Operadores de justicia. **Variable independiente:** Y= Investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad	Ausencia de formación tecnológica en delincuencia informática. Desconocimiento de la Deontología Tecnológica. Transgresiones de las legislaciones vigentes. Impropia determinación del tipo penal. Inadecuada determinación del daño causado. Insuficiente cálculo del monto indemnizatorio.	**Tipo de investigación:** descriptiva **Nivel de investigación:** Explicativo**.** **Población y Muestra** **Población.** La población es de 40 policías, 59 jueces y 59 fiscales adscritos a los juzgados y fiscalías del distrito Judicial de Lima siendo un total de 158 entrevistados.. Por lo tanto la muestra fue conformada por 50 entrevistados, de las cuales 18 fueron jueces, 18 fiscales y 12 policías e ser entrevistados en total. . **Técnicas e Instrumentos de Recolección de Datos** Para el recojo de estas informaciones, fue necesario utilizar, entre otras las siguientes técnicas: la entrevista, el análisis de contenidos, observación de la realidad problemática en relación a lo que propusimos en el universo, sesiones académicas con asesoría técnica especializada. Los cuales nos permitió obtener información, confiable y segura para la demostración de las hipótesis y cumplimiento de los objetivos del presente trabajo. **Técnicas Estadísticas de Análisis y Procesamiento de Datos** Análisis de correlación y análisis de regresión

Anexo 2. Encuesta a los Operadores de Justicia

La presente encuesta tiene como objetivo explicar la causa que influye en el desacierto del trabajo de los operadores de justicia (Policías, Fiscales y Jueces) en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad, en el Distrito Judicial de Lima. Estimados señores Operadores de Justicia, mucho les agradeceremos responder con la mayor objetividad la presente encuesta. Ello redundará en una investigación veraz que incidirá en nuestro futuro trabajo jurisdiccional.

Marque con una X los criterios según el caso

Datos generales:

Cargo: …….....Sexo: ……..... Edad: ……..

Titular……..…..Provisional: ……..……

Suplente: ……..… Supernumerario: ……...…..

VALORACION

1. Muy en desacuerdo 2. En desacuerdo 3. Indiferente 4. De acuerdo 5. Muy de acuerdo

Nº	ITEMS	
AUSENCIA DE FORMACION TECNOLOGICA EN DELITOS INFORMATICOS		
1	¿Está Ud. de acuerdo que la ausencia de formación tecnológica en delitos informáticos, de los operadores de justicia, es un obstáculo para un ejercicio eficiente y eficaz de su función?.	
2	¿Está Ud. de acuerdo, que la ausencia de formación tecnológica en delitos informáticos,	

	de los operadores de justicia se encuentra en sintonía con las necesidades de su institución?	
3	¿Esta Ud. de acuerdo, que con mayores facilidades del estado, en términos de una especialización, de los operadores de justicia sobre delitos informáticos podría favorecer el desarrollo, e su institución?	
4	¿Esta Ud. de acuerdo, que la ausencia de formación tecnológica en delitos informáticos, de los operadores de justicia, incide en la celeridad de sus funciones?	
DESCONOCIMIENTO DE LA TECNOLOGIA DEONTOLOGICA		
5	¿Esta Ud. de acuerdo, que el desconocimiento de la deontología tecnológica, de los operadores de justicia, afecta la imagen de su institución?	
6	¿Está Ud. de acuerdo que el desconocimiento de la deontología tecnológica afecta la competitividad de los operadores de justicia, de su institución que está, bien reconocida?	
7	¿Esta Ud. de acuerdo que el desconocimiento de la deontología tecnológica podría incidir en el desarrollo de calidad, de los operadores de justicia, de su institución?	
8	¿Esta Ud. de acuerdo, que el desconocimiento de la deontología tecnológica, de los operadores de justicia, de su institución es equiparable con las instituciones pares de los países de la región?	
TRANSGRESIONES DE LAS LEGISLACIONES VIGENTES		
9	¿Esta Ud. de acuerdo que la ley especial sobre delitos informáticos vigente, constituye un complemento necesario del ordenamiento ya existente, pero, que ello provoca que se cometan transgresiones a las legislaciones vigentes, por parte de los operadores de justicia?	
10	¿Esta Ud. de acuerdo que los operadores de justicia experimentaron cambios que se produjeron en el funcionamiento de su institución, a partir de la entrada en vigencia de la Ley de delitos informáticos, que se manifestaron en transgresiones a las legislaciones vigentes?	
11	¿Esta Ud. de acuerdo, que los operadores de justicia de su institución se encuentra preparado para pronunciarse eficazmente sobre la responsabilidad civil en sede penal como lo está para pronunciarse sobre la responsabilidad criminal, sin que se produzcan transgresiones a las legislaciones vigentes?	
12	¿Esta Ud. de acuerdo, que sería útil contar con marco teórico actualizado de los delitos informáticos, para los operadores no transgredan las legislaciones vigentes?	

