UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

TEMA:

"LA AUSENCIA DE NORMATIVA RESPECTO A LA INTERCEPTACIÓN DE COMUNICACIONES Y ABUSO DE DISPOSITIVOS PROVOCA LA VULNERABILIDAD DE LA INTIMIDAD EN EL DEPARTAMENTO DE INVESTIGACIÓN Y ANÁLISIS FORENSE DE LA FISCALÍA GENERAL DEL ESTADO DEL CANTÓN QUITO DURANTE EL PERÍODO 2009".

Trabajo de graduación previo a la obtención de Título de Abogado de los Juzgados y Tribunales de la República del Ecuador.

AUTOR:

César Estuardo Naranjo Mesías

TUTOR:

Dr. José Rubén Guevara

Ambato - Ecuador

2011

TEMA

"LA AUSENCIA DE NORMATIVA RESPECTO A LA INTERCEPTACIÓN DE COMUNICACIONES Y ABUSO DE DISPOSITIVOS PROVOCA LA VULNERABILIDAD DE LA INTIMIDAD EN EL DEPARTAMENTO DE INVESTIGACIÓN Y ANÁLISIS FORENSE DE LA FISCALÍA GENERAL DEL ESTADO DEL CANTÓN QUITO DURANTE EL PERÍODO 2009".

APROBACIÓN DEL TUTOR

En calidad de Tutor del Trabajo de Investigación sobre el tema **"LA AUSENCIA DE NORMATIVA RESPECTO A LA INTERCEPTACIÓN DE COMUNICACIONES Y ABUSO DE DISPOSITIVOS PROVOCA LA VULNERABILIDAD DE LA INTIMIDAD EN EL DEPARTAMENTO DE INVESTIGACIÓN Y ANÁLISIS FORENSE DE LA FISCALÍA GENERAL DEL ESTADO DEL CANTÓN QUITO DURANTE EL PERÍODO 2009".** Del Sr. César Estuardo Naranjo Mesías, Egresado de la Carrera de derecho de la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato, considero que dicho trabajo de Graduación reúne los requisitos y meritos suficientes para ser sometido a la Evaluación del Tribunal de Grado, que el H. Consejo Directivo de la Facultad designe, para su correspondiente estudio y calificación.

Ambato, 25 de octubre del 2010.

……..

Dr. José Rubén Guevara

TUTOR

APROBACIÓN DEL TRIBUNAL DE GRADO

Los miembros del Tribunal de grado **APRUEBAN** el Trabajo de Investigación sobre el tema **"LA AUSENCIA DE NORMATIVA RESPECTO A LA INTERCEPTACIÓN DE COMUNICACIONES Y ABUSO DE DISPOSITIVOS PROVOCA LA VULNERABILIDAD DE LA INTIMIDAD EN EL DEPARTAMENTO DE INVESTIGACIÓN Y ANÁLISIS FORENSE DE LA FISCALÍA GENERAL DEL ESTADO DEL CANTÓN QUITO DURANTE EL PERÍODO 2009".** Presentado por el Sr. CÉSAR ESTUARDO NARANJO MESÍAS, de conformidad con el reglamento de graduación para obtener el Título Terminal de Tercer Nivel de la U.T.A.

Ambato,……

Para constancia firman:

…….

Presidente

…… ..…….

Delegado Delegado

AUTORÍA

Los criterios emitidos en el trabajo de investigación acerca de: "La ausencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos provoca la vulnerabilidad de la intimidad en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado del cantón Quito durante el período 2009", como también los contenidos, ideas, análisis, conclusiones y propuesta son de responsabilidad del autor.

Ambato, 25 de octubre del 2010.

EL AUTOR

……..

César Estuardo Naranjo Mesías

C.C. 180359800-0

DERECHO DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga de esta tesis o parte de ella un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de línea patrimoniales de mi tesis, con fines de difusión pública, además apruebo la reproducción de esta tesis, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice mis derechos de autor.

Ambato, 11 de abril de 2011.

Cesar Estuardo Naranjo Mesías
C.C. 1803598000

Dedicatoria

Con gran satisfacción dedico a mis Padres, hermanos y familiares; personas maravillosas que con infinito amor me guiaron en el camino del estudio, y ser una persona de bien, útil a la sociedad.

A ellos dedico mi trabajo fruto de mi esfuerzo y sacrificios constantes, ya que estuvieron a mi lado en las buenas y las malas; supieron guiarme y comprenderme, me llena de una profunda alegría los logros obtenidos en este trabajo.

César Naranjo.

Agradecimiento

Agradezco a Dios por darme salud y vida, a mis padres y hermanos por brindarme su apoyo y cariño incondicional para poder culminar una etapa más en mi vida.

A mis maestros por haberme impartido sus conocimientos y apoyo, que han hecho posible avanzar a una nueva etapa en mi vida y alcanzar la meta anhelada.

A todos mis amigos que estuvieron a mi lado incondicionalmente e incentivándome para alcanzar este gran proyecto de mi vida, este trabajo es para ustedes.

César Naranjo.

Índice

CAPÍTULO III

METODOLOGÍA

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VI

PROPUESTA

Índice de Gráficos

Índice de Cuadros

Resumen Ejecutivo

Hoy en día no es extraño ver que una gran parte de la población tiene acceso a los diferentes medios de comunicación y dispositivos, muchas de las personas han sido afectadas por el mal empleo de los diferentes dispositivos de comunicación masiva como el Internet o la Intranet provocando así una gran vulnerabilidad de la intimidad de las personas que atentan directamente los derechos consagrados en nuestra Constitución.

Cuanto más avanza el desarrollo del conocimiento en la sociedad y se incrementa la necesidad de usar las comunicaciones para la transmisión de datos e información, se presentan una serie de problemas vinculados con frecuentes vulneraciones a los sistemas de comunicación e informáticos.

Actualmente, nuestro país ha sido espectador de los avances tecnológicos que cotidianamente son empleados para efectos delictivos, pues las herramientas de antaño ante el fortalecimiento de la delincuencia aparecen como ineficaces para un combate congruente, pues la delincuencia principalmente aquella que está organizada, acopia los instrumentos de mayor avance tecnológico existentes en el "mercado negro".

El presente trabajo se sustenta con el propósito no sólo de proponer una reforma a nuestro Código Penal respecto a la interceptación de comunicaciones y abuso de dispositivos, sino además pretende ir más allá en el terreno de la difícil situación que afronta nuestra sociedad por la delincuencia organizada, al no tener legislado o reconocido estas figuras delictivas en nuestra legislación, ofreciendo al lector un documento sobre elementos actuales, en diversos ámbitos de nuestro contexto, aspectos del ser humano, etc.

El propósito del documento es difundir dichos temas con el objeto de que las personas tengan acceso y cuidado a la información, tendiente a establecer una filosofía y cultura de responsabilidad.

INTRODUCCIÓN

Se concluye con una bibliografía tentativa y los anexos en los que se han incorporado los instrumentos que se aplicarán en la investigación de campo.

La presente investigación surge no sólo con el propósito de analizar las diferentes realidades que afronta la sociedad y el estado, al interceptar las comunicaciones a través del abuso indiscriminado de dispositivos que atentan directamente a la intimidad y al no existir un verdadero control de las mismas a través de los distintos avances tecnológicos, sino además se requiere urgentemente realizar una verdadera propuesta de solución al problema.

Se encuentra estructurado por capítulos. El primer Capítulo denominado: EL PROBLEMA, contiene: El Planteamiento del Problema, Contextualización: Macro, Meso y Micro que hace relación al origen de la problemática, Árbol del Problema, Análisis Crítico, Prognosis, Formulación del Problema, Interrogantes de la Investigación, Delimitación del Objeto, Unidades de Observación, Justificación, Objetivos: General, y Específicos.

El Capítulo II denominado: MARCO TEÓRICO consta de: Antecedentes Investigativos, se fundamenta en una visión Filosófica, Legal, Categorías Fundamentales, Constelación de ideas de las Variables Independiente y Dependiente, Hipótesis y Determinación de Variables.

El Capítulo III titulado: METODOLOGÍA plantea que la investigación se realizará desde el enfoque Crítico Propositivo, de Carácter Cualicuantitativo, Modalidad de la Investigación, Tipos de la Investigación, Población y Muestra, Operacionalización de Variables, Técnicas e Instrumentos, Plan para la recolección de Información, Plan de proceso de Información, Análisis e Interpretación de Resultados.

La modalidad de la investigación es bibliográfica documental de campo, de intervención social: de asociación de variables que nos permitirán estructurar

predicciones llegando a modelos de comportamiento mayoritario.

El Capítulo IV denominado: ANÁLISIS E INTERPRETACIÓN DE RESULTADOS y consta de, la guía de entrevista, los análisis y las interpretaciones del proceso observado, conclusiones respecto del proceso, la decisión y las hojas con las entrevistas.

El Capítulo V CONCLUSIONES Y RECOMENDACIONES.

El Capítulo VI es denominado: LA PROPUESTA y consta de: Datos informativos, Antecedentes de la Propuesta, Justificación, Objetivos: General y Específicos, Análisis de Factibilidad, Fundamentaciones Científico Técnica, Modelo Operativo de la Propuesta, Desarrollo de la Propuesta y Administración

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

Contextualización

Macro:

El Convenio de Ciberdelincuencia del Consejo de Europa, define a los delitos informáticos como: "Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas de comunicación, redes, datos y abuso de dispositivos".

Según el Dr. Santiago Acurio Del Pino "Director Nacional de Tecnologías de la Información de la Fiscalía General del Estado" dice: Las amenazas cada vez más numerosas que ponen en peligro a nuestros datos, nuestra intimidad, nuestros negocios y la propia Internet ha hecho que la computación sea una tarea azarosa.