VALORACION

1. Muy en desacuerdo 2. En desacuerdo 3. Indiferente 4. De acuerdo 5. Muy de acuerdo

Nº	ITEMS	
IMPROPIA DETERMINACION DEL TIPO PENAL		
13	¿Esta Ud. de acuerdo, que la impropia determinación del tipo penal, afecta la competitividad en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
14	Esta Ud. de acuerdo, que si el fiscal, contara con el auxilio de la tecnología informática y jurídica, se podría combatir la impropia determinación del tipo penal, en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
15	¿Esta Ud. de acuerdo, que la impropia determinación del tipo penal, redunda en perjuicio del agraviado en la investigación y juzgamiento de los delitos informáticos en la protección de la intimidad?	
16	¿Esta Ud. de acuerdo, que la impropia determinación del tipo penal, representa un desconocimiento de la informática jurídica actualizada en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
INADECUADA DETERMINACION DEL DAÑO CAUSADO		
17	¿Esta Ud. de acuerdo, que se cumpliría con una adecuada determinación del daño causado, si su institución contara con una guía crimino informática actualizada para favorecer la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
18	¿Esta Ud. de acuerdo que la inadecuada determinación del daño causado, afecta a la víctima en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
19	¿Esta Ud. de acuerdo, que una preparación calificada en crimino informática y asistencia técnica, enriquece y favorece la adecuada determinación del daño causado, en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
20	¿Está Ud. de acuerdo, que se necesitan algunos cambios en su ámbito para poder atender la escases de la celeridad procesal judicial de la investigación y juzgamiento de los delitos informáticos en la protección de la intimidad?	
INSUFICIENTE CALCULO DEL MONTO INDEMNIZATORIO		
21	¿Está Ud. de acuerdo, que es apremiante la necesidad de una actualización profesional calificada en delitos informáticos, para revertir el insuficiente cálculo del monto indemnizatorio, en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
22	¿Está Ud. de acuerdo, que existe descontento en la mayoría de los perjudicados respecto al insuficiente cálculo del monto indemnizatorio en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad, por ello la falta de credibilidad en la administración de justicia?	

23	¿Está Ud. de acuerdo, que es serio el papel que le corresponde a su institución, respecto de la función reparatoria en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	
24	¿Está Ud. de acuerdo, que la cifra negra de los delitos informáticos no se conoce con certeza, por una impropia determinación del tipo penal y una adecuada determinación del daño irrogado y perjuicio producido en la investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad?	

Anexo 3. Definición de términos

- **Acceso Ilícito**.- El hecho de ingresar o la intención de ingresar sin autorización, o a través del acceso de un tercero, a un sistema de información, permaneciendo o no en él.
- **Afectar**.- Alterar, provocar anomalías en cualquiera de las operaciones a realizar por un programa, software, sistema, red de trabajo, o la computadora misma, impidiendo su uso normal por parte del usuario.
- **Acción Penal**.- Es la exteriorización de la voluntad indispensable para la actuación del Derecho penal objetivo. Es, por tanto la base y la razón de ser del proceso penal, haciendo legitimo su normal desenvolvimiento.
- **Acción Publica**.- La acción penal, salvo los casos expresamente determinados por la ley, debe iniciarse de oficio, ejercitada obviamente por el ministerio público, sin perjuicio del Derecho de acusar o de intervenir como parte querellante en el juicio.
- **Acto Preparatorio del Delito**.- La actividad criminal comienza con actos previos que, en sí, no son punibles.
- **Acusación**.- Es la acción del representante del Ministerio Público o de personas con que se pide al juez penal que castigue el delito cometidos por el acusado.
- **Adware**. El adware es el software que utilizan los programas de spyware, que durante su funcionamiento despliega publicidad de

distintos productos o servicios. Estas aplicaciones incluyen código adicional que muestra la publicidad en ventanas emergentes o a través de una barra que aparece en la pantalla. Esta práctica se utiliza para subvencionar económicamente la aplicación, permitiendo que el usuario la obtenga por un precio más bajo e incluso gratis y, por supuesto, puede proporcionar al programador un beneficio, que ayuda a motivarlo para escribir, mantener y actualizar un programa valioso. Algunos programas adware son también shareware, y en estos los usuarios tiene la opción de pagar por una versión registrada o con licencia, que normalmente elimina los anuncios.

- **Agraviado.**- El damnificado por el delito. Es la víctima de una ofensa o perjuicio que se ha irrogado a sus derechos e intereses.
- **Ataques de Autenticación**: Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password.
- **Bomba lógica.** Es una parte de código, insertada en un programa informático intencionadamente que permanece oculto hasta cumplirse una o más condiciones pre programadas, en ese momento se ejecuta una acción maliciosa.
- **Ciberespacio.** El auge de las comunicaciones entre ordenadores, cuyo máximo exponente es la macrored mundial Internet, ha creado un nuevo espacio virtual, poblado por millones de datos, en el que se

puede “navegar” infinitamente en busca de información. Se trata, en una contracción de cibernética y espacio, del ciberespacio.

- **Caballos de Troya**: Programas que introducen conjunto de instrucciones no autorizadas. Consiste en introducir en un sistema conocido por el autor de la maniobra y desconocido por la víctima, un programa a través del cual el autor puede acceder a ese u otros programas del usuario.
- **Causa Criminal**.- Es el expediente que se inicia con la presentación de la denuncia ante las autoridades, competentes, hasta el nivel de pronunciamiento de la sentencia y el fallo del más alto nivel del tribunal.
- **Código De Acceso**.- Información o contraseña que autentica a un usuario autorizado en un sistema de información, que le permite el acceso privado y protegido ha dicho sistema.
- **Código de Identificación**.- Información, clave o mecanismo similar, que identifica a un usuario autorizado en un sistema de información.
- **Código Malicioso**.- Todo programa, documento, mensaje y/o secuencia de cualquiera de estos, en un lenguaje de programación cualquiera, que es activado induciendo al usuario quien ejecuta el programa de forma involuntaria y que es susceptible de causar algún tipo de perjuicio por medio de las instrucciones con las que fue programado, sin el permiso ni el conocimiento del usuario.

- **Copiado de Fuentes**: Consiste en que empleados de una empresa obtienen una copia de un determinado software hecho a medida de ésta, lo modifican y lo venden como si fuera un desarrollo propio.
- **Clonación**.- Duplicación o reproducción exacta de una serie electrónica, un número o sistema de información, que le permite el acceso privado y protegido a dicho sistema.
- **Delito.** Culpa, crimen, violación o quebrantamiento de la ley. Acción u omisión voluntaria, que la ley castiga con pena grave.
- **Delito de Alta Tecnología**.- Aquellas conductas atentatorias a los bienes jurídicos, protegidos por la Constitución, las leyes, decretos, reglamentos y resoluciones relacionadas con los sistemas de información. Se entenderán comprendidos dentro de esta definición los delitos electrónicos, informáticos, telemáticos, cibernéticos y de telecomunicaciones.
- **Firma electrónica.** Datos cifrados de tal manera que el receptor pueda comprobar la identidad del transmisor.
- **Hackers.** Usuario de ordenadores especializado en penetrar en las bases de datos de sistemas informáticos estatales con el Fin de obtener información secreta. En la actualidad, el término se identifica con el de delincuente informático, e incluye a los cibernautas que realizan operaciones delictivas a través de las redes de ordenadores existentes. Experto que puede conseguir da un sistema informático cosas que sus creadores no imaginan.