Los riesgos familiares, como los virus y el correo indeseado, ahora cuentan con la compañía de amenazas más insidiosas desde el llamado malware, los programas publicitarios, y de espionaje que infectan su PC a los ladrones de identidad que atacan las bases de datos importantes de información personal y las pandillas de delincuencia organizada que merodean por el espacio cibernético.
De acuerdo con el desarrollo doctrinal del tema, el concepto de delito informático puede comprender tanto aquellas conductas que valiéndose de medios informáticos lesionan otros intereses jurídicamente protegidos como la intimidad, el patrimonio económico, la fe pública, la seguridad, etc., como aquellas que recaen sobre herramientas informáticas propiamente tales como programas,

ordenadores, etc.

Los incidentes de seguridad en un Sistema de Información pueden caracterizarse modelando el sistema como un flujo de mensajes de datos desde una fuente, como por ejemplo un archivo o una región de la memoria principal, a un destino, como por ejemplo otro archivo o un usuario. Un incidente no es más que la realización de una amenaza en contra de los atributos funcionales de un sistema de comunicación.

Existe una necesidad urgente de incluir en el derecho penal vigente una tipificación básica de la interceptación de comunicaciones y abusos de dispositivos informáticos que afectan directamente a la intimidad de las personas naturales o jurídicas, el interés social y el patrimonio público. En primer término en lo que concierne a las conductas punibles, sería imprescindible crear nuevos tipos penales y en otros casos modificar los ya existentes.

Con el término interceptación de comunicaciones y abusos de dispositivos aglutinamos los hechos que basándose en técnicas o mecanismos, que para vulnerar la intimidad, sin su consentimiento procure la interceptación deliberada e ilegítima de sus comunicaciones ya sean tanto telefónicas como informáticas a través del uso de dispositivos deben ser tipificados de inmediato como delitos en el Código Penal Ecuatoriano debido a los avances tecnológicos que permiten delinquir se ha hecho necesario introducir y modificar determinados artículos que permitan aglutinar éstos.

Como señala Camacho Losa, “En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia.”

La interceptación de comunicaciones, tal como la concebimos hoy es una ofensa para cualquier persona que intencionalmente y sin autorización legal, para interceptar las comunicaciones o utilizar dispositivos que permitan el acceso

deliberado e ilegal a la información especialmente personal, en el curso de su transmisión a través de un sistema de comunicaciones y salvo en determinadas circunstancias a través de un sistema de telecomunicaciones privadas o el Internet.

A nadie se escapa la enorme influencia que ha alcanzado las comunicaciones en la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc.; son todos los aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

Junto al avance de la tecnología de comunicación y la informática su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos contra la intimidad o inviolabilidad del secreto.

Sin embargo, las categorías que los definen son aún mayores y complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes de comunicación han sido utilizados.

Con el desarrollo de las comunicaciones, la programación y el Internet, estos delitos se han vuelto más frecuentes y sofisticados que no necesariamente pueden ser cometidos totalmente por estos medios, sino también a partir de los mismos como es el abuso de dispositivos y la interceptación de comunicaciones, etc.

Estas actividades pueden ser absolutamente virtuales, porque la información se encuentra almacenada en forma digital; el daño aunque real no tiene consecuencias físicas distintas a los daños morales y económicos causados sobre las personas.

En algunos sistemas judiciales la propiedad intangible no puede ser robada y el daño debe ser visible. Un ordenador puede ser fuente de evidencia y, aunque

el ordenador no haya sido directamente utilizado para cometer el crimen, es un excelente artefacto que guarda los registros, especialmente en su posibilidad de codificar los datos. Esto ha hecho que los datos codificados de un ordenador o servidor tengan el valor absoluto de evidencia ante cualquier corte del mundo.

Meso:

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible.

En algunos casos la motivación para la interceptación de comunicaciones y abuso de dispositivos no es económica sino que se relaciona con el deseo de ejercitar; y, a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

Desde que Sutherland, planteo su teoría acerca de los delitos de cuello blanco se observa como la misma cuenta con una cierta marginación en el sistema penal; y por lo tanto, luego de los estudios actuales, los delitos de esta especie han tratado de adecuarse a las figuras convencionales, dentro de aquellos que lesionan la regulación jurídica de la producción, distribución y consumo de los bienes y servicios que afectan los bienes jurídicos intermedios entre los intereses del Estado y los de un agente económico individual o constituido en sociedad, que gravitan sobre determinados sujetos.

Por ende es preciso abordar cuán importante es tener en cuenta esta persona dicho ámbito, puesto que una gran parte de estos delitos se gestan y

ejecutan en el seno de una corporación o las grandes trasnacionales que mueven el mundo económico en la actualidad y en tal sentido, como personas jurídicas son utilizadas como vehículo ideal para propiciar o encubrir las actividades que se cometen y por lo difícil que se tornan en ocasiones los mecanismos económicos, se complica la exigencia de la responsabilidad penal individual, pero es posible incluso delimitar una responsabilidad penal también para la propia persona jurídica.

Es indispensable traer a colisión el hecho de la relevancia que representa que los sujetos sean personas jurídicas o personas naturales.

La última es, por lo general, el típico sujeto activo que se sancionará acorde con la norma jurídica a fin con este, y sin tanta complicación, pues la medida sancionadora repercutirá individualmente sobre una sola persona.

En cambio en la primera, vemos que su estatus es el más proclive a ocupar la posición de pasivo, debido a que los daños que le atañen siempre serán más severos que lo que pudieran ocasionársele a la otra persona pues posee un gran patrimonio que se mantiene en constante movimiento en el mercado para la obtención de ganancias, entendiéndola en el presente trabajo de investigación como entidad a la que la ley confiere personalidad jurídica.

A esta persona haremos referencia con un poco más de profundidad entendiendo a la norma jurídica relativa a la misma, algo atípica en el ámbito penal debido a su poco uso por los tribunales populares de nuestro estado.

La persona jurídica merece especial atención debido a que la misma es la única que posee plena y absoluta capacidad jurídica desde su constitución, acreditación, y reconocimiento ante la sociedad para hacer uso de los servicios de Internet que brinda nuestro país aún más con el decreto ejecutivo de la Presidencia del Economista Rafael Correa referente al manejo de software libre lo cual se necesita de un tratamiento especial para que la información no sea vulnerada o manejada irresponsablemente por terceras personas.

Esta capacidad por ende debería crearse un organismo que legalice su creación y su función como el ministerio rector y custodio de las actividades que en este ámbito de la informática se realicen en el país, o que estén relacionados con las mismas.

Luego otra razón para ser una persona privilegiada es el alto poder de dependencia con el Estado y el papel tan preponderante que tiene ésta en el campo mercantil, tanto nacional como internacional, en el movimiento y desarrollo económico del país el uso de estos servicios es necesario.

Dichas entidades se controlan por servidores que conforman redes cerradas (especialmente las estatales, Intranet) y abiertas cuando tienen acceso a la Aldea Global el Internet. Mediante estas redes pueden maniobrarse los delitos en perjuicio contra ellas mismas.

De aquí que remotamente pudiese sólo tener conocimiento de la información y prevenirse ella misma de cualquier acción que contra ella se tramara, o poner en práctica medidas estratégicas para su autoprotección en lo que a ella pudiese afectar, primordialmente en el mercado internacional donde se juegan los roles principales.

Puede verse la entidad dedicada a la expansión o comercialización o publicidad de otras entidades por todos los medios de publicidad posible, en los que se incluye el sistema informatizado como medio de llevar a cabo su actividad.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943.

Esta categoría requiere que: el sujeto activo del delito sea una persona de cierto estatus socioeconómico; su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni

por inestabilidad emocional.

El sujeto pasivo en el caso de los delitos informáticos, pueden ser individuos, instituciones crediticias, órganos estatales, etc. que utilicen sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

Micro:

La define Gómez Perals como conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.

Ruiz Vadillo recoge la definición que adopta el mercado de la OCDE en la Recomendación número R(81) 12 del Consejo de Europa indicando que abuso de dispositivos: “Es todo comportamiento ilegal o contrario a la ética o no autorizado que concierne a un tratamiento automático de datos y/o transmisión de datos”.

Según el mexicano Julio Tellez Valdez, los delitos informáticos presentan las siguientes características principales:

- Son conductas criminales de cuello blanco (white collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos) puede llegar a cometerlas.
- Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.
- Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.
- Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.

- Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
- Son muy sofisticados y relativamente frecuentes en el ámbito militar.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación. Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

Conviene destacar entonces, que diferentes autores y organismos han manifestado diferentes apreciaciones para señalar las conductas ilícitas en las que se utiliza los diferentes tipos de equipos de comunicación e informáticos, esto es "delitos contra la inviolabilidad del secreto", "delitos electrónicos", "delitos relacionados con la computadora", "crímenes por computadora", "delincuencia relacionada con el computador".

Actualmente se requieren serias modificaciones y en otros casos nuevas normas para disminuir en cierta forma la incertidumbre jurídica en que se encuentran sumergidas las nuevas disposiciones penales en materia de delito informático

A pesar de algunos avances, como la tipificación del acceso abusivo a sistemas informáticos en el nuevo estatuto represor y poder encasillar en nuestro marco legal.

Cada vez más, se hace necesario el respaldo legal como la mejor y más adecuada forma de reprimir y castigar estos delitos ya que dichas conductas reprochables, resultan en la mayoría de los casos impunes debido a la inidoneidad de las figuras incriminatorias tradicionales.

Al no ser castigados dichos comportamientos ilícitos, debido a la carencia de claridad sobre la naturaleza jurídica de los bienes objeto material de los delitos, ni del interés jurídico protegido.

- El Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado no puede iniciar las investigaciones y análisis criminalístico por la falta de una norma clara y precisa.
- La atipicidad relativa generada por la ausencia de uno de los elementos de tipo cuando se trata de subsumir la conducta ilícita.
- La falta de control a las grandes redes como el Internet o la Intranet y aparte el acceso ilegal o deliberado a la información por medio de dispositivos comunes.