- **Informática.** Ciencia que estudia el tratamiento automático y racional de la información, a través de los ordenadores. Este término se refiere a lo mismo que computación, solo que informática tiene origen francés y computación origen inglés.
- **Internet.** Conjunto de redes de ordenadores creada a partir de redes de menos tamaño, cuyo origen reside en la cooperación de dos universidades estadounidenses. Es la red global compuesta de limes de redes de área local y de redes de área extensa que utiliza un protocolo para proporcionar comunicaciones de ámbito mundial a hogares, negocios, escuelas y gobiernos.
- **Información.** Tras la revolución industrial, se habla de la revolución de la información, que se ha convertido en el mayor valor de las empresas y de las personas. El auge, proliferación y universalización de sistemas de interconexión global como Internet, ha llevado a hablar de la sociedad de la información como el nuevo paradigma del mundo en que vivimos.
- **Microforma.** Es una figura jurídica con un alto componente informático, creada en el Perú para que las imágenes de los documentos digitalizados tengan el mismo valor probatorio que un documento en papel.
- **Passwords.** Es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se

les permite el acceso. Aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

- **Programas.** Es un conjunto de instrucciones que una vez ejecutadas realizarán una o varias tareas en una computadora. Sin programas, estas máquinas no pueden funcionar correctamente. Al conjunto general de programas, se le denomina software y así, se refiere al equipamiento lógico o soporte lógico de una computadora digital.
- **Pharming.** Es una variante de Phishing, pero más sofisticada. A través de esta acción, los ladrones de datos consiguen que las páginas visitadas no se correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca online. El internauta introducirá sus datos confidenciales sin ningún temor, sin saber que los está remitiendo a un delincuente.
- **Phishing.** Los phishers simulan pertenecer a entidades bancarias de reconocido prestigio y solicitan a los cibernavegantes datos de tarjetas de crédito o claves bancarias, a través de un formulario o un correo electrónico con un enlace que conduzca a una falsa página web, con una apariencia similar a la de la web original. En este caso, es el propio incauto internauta quien proporciona los datos requeridos, permitiendo al autor del ilícito lograr un beneficio económico ilegitimo.
- **Piratería De Software.** Es en principio el copiado y la utilización no autorizada de programas protegidos por las leyes de copia o fuera de lo

establecido en el contrato de licencia del mismo. Esto puede tener como agravante la venta del soft a terceros. Puede efectuarse sobre textos, fotografías, y ahora aún el diseño de las páginas Web.

- **Prehacking.** Es la utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio.
- **Red Informática**. Interconexión entre dos o más sistemas informáticos o entre sistemas informáticos y terminales remotas, incluyendo la comunicación por microondas medios ópticos, electrónicos o cualquier otro medio de comunicación, que permite el intercambio de archivos, transacciones y datos, con el fin de atender las necesidades de información y procesamiento de datos de una comunidad, organización o un particular.
- **Seguridad.** Calidad de seguro. Condición de ciertos mecanismos que aseguran el buen funcionamiento de alguna cosa.
- **Sujeto Activo**.- Es aquel que intencionalmente viole o intente violar, por acción, omisión o por mandato cualquiera las actuaciones descritas en la Ley.
- **Sujeto Activo**.- Es aquel que se sienta afectado o amenazado en cualquiera de sus derechos por la violación de las disposiciones previstas en la Ley.
- **Spoofing.** Técnica para conseguir el nombre o pasword de un usuario legítimo, una vez que se ingresa al sistema consiguiendo este nombre

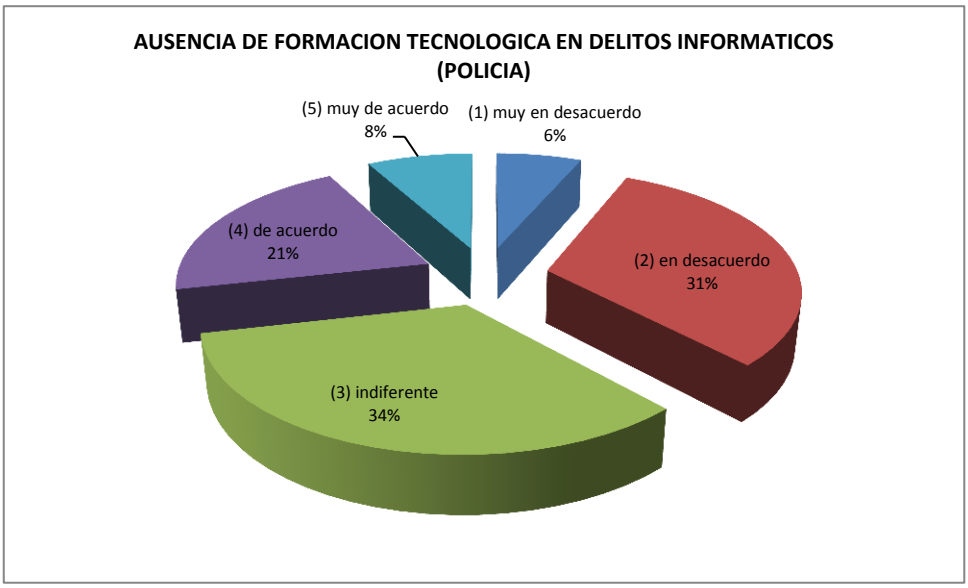
se puede cometer cualquier tipo de actos irregulares en nombre del legítimo usuario. Ejemplo envío de falsos e-mails.