Árbol de Problemas

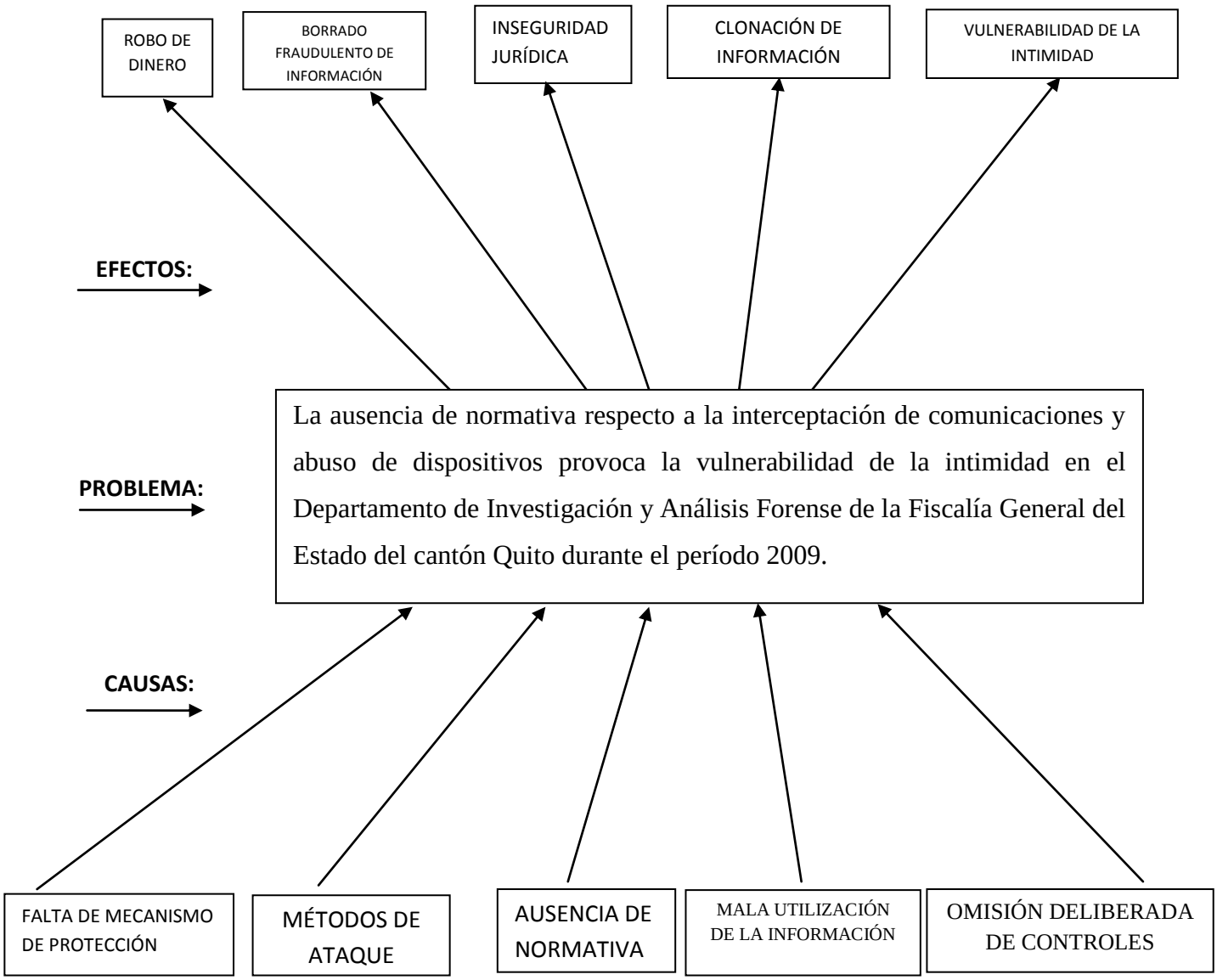

GRÁFICO Nº 01
Fuente: Investigador
Elaboración por: César E. Naranjo Mesías

Análisis Crítico

En la actualidad las comunicaciones se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información; y la falta de mecanismos de control, las ubica también como un nuevo medio fácil para la interceptación de información, y condiciona su desarrollo de la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos; generando de esta manera el robo de dinero más fácilmente sin tener que recurrir a acciones violentas.

La importancia reciente de identificar los métodos de ataque a los sistemas de datos, por su gran incidencia en la marcha de las empresas y movimientos económicos personales, que incluso violenta la intimidad personal; los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme como el borrado fraudulento de información, que va mucho más allá del valor material de los objetos destruidos a través de varios dispositivos informáticos.

A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

Por razones similares, las empresas constructoras, bancos y compañías de seguros, e inclusive el Estado mismo están más expuestos a la interceptación deliberada e ilegal de comunicaciones por medio del uso abusivo de dispositivos que generan graves perjuicios materiales y morales. Aunque depende en gran medida del tipo de organización, se puede mencionar que la interceptación ilegal de comunicaciones y el uso indiscriminado de dispositivos son los delitos de mayor incidencia en las organizaciones especialmente empresariales e incluso personales.

Además, aquellos que no están claramente definidos y publicados como un delito.

El espectacular desarrollo de la tecnología y la ausencia de normativa ha abierto las puertas a nuevas posibilidades de delincuencia informática antes impensables provocando grandes estragos a la sociedad o al estado con el fin de obtener réditos económicos.

De esta manera estamos totalmente desprotegidos y por ende se genera inestabilidad jurídica al momento en que nos encontramos inmersos en este tipo de conductas atípicas. La manipulación fraudulenta de los dispositivos con ánimo de lucro, la destrucción de programas o datos, la utilización indebida de la información que puede afectar directamente la esfera de la privacidad. Estos son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños a través de la duplicación o suplantación de información.

Por otra parte, al no existir la adecuada intervención estatal, con la creación de organismos que controlen eficazmente este tipo de conducta delictiva, el Estado no está garantizando la protección total de la información.

En cuanto a la inviolabilidad de la intimidad de las personas, consagrados en la Constitución de la República del Ecuador y otros cuerpos legales, conculcando de esta manera los derechos del Buen Vivir.

Prognosis

La situación jurídica en la que se ve envuelta el problema propuesto frente a la falta de eficacia de la ley para proteger la información genera en la sociedad inseguridad.

Nuestra legislación penal actual requiere de una adecuación normativa que está en una categoría sui generis, ya que dichas infracciones no son de recibo en las actuales formas descriptivas, pese a que ya las contienen la mayoría de legislaciones penales.

Crear o modificar es el dilema, decidir si conviene crear una ley individual sobre la materia o si los diversos tipos penales deben ser encasillados en diferentes capítulos del Código Penal mediante la ampliación de algunos tipos penales.

Esta es la situación que se va a desarrollar en la investigación y se anota especial cuidado en los pilares de la seguridad de la información, la confidencialidad, integridad y disponibilidad.

Se expondrán cada una de las modificaciones a las conductas punibles contra la vulnerabilidad de la intimidad acerca lo que se basa esta investigación, que necesitan de verdaderos cambios, con miras de que exista en este país una penalización para la criminalidad informática.

Formulación del Problema

La ausencia de normativa respecto a la Interceptación de Comunicaciones y Abuso de Dispositivos provoca la Vulnerabilidad de la Intimidad en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado del cantón Quito durante el período 2009.

Interrogantes de la Investigación

Frente a la problemática que se presenta con la ausencia de normativa respecto a la interceptación de comunicaciones y el abuso de dispositivos informáticos, al respecto surge las siguientes interrogantes:

- ¿Cómo la ausencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos coadyuva a la vulnerabilidad de la intimidad?
- ¿Cuáles son los efectos que produce la vulnerabilidad de la intimidad?
- ¿Existe alternativas de solución a la falta de especificación del Art. 202 del Código Penal?

Delimitación del Objeto de la Investigación

Delimitación de Contenidos:

CAMPO : Derecho Penal
ÁREA : Informática Jurídica
ASPECTO : Interceptación de Comunicaciones y Abuso de Dispositivos

Delimitación Espacial:

La investigación se realizará en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado.

Delimitación Temporal:

La investigación va a ser realizada durante el período 2009.

Unidades de Observación

1. Fiscalía General del Estado (Departamento de Investigación y Análisis Forense Quito).
2. Policía Judicial (Departamento de Criminalística).
3. Biblioteca.
4. Sociedad.

Justificación

La presente investigación tiene por interés, verificar si es o no necesaria o no una reforma al Libro II, Título II, Capítulo V, artículo 202 del Código Penal el cual deja al libre criterio del juzgador acerca de la interceptación de comunicaciones y abuso de dispositivos informáticos, así mismo dicho interés se extenderá a un análisis al Código de Procedimiento Penal, en posibles reformas que se puedan introducir al contorno de las interrogantes planteadas en la formulación del problema.

La presente investigación ha sido seleccionada porque a medida que avanzamos hacia un mundo donde la vigilancia digital de los seres humanos crece exponencialmente, debemos preguntarnos hacia dónde vamos; por lo tanto la investigación es de mucha importancia, ya que se busca aclarar un vacío legal y regularlo con posibles reformas que acarrearán consecuencias sociales y legales en cuanto a la interceptación de comunicaciones y abuso de dispositivos.

Por el momento siguen siendo ilícitos e impunes de manera manifiesta ante la ley. Pronto los chips de identificación por frecuencia de radio en las ropas que usamos y los carnets de identidad que llevamos se comunicarán con el medio donde vivimos y transmisores incorporados seguirán nuestros movimientos. Si alguien falsifica correctamente esas huellas, un ser humano real podría enfrentarse en la corte a una persona digital, muy bien fabricada fuera del control del individuo en cuestión.

En la sociedad informatizada que se pretende alcanzar en nuestro país, una gran mayoría de los quehaceres de nuestra vida cotidiana se encuentra relacionado con la informática, desde su centro laboral, su tarjeta de crédito, su correo electrónico, sus datos personales fichados en los registros y archivos nacionales, en la actividad tributaria, entre otros.