- **Spyware.** Los programas espía o spyware son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos. Persona física o jurídica que adquiere de manera, legitima bienes o servicios de otra.
- **Snooping.** Obtener información sin modificarla por curiosidad y también con fines de espionaje o de robo.
- **Spam.** Son mensajes electrónicos (habitualmente de tipo comercial) no solicitados y en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. Otras tecnologías de internet que han sido objeto de spam incluyen mensajes, grupos de noticias usenet, motores de búsqueda y blogs. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.
- **Sistema de Información**. Dispositivo o conjunto de dispositivos que utilizan las tecnologías de información y comunicación, así como cualquier sistema de alta tecnología, incluyendo, pero no limitado a los

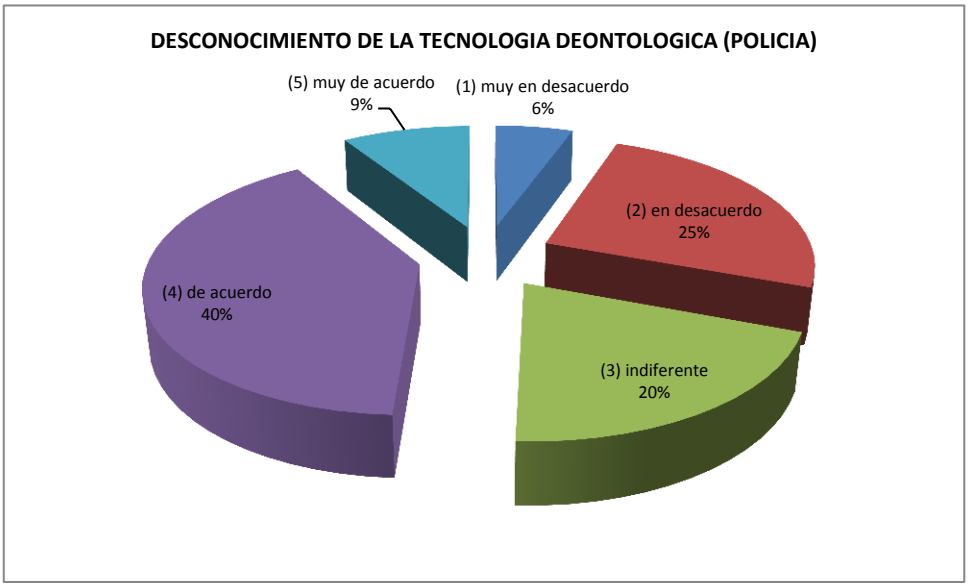
sistemas electrónicos, informáticos, de telecomunicaciones y telemáticos, que separado o conjuntamente sirvan para generar, enviar, recibir, archivar o procesar información, documentos digitales, mensajes de datos, entre otros.

- **Sistema Electrónico**. Dispositivo o conjunto de dispositivos que utilizan los electrones en diversos medios bajo la acción de campos eléctricos y magnéticos, como semiconductores o transistores.
- **Sistema Informático**.- Dispositivo o conjunto de dispositivos relacionados, conectados o no, que incluyen computadoras u otros componentes como mecanismos de entrada, salida, transferencia y almacenaje, además de circuitos de comunicación de datos y sistemas operativos, programas y datos para el procesamiento y transmisión automatizada de datos.
- **Tecnología.** Conjunto de los conocimientos propios de las ciencias. Tratado de los términos técnicos.

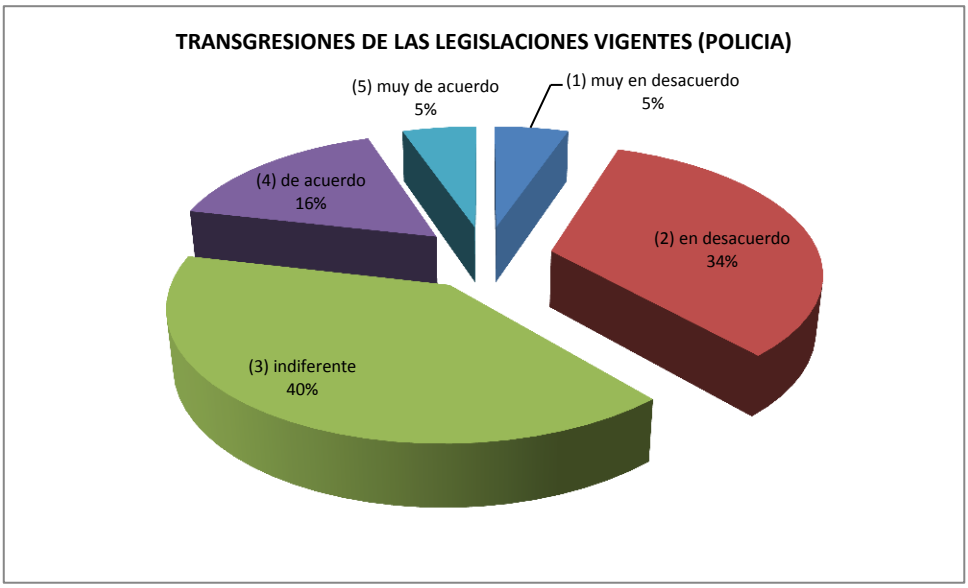
Anexo 4. Ausencia de formación tecnológica en delitos informáticos.



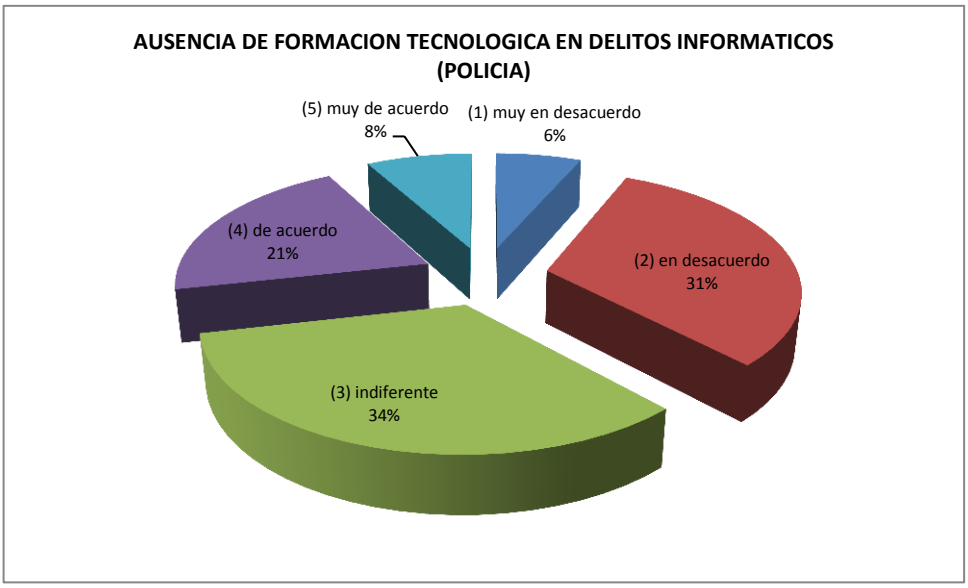
Anexo 5. Desconocimiento de la tecnologia deontologica.