Esta dimensión transgresora y abusiva del empleo de las nuevas tecnologías debe ser enfrentada por el Derecho Penal, como disciplina garante de la convivencia pacífica e instrumento de control social.

Por lo que, los beneficiarios de la presente investigación y de los resultados que aparezcan de la misma, serán sin duda los jueces, fiscales, policías judiciales y especialmente a la sociedad en general.

La investigación es factible ya que el problema está presente, y por lo tanto el mismo debe ser resuelto lo más pronto posible a fin de que facilite las actuaciones de los jueces y brindar así una mayor seguridad jurídica en la protección de los derechos de comunicación e información.

Objetivos

General

Estudiar y conocer acerca de la interceptación de comunicaciones y el abuso de dispositivos amerita o no una propuesta de reforma en el Art. 202 del Código Penal Ecuatoriano.

Específicos

- Analizar los efectos que provoca la ausencia de normativa respecto a la interceptación de comunicaciones y abusos de dispositivos.

- Identificar que tipos de medios o técnicas sirven para violentar la intimidad.

- Proponer lineamientos para que sea normada la Interceptación de Comunicaciones y Abusos de Dispositivos que generan nuevos delitos informáticos.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes Investigativos

En el presente capítulo para iniciar la investigación se revisó la Ley de Comercio Electrónico, Firmas y Documentación, Ley de Telecomunicaciones, Ley de la Propiedad Intelectual, Código Penal, Código de Procedimiento Penal, y; archivos en la Facultad de Jurisprudencia y Ciencias Sociales de la Universidad Técnica de Ambato para conocer anteriores investigaciones del tema propuesto, no existe trabajo alguno.

Publicaciones, reportes e informes sobre procesos judiciales producidas por el cometimiento de delitos a través de la Interceptación de Comunicaciones y Abusos de Dispositivos; siendo poco los tratados de esta problemática y en varias obras consultadas corresponden a realidades de otros países latinoamericanos e inclusive en el Continente Europeo.

Actualmente se requieren serias modificaciones y en otros casos nuevas normas para disminuir en cierta forma la incertidumbre jurídica en que se encuentran sumergidas las nuevas disposiciones penales en materia de interceptación de comunicaciones y abuso de de dispositivos, pese a algunos avances, para que el lector comprenda la evolución de los diferentes delitos informático que se pueden suscitar, y así conseguir el entendimiento del porque las organizaciones y la sociedad deben revisar sus controles periódicamente con la finalidad de determinar sus seguridades tanto lógicas como físicas y además mejorar sus procesos.

Lo que implica el presente informe basado en una investigación de campo es original y de actualidad, abordando una temática muy poco estudiada por los

tratadistas y filósofos del derecho, y por lo tanto es un aporte a la búsqueda de sanciones y reglamentación adecuada sobre este tipo de criminalidad.

Fundamentación

Fundamentación Filosófica

En la sociedad informatizada que se pretende alcanzar en nuestro país, una gran mayoría de los quehaceres de nuestra vida cotidiana se encuentra relacionado con la informática, desde su centro laboral, su tarjeta de crédito, su correo electrónico, sus datos personales fichados en los registros y archivos nacionales, en la actividad tributaria, entre otros.

Las ventajas que ofrece el empleo de esta nueva tecnología en la optimización de los servicios que se brinden en estas esferas mencionadas y en muchas más son incuestionables, pero como casi todo tiene su lado oscuro.

Nuestra posición en estas tecnologías es neutral en un porciento mayoritario comparado con aquellos que se dedican por entero.

Por razones laborales o de entretenimiento a hacer modificaciones constantes en dichos sistemas computarizados, por lo que estamos expensas a ser víctimas de las acciones antijurídicas que se lleven contra estos medios informáticos, los cuales pueden ser manejados o plenamente afectados quiénes pretenden saciar necesidades con su uso.

Esta dimensión transgresora y abusiva del empleo de las nuevas tecnologías debe ser enfrentada por el Derecho Penal, como disciplina garante de la convivencia pacífica e instrumento último de control social. Así que estamos en presencia de una acción u omisión socialmente peligra, prohibida por ley bajo la conminación de una sanción penal a la que es considerada delito informático, pues de forma expresa se manifiesta como la "acción típica, antijurídica y dolosa cometido mediante el uso normal de la informática, o sea, un elemento

informático o telemático, contra el soporte lógico o software, de un sistema de tratamiento autorizado de la información".

Existe una necesidad urgente de incluir en el derecho penal vigente una tipificación básica acerca de la interceptación de comunicaciones y abuso de dispositivos que afecten el interés social y el patrimonio público.

En primer término en lo que concierne a las conductas punibles, sería imprescindible crear nuevos tipos penales y en otros casos modificar los ya existentes.

Con el avance de la tecnología digital de los últimos años, surgen nuevas generaciones de delincuentes que exponen a los gobiernos, las empresas y los individuos a este tipo de peligros, la difusión de pornografía infantil, el incremento de incidentes de inseguridad e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos que presentan una realidad difícil de controlar, y que traspasa las fronteras de los países, por ello, es primordial la cooperación entre organismos estatales internacionales para hacer frente a estos nuevos delincuentes.

Fundamentación legal

La investigación tiene su sustento en la Constitución Política del Estado, la cual en el Título II, Sección Tercera, en el Art. 20 dice:

"El Estado garantizará la cláusula de conciencia a toda persona, el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier medio de comunicación."

De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto pre procesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal.

Es por tanto el Fiscal quien deberá llevar como quién dice la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contará como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control de la Fiscalía.

En tal virtud cualquier resultado de dichas investigaciones se incorporarán en su tiempo ya sea a la instrucción fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudarán posteriormente al representante de la Fiscalía a emitir su dictamen correspondiente. Este entorno permitirá el acceso universal de tecnologías de comunicación y de información, con el apoyo de políticas intersectoriales nacionales y locales.

De esta forma la investigación tiene también su carácter legal en el Código Penal en los Art. 197, 199,200 201 y 202.

Según lo dispuesto en el Art. 197: "Serán sancionados con penas de dos meses a un año de prisión, quienes interceptaren sin orden judicial, conversaciones telefónicas o realizadas por medios afines y quienes se sustrajeren a abrieren sobres de correspondencia que pertenecieren a otro sin autorización expresa.

Se exime la responsabilidad de quien lo hizo cuando la interceptación telefónica o la apertura de sobres se produce por error, en forma accidental o fortuita".

El Art. 199, nos dice: "El que hallándose en posesión de una correspondencia no destinada a la publicación, la hiciera publicar, o presentare en juicio sin orden judicial, aunque haya sido dirigida a él, será reprimido con multa de seis a treinta y un dólares de los Estados Unidos de Norteamérica, si el acto puede causar perjuicio a terceros; a no ser que se trate de correspondencia en que consten obligaciones a favor del tenedor de ella, caso en el que puede presentarse en juicio".

El Art. 200 nos manifiesta que: “En la misma pena incurrirá el que, sin ser empleado público, divulgare actuaciones o procedimientos de que haya tenido conocimiento y que, por ley, deben quedar reservados”.

El Art. 201 nos dice: “El que teniendo noticia, por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación puede causar daño, lo revelare sin causa justa, será reprimido con prisión de seis meses a tres años y multa de ocho a sesenta y siete dólares de los Estados Unidos de Norteamérica”.

El Art. 202 nos dice: “Los que sustrajeren cartas confiadas al correo serán reprimidos con prisión de quince a sesenta días, excepto los padres, maridos o tutores que tomaren las cartas de sus hijos, consortes o pupilos, respectivamente, que se hallen bajo su dependencia”.

El Art. 202.1 manifiesta: “El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la

información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica".

El Art. 202.2 menciona acerca de la Obtención y utilización no autorizada de información.- " La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

El Art. 606 acerca de las contravenciones de tercera clase dice: "Serán reprimidos con multa de siete a catorce dólares de los Estados Unidos de Norteamérica y con prisión de dos a cuatro días, o con una de estas penas solamente"; y, en su numeral 20 menciona que: " Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos."

Según el Art. 155 del Código de Procedimiento Penal menciona acerca de la interceptación y grabaciones lo siguiente: "El juez puede autorizar por escrito al Fiscal para que intercepte y registre conversaciones telefónicas o de otro tipo, cuando lo considere indispensable para impedir la consumación de un delito, o para comprobar la existencia de uno ya cometido, o la responsabilidad de los partícipes.

La cinta grabada deberá ser conservada por el Fiscal, con la transcripción suscrita por la persona que la escribió. Las personas encargadas de interceptar, grabar y transcribir la comunicación tienen la obligación de guardar secreto sobre su contenido, salvo cuando se las llame a declarar en el juicio".