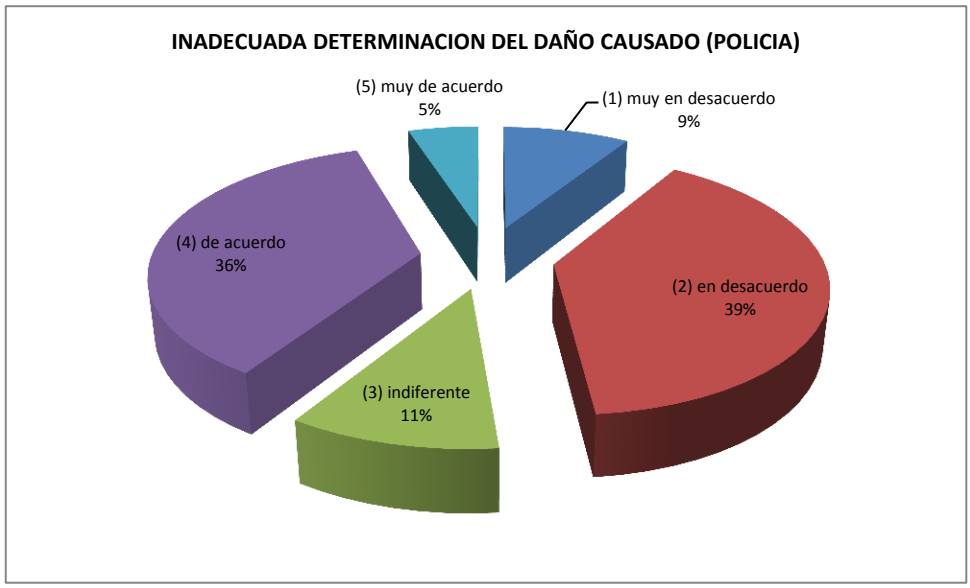
Anexo 6. Transgresiones de las legislaciones vigentes.



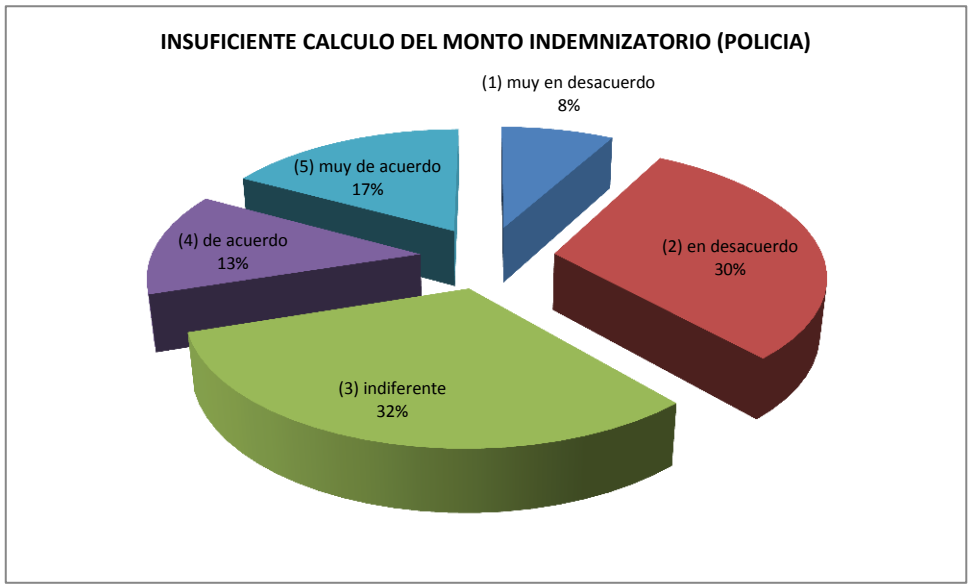
Anexo 7. Impropia determinación del tipo penal.



Anexo 8. Inadecuada determinación del daño causado.



Anexo 9. Insuficiente cálculo del monto indemnizatorio.



Anexo 10. Análisis de regresión múltiple de los operadores de justicia sobre investigación y juzgamiento de los delitos informáticos en la protección penal de la intimidad.

JUECES

.

The SAS System

The SAS System 107

The REG Procedure
Model: MODEL3
Dependent Variable: X18

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X3	X18
Intercept	0.5643086817	-0.147909968	1.8408360129
X3	-0.147909968	0.040192926	0.5160771704
X18	1.8408360129	0.5160771704	14.993569132

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	6.62643	6.62643	21.21	<.0001
Error	48	14.99357	0.31237		
Corrected Total	49	21.62000			

Root MSE	0.55890	R-Square	0.3065
Dependent Mean	3.74000	Adj R-Sq	0.2920
Coeff Var	14.94377		

The REG Procedure
Model: MODEL6
Dependent Variable: X13

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X6	X13
Intercept	0.4600402955	-0.121558093	0.8509066488
X6	-0.121558093	0.0335795836	0.7649429147
X13	0.8509066488	0.7649429147	12.354600403