CATEGORÍAS FUNDAMENTALES

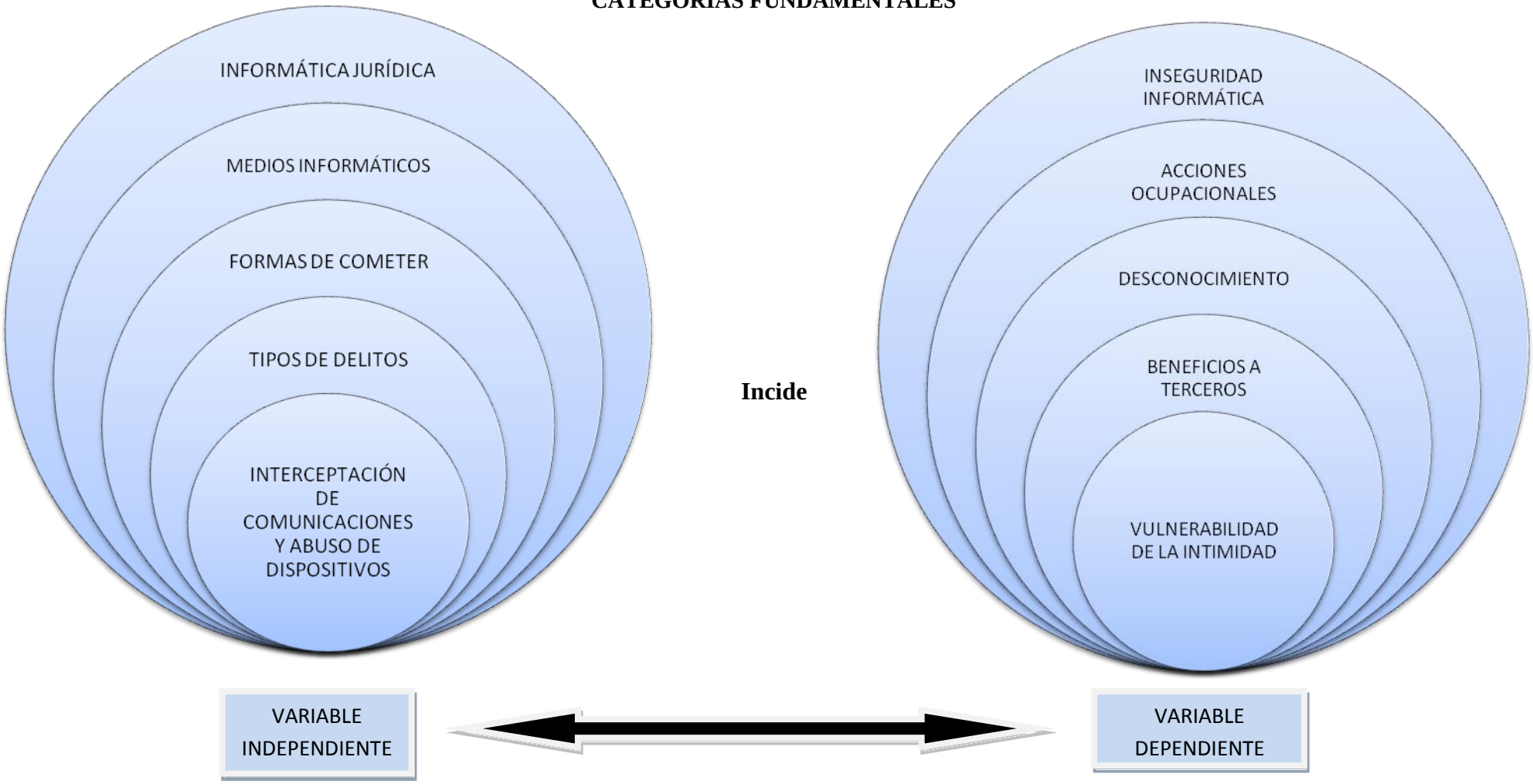

GRÁFICO Nº 0 2

Fuente: Investigador

Elaborado por: César E. Naranjo Mesías

Rueda de Atributos de la Variable Independiente

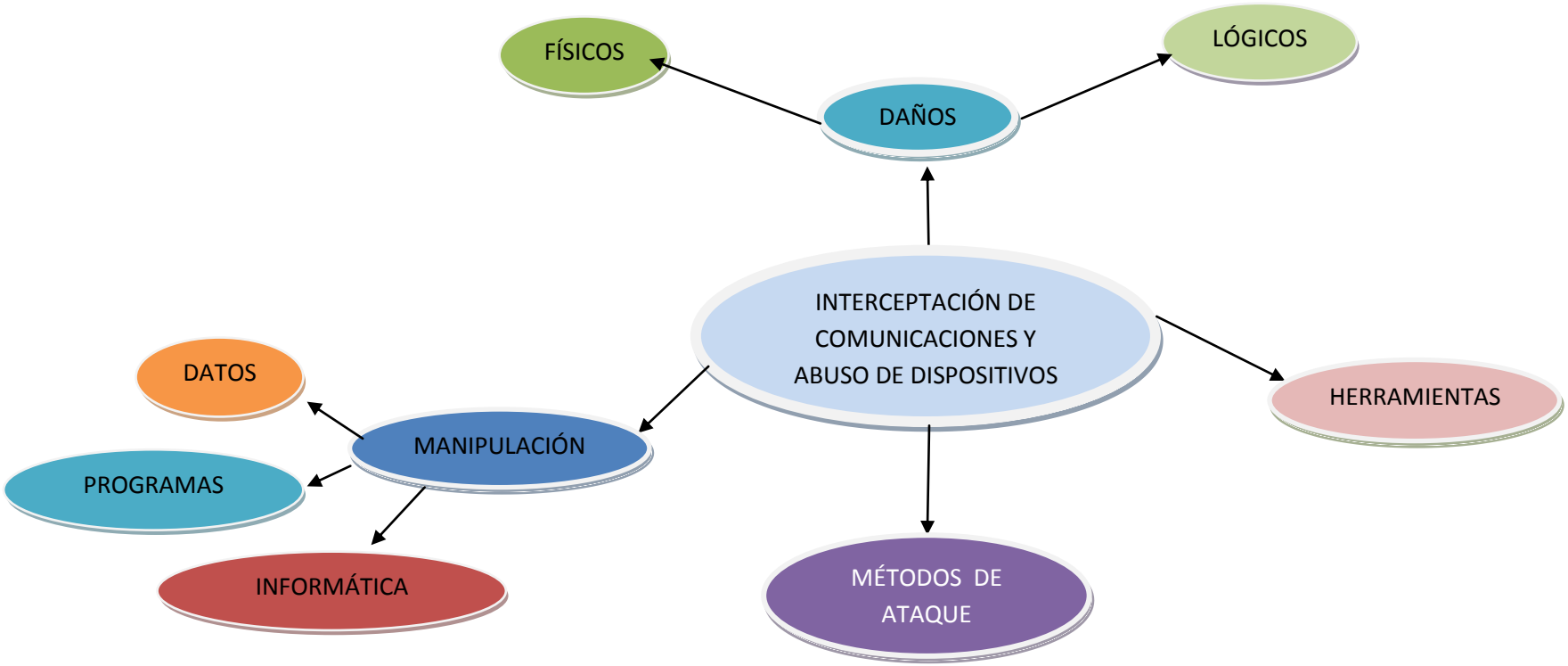

GRÁFICO Nº 0 3

Fuente: Investigador
Elaborado por: César E. Naranjo Mesías

Rueda de Atributos de la Variable Dependiente

GRÁFICO Nº0 4
Fuente: Investigador
Elaborado por: César E. Naranjo Mesías

Informática Jurídica

La Informática Jurídica es una rama del Derecho que permite otorgar las soluciones jurídicas adecuadas a los problemas originados por el uso de las tecnologías, en las diversas actividades del ser humano.

Un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática.

Es una ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del derecho. En otras palabras, es ver el aspecto instrumental dado a raíz de la informática en el derecho.

Medios Informáticos

Dirección Nacional de Tecnología de la Información, Manual de Manejo de Evidencias Digitales y Entornos Informáticos (Pág. 8 -10, Año 2009) los clasifica en tres grandes grupos:

1. SISTEMAS DE COMUNICACIÓN ABIERTOS.- Son aquellos que están compuestos de las llamadas computadores personales y todos sus periféricos como teclados, ratones y monitores, las computadoras portátiles y los servidores. Actualmente estos computadores tienen la capacidad de guardar gran cantidad de información dentro sus discos duros, lo que los convierte en una gran fuente de información.
2. SISTEMAS DE COMUNICACIÓN.- Estos están compuestos por las redes de telecomunicaciones, la comunicación inalámbrica y el Internet. Son también una gran fuente de información y de evidencia digital.
3. SISTEMAS CONVERGENTES DE COMPUTACIÓN.- Son los que están formados por teléfonos celulares llamados inteligentes o Smartphones, los asistentes personales digitales PDA’s, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que puedan contener evidencia digital.

Dada la ubicuidad de la evidencia digital es raro el delito que no esté asociado a un mensaje de datos guardado y trasmitido por medios informáticos.

Ejemplos de aparatos electrónicos e informáticos:

- Computador de escritorio.
- Computador Portátil.
- Estación de Trabajo.
- Hardware de Red.
- Servidor – aparato que almacena o transfiere datos electrónicos por el Internet.
- Teléfono celular.
- Teléfono inalámbrico.
- Aparato para identificar llamadas.
- Localizador – beeper.
- "GPS" – aparato que utiliza tecnología satélite capaz de ubicar geográficamente al persona o vehículo que lo opera.
- Cámaras, videos.
- Sistemas de seguridad.
- Memoria "flash" – Pequeño dispositivo que puede conservar hasta 4 gigabytes de datos o 4,000,000,000 bytes de información
- "Palm" – asistente personal electrónico que almacena datos y posiblemente tiene conectividad inalámbrica con el Internet.
- Juegos electrónicos – en su unidad de datos se puede guardar, incluso, una memoria de otro aparato.
- Sistemas en vehículos – computadoras obvias y computadoras del sistema operativo del vehículo que registra cambios en el ambiente y el mismo vehículo.
- Impresora
- Copiadora
- Grabadora
- Videograbadora, DVD

- Duplicadora de discos
- Discos, disquetes, cintas magnéticas
- Aparatos ilícitos – tales como los aparatos que capturan el número celular de teléfonos cercanos para después copiarlo en otros teléfonos, o los llamados sniffers, decodificadores, escáners de radio, sistemas de intercom residenciales, Speakerphones, Micrófonos inalámbricos, Cámaras de video inalámbricas, Llamadas hechas desde un avión**.**

Otros Aparatos Electrónicos

Aparatos de mensajería instantánea, beepers.

1. Beepers Numéricos (reciben solo números y sirven para transmitir números y códigos)
2. Beepers Alfanuméricos (reciben números y letras, pueden cargar mensajes completos en texto)
3. Beepers de Voz (pueden transmitir la voz y también caracteres alfanuméricos)
4. Beepers de dos vías (contienen mensajes de entrada y salida)
5. Buenas Prácticas.- Una vez que el beeper está alejado del sospechoso, este debe ser apagado. Si se mantiene encendido los mensajes recibidos, sin tener una orden judicial para ello puede implicar una interceptación no autorizada de comunicaciones.
6. Cuando se debe buscar en el contenido del aparato.

- Cuando es la causa de la aprehensión del sospechoso
- Cuando haya presunción del cometimiento de un delito Flagrante
- Con el consentimiento del dueño o receptor de los mensajes

Máquinas de Fax

1. En las máquinas de fax podemos encontrar:

- Listas de marcado rápido
- Fax guardados (transmitidos o recibidos)

- Bitácoras de transmisión del Fax (transmitidos o recibidos)
- Línea del Encabezado
- Fijación de la Hora y Fecha de la transmisión del Fax

2. Buenas Prácticas

Si la máquina de fax es encontrada prendida “ON”, el apagarla causaría la perdida de la memoria de último número marcados así como de los facsímiles guardados.

3. Otras consideraciones

Busque la concordancia entre el número de teléfono asignado a la máquina de fax y la línea de teléfono a la que está conectada.

De igual forma busque que el encabezado del mensaje y el número impreso coincidan con el del usuario y la línea telefónica.

Es necesario que el investigador busque el manual del usuario relacionado con el aparato encontrado.

Dispositivos de Almacenamiento

Los dispositivos de almacenamiento son usados para guardar mensajes de datos e información de los aparatos electrónicos.

Existen dispositivos de almacenamiento de tres clases, a saber: dispositivo magnético (como discos duros o los disquetes), dispositivos de estado sólido o memoria sólida (como las memorias flash y dispositivos USB) y los dispositivos ópticos (como los discos compactos y DVD).

Existen gran cantidad de Memorias USB en el mercado y otros dispositivos de almacenamiento como tarjetas SD, Compact flash, Tarjetas XD,

Memory Stick, etc.

Tipos de Delitos

La Convención de Delitos Informáticos del Consejo de Europa del 2001, La Unión Europea, en la Propuesta de Decisión-Marco del Consejo Relativa a los Ataques de los que son Objeto los Sistemas de Información; y, las Naciones Unidas en agosto del 2002, clasifican las conductas lesivas a la información en cuatro tipos:

a) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.- Sanciona el acceso y la intercepción ilegal, interferencia de datos y sistemas y el mal uso de dispositivos.
b) Delitos de fraude informático.- Falsificación y fraude computacional.
c) Delitos por su contenido.- Producción, diseminación y posesión de pornografía infantil.
d) Delitos relacionados con la infracción de la propiedad intelectual y derechos afines.

La amplia gama de reproducciones ilícitas por medios informáticos de obras protegidas por el derecho de autor.

Para entender de mejor manera los atentados contra la información a partir de sus propiedades esenciales: **confidencialidad**, **integridad** y **disponibilidad**.

Conductas lesivas a la confiabilidad de la información

Entre estas se encuentran:

7. **El Espionaje Informático (Industrial o Comercial).** Con los términos industrial y comercial se pretende delimitar esta categoría, excluyendo bienes jurídicos distintos como sería el caso de delitos contra el Estado y la defensa nacional o contra la intimidad. Debe entenderse como la obtención con ánimo de lucro y sin autorización, de datos de valor para el tráfico económico de la industria o comercio. Dentro de los comportamientos que

pueden ser incluidos en esta descripción se identifican los siguientes: La fuga de datos (Data Leakage), que las empresas o entidades guardan en sus archivos informáticos; las puertas falsas (Trap Doors), consistentes en acceder a un sistema informático a través de entradas diversas a las que se utilizan normalmente dentro de los programas. Las "llaves maestras" (Supperzapping) que implica el uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en los sistemas de información. El pinchado de líneas (Wiretapping), que consiste en la interferencia en líneas telefónicas o telemáticas, mediante las cuales se trasmiten las informaciones procesadas. La apropiación de informaciones residuales (Scavenging) que consiste en la obtención de información a partir de lo que desechan los usuarios legítimos de un sistema informático.

2. **El Intrusismo informático.** Se define como la mera introducción a sistemas de información o computadoras, infringiendo medidas de seguridad destinadas a proteger los datos contenidos en ellos.

A primera vista pareciera que el Sabotaje Informático y el Intrusismo fueran comportamientos idénticos, sin embargo el elemento subjetivo delimita estos comportamientos. En el primer supuesto, la intencionalidad del agente es obstaculizar el funcionamiento de un sistema informático, en el segundo caso la acción realizada busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la producción de perjuicio, que se produzca, es ajeno al comportamiento aunque es evidente que lo agrava.

Conductas lesivas a la integridad de la Información

Consisten en el acceso directo u oculto no autorizado a un sistema informático mediante la introducción de nuevos programas denominados virus, "gusanos" o "bombas lógicas". El acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema, recibe el nombre de "sabotaje informático".

Conductas lesivas a la disponibilidad

Las bombas lógicas y los virus informáticos pueden afectar transitoriamente la disponibilidad de la información, sin destruirla. Otro de los mecanismos que pueden impedir el acceso a un sistema de información por parte de los usuarios legítimos, son los denominados "spam" o el "electronic-mail bombing", que consisten en el envío de cientos de miles de mensajes de correo electrónico no solicitados o autorizados, para bloquear los sistemas.

D´ALESIO, Andrés José y DIVITO, Mauro, Delitos Informáticos comentados y anotados, parte especial, (Año 2002 - Pág. 153): "Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es inimaginable, a decir de Camacho Losa, el único limite existente viene dado por la conjugación de tres factores: la imaginación del autor, su capacidad técnica y las deficiencias de control existentes en las instalaciones informáticas.

Por tal razón y siguiendo la clasificación dada por el estadounidense B. Parker más la lista mínima de ilícitos informáticos señalados por las Naciones Unidas, he querido lograr una clasificación que desde el punto de vista objetivo sea lo más didáctica posible al momento de tratar esta clase de conductas delictivas, por lo expuesto anteriormente y sin pretender agotar la multiplicidad de conductas que componen a esta clase de delincuencia.

Es probable que al escribir estas líneas ya hayan quedado sobrepasada las listas de modalidades conocidas o imaginables, que ponemos a consideración del lector en forma breve en que consiste cada una de estas conductas delictivas:

Los Fraudes

LOS DATOS FALSOS O ENGAÑOSOS (Data diddling), conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en

transacciones de una empresa. Este tipo de fraude informático conocido también como **manipulación de datos de entrada**, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

MANIPULACIÓN DE PROGRAMAS O LOS "CABALLOS DE TROYA" (Troya Horses), Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

LA TÉCNICA DEL SALAMI.- Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes.

FALSIFICACIONES INFORMÁTICAS (Como objeto)**:** Cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Cuando empezó a disponerse de fotocopiadoras computarizadas en color

basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

MANIPULACIÓN DE LOS DATOS DE SALIDA.- Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos.

Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

PISHING.- Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo.

El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes.

El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las victimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aun peor.

En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar.”

El sabotaje informático:

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

BOMBAS LÓGICAS (LOGIC BOMBS).- Es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

GUSANOS.- Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno.

Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

VIRUS INFORMÁTICOS.- Son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de

ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. Han sido definidos como "pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de autoreproducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar".

CIBERTERRORISMO.- Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

El espionaje informático y el robo o hurto de software:

FUGA DE DATOS (DATA LEAKAGE).- Es conocida como la divulgación no autorizada de datos reservados, es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, "la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera"**.**

REPRODUCCIÓN NO AUTORIZADA DE PROGRAMAS INFORMÁTICOS DE PROTECCIÓN LEGAL. Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, considero, que la reproducción no

autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los contenidos específicos del Derecho Informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

El robo de servicios:

HURTO DEL TIEMPO DEL COMPUTADOR.- Consiste en el hurto de el tiempo de uso de las computadoras, un ejemplo de esto es el uso de Internet, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la súper carretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no esta autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

APROPIACIÓN DE INFORMACIONES RESIDUALES (SCAVENGING).- Es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. Toscavenge, se traduce en recoger basura. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos.

PARASITISMO INFORMÁTICO (PIGGYBACKING) Y SUPLANTACIÓN DE PERSONALIDAD (IMPERSONATION).- Son figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos, el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de

su capacidad y posición al interior de una organización o empresa determinada.

El acceso no autorizado a servicios informáticos:

LAS PUERTAS FALSAS (TRAP DOORS).- Consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante.

LA LLAVE MAESTRA (SUPERZAPPING).- Es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador.

Su nombre deriva de un programa utilitario llamado superzap, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador.

Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación.

PINCHADO DE LÍNEAS (WIRETAPPING).- Consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora.

Como se señalo anteriormente el método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la

que se envió en origen.

PIRATAS INFORMÁTICOS.- El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema.

A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Interceptación de Comunicaciones y Abuso de Dispositivos

Montón Redondo Alberto, Las interceptaciones telefónicas constitucionalmente correctas en "Revista Jurídica Española La Ley" (Pág. 1046 - Año: 2003) dice: "Es el proceso mediante el cual se capta información que se trasmite a través de comunicaciones telefónicas, radiotelefónicas, informáticas y otras similares que utilicen el espectro radiomagnético".

El artículo 615 del Código Penal Italiano dice: "El uso abusivo de un sistema informático o telemátic, se configura exclusivamente en caso de sistemas informáticos o telemáticos protegidos por dispositivos de seguridad (contraseñas o llaves de hardware) que indiquen claramente la privacidad del sistema y la voluntad del derechohabiente de reservar el acceso al mismo sólo a las personas autorizadas. La comisión de este delito se castiga con reclusión de hasta tres años, previendo agravantes."

El artículo 617 del Código Penal Italiano dice: "Es la Interceptación Abusiva de Comunicaciones que está tratado junto con el delito de falsificación, alteración o supresión de comunicaciones telefónicas o telegráficas. La intercepción fraudulenta, el impedimento o intrusión de comunicaciones relativas a sistemas informáticos o telemáticos, además de la revelación al público, de todo

o parte, por cualquier medio del contenido de la comunicación se castiga con reclusión de seis meses a cuatro años. Se castiga también la instalación de aparatos para interceptar, impedir o interrumpir las comunicaciones informáticas o telemáticas."