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	17.42540	17.42540	67.70	<.0001
Error	48	12.35460	0.25739		
Corrected Total	49	29.78000			

Root MSE	0.50733	R-Square	0.5851
Dependent Mean	3.62000	Adj R-Sq	0.5765

Coeff Var 14.01474

The SAS System
The REG Procedure
Model: MODEL5
Dependent Variable: X13

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X11	X13
Intercept	0.3731343284	-0.097014925	1.8582089552
X11	-0.097014925	0.026652452	0.4840085288
X13	1.8582089552	0.4840085288	20.990405117

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	8.78959	8.78959	20.10	<.0001
Error	48	20.99041	0.43730		
Corrected Total	49	29.78000			

Root MSE	0.66129	R-Square	0.2952
Dependent Mean	3.62000	Adj R-Sq	0.2805
Coeff Var	18.26759		

FISCALES

The SAS System
The REG Procedure
Model: MODEL6
Dependent Variable: X16

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X12	X16
Intercept	0.2539461467	-0.072887651	3.7381615599
X12	-0.072887651	0.0227483751	-0.281337047
X16	3.7381615599	-0.281337047	33.21448468

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	3.47939	3.47939	4.92	0.0314
Error	47	33.21448	0.70669		
Corrected Total	48	36.69388			

Root MSE	0.84065	R-Square	0.0948
Dependent Mean	2.83673	Adj R-Sq	0.0756
Coeff Var	29.63440		

The SAS System
The REG Procedure
Model: MODEL5
Dependent Variable: X13

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X11	X13
Intercept	0.1915294118	-0.063529412	1.4856470588
X11	-0.063529412	0.0235294118	0.6423529412
X13	1.4856470588	0.6423529412	45.043764706

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	17.53624	17.53624	18.69	<.0001
Error	48	45.04376	0.93841		
Corrected Total	49	62.58000			

Root MSE	0.96872	R-Square	0.2802
Dependent Mean	3.22000	Adj R-Sq	0.2652
Coeff Var	30.08437		

The SAS System
The REG Procedure
Model: MODEL6
Dependent Variable: X13

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X12	X13
Intercept	0.1648044693	-0.05027933	1.0921787709
X12	-0.05027933	0.0174581006	0.7388268156
X13	1.0921787709	0.7388268156	31.312849162

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	31.26715	31.26715	47.93	<.0001
Error	48	31.31285	0.65235		
Corrected Total	49	62.58000			

Root MSE	0.80768	R-Square	0.4996
Dependent Mean	3.22000	Adj R-Sq	0.4892
Coeff Var	25.08331		

The SAS System
The REG Procedure
Model: MODEL6
Dependent Variable: X14

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X12	X14
Intercept	0.1648044693	-0.05027933	1.0921787709
X12	-0.05027933	0.0174581006	0.7388268156
X14	1.0921787709	0.7388268156	31.312849162

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	31.26715	31.26715	47.93	<.0001
Error	48	31.31285	0.65235		
Corrected Total	49	62.58000			

Root MSE	0.80768	R-Square	0.4996
Dependent Mean	3.22000	Adj R-Sq	0.4892
Coeff Var	25.08331		

The SAS System
The REG Procedure
Model: MODEL6
Dependent Variable: X15

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X12	X15
Intercept	0.1648044693	-0.05027933	1.3715083799
X12	-0.05027933	0.0174581006	0.655726257
X15	1.3715083799	0.655726257	26.990921788

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	24.62908	24.62908	43.80	<.0001
Error	48	26.99092	0.56231		
Corrected Total	49	51.62000			

Root MSE	0.74987	R-Square	0.4771
Dependent Mean	3.26000	Adj R-Sq	0.4662
Coeff Var	23.00227		

The SAS System
The REG Procedure
Model: MODEL6
Dependent Variable: X16

X'X Inverse, Parameter Estimates, and SSE

Variable	Intercept	X12	X16
Intercept	0.1648044693	-0.05027933	1.5418994413
X12	-0.05027933	0.0174581006	0.6312849162
X16	1.5418994413	0.6312849162	38.69273743

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Value	Pr > F
Model	1	22.82726	22.82726	28.32	<.0001
Error	48	38.69274	0.80610		
Corrected Total	49	61.52000			