Jeimy J. Cano, El Arte del Peritaje Informático en Latinoamérica (Pág. 40 – Año: 2005) dice: "El Abuso de Dispositivos consiste en la posesión y el uso ilícitos de aparatos de comunicación y de cualquier medio electrónico diseñado para emitir o recibir señales".

Es el uso y la posesión de la tecnología utilizada por los atacantes para lograr explotar las vulnerabilidades que representa el riesgo denominado como Tempest por los estándares internacionales de seguridad de la información.

Este riesgo consiste en captar a distancia la radiación emitida por los equipos que conforman los sistemas de información, con el ánimo de decodificarla y obtener una lectura de la información que viaja o es presentada a través de ellos.

Daños

Guillermo Cabanellas de las Cuevas, Diccionario Elemental Jurídico (Pág. 109, Año 2003) dice: "El daño puede provenir de dolo, de culpa o de caso fortuito, según el grado de malicia, negligencia o casualidad entre el autor y el efecto. En principio el daño doloso obliga al resarcimiento y acarrea una sanción penal, el culposo suele llevar consigo tan sólo indemnización; y el fortuito exime en la generalidad de los casos, dentro de la complejidad de esta materia."

Físicos

http://www.monografias.com/trabajos28/dano-derecho/danoderecho.shtml dice: "Esto es cuando la persona que comete el delito causa daños físicos al hardware del equipo objeto del delito". Aquí el daño físico se puede ocasionar de

muchas formas por la persona que tiene la intención de causar daño.

Esto puede ocurrir de varias formas, por ejemplo:

- Uso de instrumentos para golpear, romper o quebrar un equipo de cómputo, ya sea el daño completo o parcial.
- Uso de líquidos como café, agua o cualquier líquido que se vierta sobre el equipo y dañe las piezas y componentes electrónicos.
- Provocar apagones o cortos en la energía eléctrica con intención de causar daños en el equipo.
- Utilizar bombas explosivas o agentes químicos que dañen el equipo de cómputo.
- Arrancar, o quitar componentes importantes de algún dispositivo del equipo, como CD-ROM, CD-RW, Disco de 3 ½, Discos Duros, Impresoras, Bocinas, Monitores, MODEM, Tarjetas de audio y video, etc.

Y cualquier otra forma que dañe la integridad del equipo de cómputo.

Lógicos

http://www.monografias.com/trabajos28/dano-derecho/danoderecho.shtml dice: "Esto comprende los daños causados a la información y todos los medios lógicos de los cuales se vale un Sistema de Cómputo para funcionar adecuadamente; o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático".

Este tipo de daño a un sistema se puede alcanzar de diversas formas. Desde la más simple que podemos imaginar, como desenchufar el ordenador de la electricidad mientras se esta trabajando con él o el borrado de documentos o datos de un archivo, hasta la utilización de los más complejos programas lógicos destructivos (crash programs), sumamente riesgosos para los sistemas, por su posibilidad de destruir gran cantidad de datos en un tiempo mínimo. Estos

programas destructivos, utilizan distintas técnicas de sabotaje, muchas veces, en forma combinada.

La jurisprudencia francesa registra un ejemplo de este tipo de casos. Un empleado programó el sistema de tal forma que los ficheros de la empresa se destruirían automáticamente si su nombre era borrado de la lista de empleados de la empresa.

Otra modalidad que actúa sobre los programas de aplicación es el llamado «cáncer de rutinas» («cancer routine»).

En esta técnica los programas destructivos tienen la particularidad de que se reproducen, por sí mismos, en otros programas, arbitrariamente escogidos.

Una variante perfeccionada de la anterior modalidad es el «virus informático» que es un programa capaz de multiplicarse por sí mismo y contaminar los otros programas que se hallan en el mismo disco rígido donde fue instalado y en los datos y programas contenidos en los distintos discos con los que toma contacto a través de una conexión.

Sujetos

SOLER, Sebastián, Derecho Penal Argentino, tomo 4, (Año 1992 - Pág. 121): "En derecho penal, es la ejecución de la conducta punible supone la existencia de dos sujetos, a saber, un sujeto activo y otro pasivo. Estos, a su vez, pueden ser una o varias personas naturales o jurídicas. De esta suerte, el bien jurídico protegido será en definitiva el elemento localizador de los sujetos y de su posición frente al delito.

Así, el titular del bien jurídico lesionado será el sujeto pasivo, quien puede diferir del sujeto perjudicado, el cual puede, eventualmente, ser un tercero. De otra parte, quien lesione el bien que se protege, a través de la realización del tipo penal, será el ofensor o sujeto activo".

Sujeto Activo

De acuerdo al profesor chileno Mario Garrido Montt, se entiende por tal quien realiza toda o una parte de la acción descrita por el tipo penal.

Son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aún cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "**delitos informáticos**", estudiosos en la materia los han catalogado como "**delitos de cuello blanco**" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

Entre las características en común que poseen ambos delitos tenemos que: "el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional".

A este respecto Marcelo Huerta y Claudio Líbano dicen que: "En lo relativo a tratarse de "Ocupacional Crimes", es cierto que muchos de los delitos se

cometen desde dentro del sistema por personas que habitualmente lo operan y que tienen autorizado los accesos. Sin embargo, las tendencias modernas apuntan hacia el campo de la teleinformática a través del mal uso del ciberespacio y las super carreteras de la información o redes de telecomunicaciones. Es decir, cada día gana más terreno el delito informático a distancia."

Como sostiene Gutiérrez Francés, "con carácter general, la delincuencia mediante computadoras se inscribe dentro de las formas de criminalidad de "Cuello Blanco", propias de la delincuencia económica, por lo cual desde el punto de vista criminológico, presentan las mismas peculiaridades que ésta, con las notas específicas que aporta lo informático"**.**

Los principales responsables de estos ataques son personas o grupo de personas que aprovechan las vulnerabilidades y son:

Hackers

El apelativo de hacker se crea a fines del siglo pasado cuando los Estados Unidos de América empiezan a recibir un masivo movimiento migratorio de personas de todos los países del mundo que esperaban encontrar en el "país de las oportunidades" un bienestar económico y progreso.

Los hackers eran estibadores informales que se pasaban todo el día bajando las maletas y bultos de las personas y familias completas que llegaban en los barcos a los puertos de New York, Boston, San Francisco, etc. Estos trabajadores eran infatigables, pues trabajaban muchas veces sin descansar y hasta dormían y comían entre los bultos de los muelles con el objeto de no perderse una oportunidad de ganar dinero.

La palabra "hack" en inglés tiene varios significados en español, entre ellos "hacha". Como si fuesen taladores de árboles que usan su hacha, en forma infatigable hasta llegar a tumbarlos, su tesonero propósito les mereció este apelativo.

La palabra hacker aplicada en la computación se refiere a las personas que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites.

Los hackers tienen "un saludable sentido de curiosidad: prueban todas las cerraduras de las puertas para averiguar si están cerradas. No sueltan un sistema que están investigando hasta que los problemas que se le presenten queden resueltos".

Cracker

Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en Internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas.

Obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. Asimismo se debe mencionar que no todos los hackers se convierten en crackers.

Phreaker

El phreaker es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares.

Construyen equipos electrónicos artesanales que pueden interceptar y hasta

ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos.

Insiders

Según un reciente informe de la publicación estadounidense InformationWeek, un porcentaje sustancial de instrucciones en las redes de las empresas (ya sean chicas, medianas o grandes) proviene de ataques internos. Es decir, los mismos empleados hackean a su propia organización.

Outsiders

El outsider es la persona que conoce muy bien la instalación de una organización pero no pertenece a ella. Son aquellos que ingresan a la red simplemente averiguando un password autorizada. El aprovechamiento ilícito de las vulnerabilidades da lugar al delito informático que pueden originar en muchos casos siniestros informáticos

Sujeto Pasivo

El sujeto pasivo es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo.

En primer término tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los "delitos informáticos", ya que mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever

las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Dado lo anterior, “ha sido imposible conocer la verdadera magnitud de los “delitos informáticos”, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables” y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos.

La falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada “cifra oculta” o “cifra negra”.

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro.

Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".

Este nivel de criminalidad se puede explicar por la dificultad de reprimirla en forma internacional, ya que los usuarios están esparcidos por todo el mundo y, en consecuencia, existe una posibilidad muy grande de que el agresor y la víctima estén sujetos a leyes nacionales diferentes.

Además, si bien los acuerdos de cooperación internacional y los tratados de extradición bilaterales intentan remediar algunas de las dificultades ocasionadas por los delitos informáticos, sus posibilidades son limitadas, además de que en algunos países como el nuestro no existe legislación alguna sobre esta clase de conductas ilícitas lo que empeora más la situación de las víctimas de estas conductas ilícitas.

Manipulación

La manipulación es la sustracción de datos, modificación de programas existentes en el sistema o en insertar nuevos programas o rutinas. Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente tiene conocimientos técnicos concretos de informática y programación.

Manipulación de los datos

Este fraude conocido también como sustracción de datos, representa el delito informático mas representativo ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos. De acuerdo a la información entregada por entidades de

seguridad a nivel mundial, el 75% de los casos de sustracción de datos lo realiza personal interno de la organización o que pertenecieron a ellos.

Manipulación de programas

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas. Uno de los métodos utilizados por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Manipulación informática

Es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.

Existe una diferencia en las estafas informáticas cometidas dentro del sistema y las cometidas fuera del sistema. Las primeras son las manipulaciones realizadas directamente sobre el sistema operativo, y no existe ningún engaño ni error sobre un ser humano. Las estafas cometidas fuera del sistema, son las manipulaciones de datos hechas antes, durante o después de la elaboración de los programas, siendo éstas las causantes del engaño que determina una alteración intencional de la disposición patrimonial.

Metodología de ataque

Los ataques pueden servir a varios objetivos incluyendo fraude, extorsión, robo de información, venganza o simplemente el desafío de penetrar un sistema. Esto puede ser realizado por empleados internos que abusan de sus permisos de

acceso, o por atacantes externos que acceden remotamente o interceptan el tráfico de red. A esta altura del desarrollo de la "sociedad de la información" y de las tecnologías computacionales, los piratas informáticos que producen los ataques ya no son novedad.

Los hay prácticamente desde que surgieron las redes digitales, hace ya unos años atrás. Sin duda a medida que el acceso a las redes de comunicación electrónica se fue generalizando, también se fue multiplicando el número de quienes ingresan "ilegalmente" a ellas, con distintos fines, por eso es importante conocer la metodología de ataque que usan los atacantes.

El objetivo de la metodología de ataque es describir cuales son los métodos más comunes que se utilizan hoy para perpetrar ataques a la seguridad informática (estos ataques a la confidencialidad, integridad y disponibilidad de la información) de una organización o empresa, y que armas podemos implementar para la defensa, ya que saber cómo nos pueden atacar. Es tan importante como saber con qué soluciones contamos para prevenir, detectar y reparar un siniestro de este tipo. Sin olvidar que éstas últimas siempre son una combinación de herramientas que tienen que ver con tecnología y recursos humanos (políticas, capacitación), las cuales se describen a continuación:

Identificación

Networks Scanners.- Hacen un mapa de la red identificando: dominios, servidores, sistemas operativos. Recogiendo información sin atacar y descubriendo: Los servidores activos, servidores de correo, nombres de empleados, rango de direcciones IP.

Exploración

Ports Scanners.- Scanean las máquinas para detectar puertos abiertos, a fin de identificar posibles exposiciones o vulnerabilidades a explotar. Sistemas activos, servicios a la escucha, sistemas operativos.

Enumeración.- Obtención de usuarios válidos o recursos compartidos mal protegidos.

Obteniendo acceso

Passwords Crakers.- Se usan para detectar la confirmación de usuarios y passwords válidos. Obteniendo la password para los usuarios/servicios

Escalando privilegios.- Obteniendo el Super Usuario, que es el usuario administrador, que permite realizar todas las operaciones posibles en el sitio y/o la red.

Robando accesos.- Buscando otros accesos válidos o rutas que permitan obtener información de la organización.

Cubriendo la huella.- Buscando logs y borrando todas las pistas de Auditoría, de manera tal que salgan sin dejar rastro.

Creando entradas traseras

Crear cuentas de usuario, buscando los archivos deseados.

Los métodos de ataque descritos, están divididos en categorías generales que pueden estar relacionadas entre sí, ya que el uso de un método en una categoría permite el uso de otros métodos en otras. Por ejemplo: después de crackear una password, un intruso realiza un login como usuario legítimo para navegar entre los archivos y explotar vulnerabilidades del sistema. Eventualmente también, el atacante puede adquirir derecho de acceso a lugares que le permitan dejar un virus u otras bombas lógicas para paralizar todo un sistema antes de huir.

Herramientas de Ataque

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para explotar "agujeros" en el diseño, configuración y operación de los sistemas. Esto permitió a los nuevos atacantes tomar control de sistemas completos, produciendo verdaderos desastres que en muchos casos llevó a la desaparición de aquellas organizaciones o empresas con altísimo grado de

dependencia tecnológica (bancos, servicios automatizados, etc.).

Detallaré a continuación las herramientas más utilizadas en el área de un siniestro informático son:

- **Networks Scanners**.- Es la que ayuda mediante un mapa de la red identificando: dominios, servidores y sistemas operativos.

- **Ports Scanners.-** Escanean las máquinas para detectar ports abiertos, a fin de identificar posibles exposiciones a explorar.

- **Passwords crackers.-** Se usan para detectar la confinación de usuarios y passwords válidos.

- **Packet Sniffers.-** Permiten leer la información de los paquetes que pasan por la red donde están instalados.

- **War Dialers.-** Son los que permiten detectar modems en las líneas de teléfono.

- **Trojans.-** Permiten introducir back doors en las redes.

Inseguridad Informática

Revista de Ingeniería. No.19. Universidad de los Andes. Facultad de Ingeniería. (Pág. 01 - Año: 2004) dice: "Es el conjunto de técnicas de hacking y análisis de riesgos, que permita a las organizaciones aprender de sus fallas de seguridad y fortalecer sus esquemas de seguridad, no para contar con mayores niveles de seguridad, sino para evidenciar el nivel de dificultad que deben asumir los intrusos para ingresar a los sistemas".

La inseguridad informática es la falta o poca presencia de seguridad informática en un sistema operativo, aplicación, red o dispositivo, esto permite su

demostración por hackers éticos (sombreros blancos) o su explotación por hackers mal intencionados (sombreros negros).

Desconocimiento

Guillermo Cabanellas de las Cuevas, Diccionario Elemental Jurídico (Pág. 125, Año 2003) respecto a desconocer dice: “No conocer o ignorar. No identificar a una persona”.

Muchas de las veces existen muchas personas que por desconocimiento de las diferentes actividades delictuosas que por el avance tecnológico se dan y por la interceptación de comunicaciones de los diferentes medios que hoy en día existen permiten la vulnerabilidad de la intimidad de las personas ya sean estas públicas o privadas.

Beneficios a terceros

Guillermo Cabanellas de las Cuevas, Diccionario Elemental Jurídico (Pág. 125, Año 2003) respecto a Beneficio dice: “El bien que se hace o se recibe”. Pudiendo así ratificar que por la comitiva de este tipo de delitos se benefician terceras personas especialmente económicamente ya que la información que se obtenido de manera ilegal permite mejorar la calidad de esta para provocar graves daños económicas y especialmente morales a las personas o inclusive a la sociedad. No olvidemos que también puede de una u otra manera beneficiarse cierta parte del sector empresarial”.

Vulnerabilidad de la Intimidad

Para Wilches la vulnerabilidad consiste en: "La incapacidad de una comunidad para absorber, mediante auto ajuste, los efectos de un determinado cambio en su medio ambiente, o sea, su no flexibilidad o incapacidad para adaptarse a ese cambio, que para la comunidad constituye un riesgo".

Según el profesor Sanz Caja la vulnerabilidad, “Es la cualidad que le hace

susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseada, de recibir algún daño o perjuicio en cualquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático".

Según el diccionario de la Real Academia de la Lengua Española Intimidad es la "zona espiritual y reservada de una persona o un grupo, especialmente una familia".

Miguel A. Ekmekdjian, Intimidad lo definió como: "La facultad que tiene cada persona de disponer de una esfera, ámbito: privativo o reducto infranqueable de libertad individual, el cual no puede ser invadido por terceros, ya sean particulares o el propio Estado, mediante cualquier tipo de intromisiones, las cuales pueden asumir diversos signos"

Con otros fundamentos, Humberto Quiroga Lavié reflexiona que en el concepto de intimidad y lo define como: "el respeto a la personalidad humana, del aislamiento del hombre, de lo íntimo de cada uno, de la vida privada, de la persona física, innata, inherente y necesaria para desarrollar su vida sin entorpecimientos, perturbaciones y publicidades indeseadas". Y continúa: "Es un derecho personalísimo que permite sustraer a las personas de la publicidad o de otras turbaciones a su vida privada, el cual está limitado por las necesidades sociales y los intereses públicos".

La intimidad es un derecho fundamental establecido en la Constitución Española de 1978, el Art. 18 establece:

1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

Las vulnerabilidades que no son otras cosas que debilidades, fallas de los sistemas, los mismos que son explotados por personas mediante ataques informáticos. Estos ataques son los incrementados al punto que ya contamos con estadísticas de los mismos.

Violación de reserva industrial o comercial.

Es el empleo, la revelación y la divulgación de descubrimientos, invenciones científicas, procesos o aplicaciones industriales o comerciales que deban permanecer en reserva, llegados al conocimiento del delincuente en razón de su cargo o habiendo accedido a ellos indebidamente. Pueden encuadrarse las actividades de hacking mediante las cuales es publicada en la Red información confidencial de empresas privadas que han sido previamente atacadas, cuando esa información se refiere, por ejemplo, a las formas de burlar las medidas de seguridad anticlonación de teléfonos celulares por parte de un ingeniero empleado por una de las empresas de telefonía móvil.

Persona

Jurídicamente se define a la persona, como todo ente susceptible de adquirir derechos y contraer obligaciones. En el mismo sentido entienden generalmente al concepto la mayoría de los ordenamientos jurídicos actuales; no obstante, el contenido semántico de dicho concepto ha variado considerablemente en distintas épocas y sistemas jurídicos. Así por ejemplo, en la antigua Roma se requería los status de hombre libre, ciudadano y pater familias para ser persona y no se consideraban tal a muchísimos seres humanos (tal es el caso de los esclavos). Actualmente se las clasifica en personas de existencia visible o físicas (ser humano) y personas de existencia ideal o jurídica (como las sociedades, las corporaciones, las fundaciones, el Estado y otras).

Persona Natural

Persona Natural es una persona humana que ejerce derechos y cumple obligaciones a título personal, individuales, físicas, simples o concretas que son los individuos de la especie humana y sólo ellos.

Persona Jurídica

Se entiende por persona jurídica (o persona moral) a un sujeto de derechos y obligaciones que existe físicamente pero no como individuo humano sino como institución y que es creada por una o más personas físicas para cumplir un papel. En otras palabras, persona jurídica es todo ente con capacidad para adquirir derechos y contraer obligaciones. Persona Jurídica es una empresa que ejerce derechos y cumple obligaciones a nombre de ésta. Al constituir una empresa como Persona Jurídica, es la empresa (y no el dueño) quien asume todos los derechos y las obligaciones de la empresa. Lo que implica que las deudas u obligaciones que pueda contraer la empresa, están garantizadas y se limitan sólo a los bienes que pueda tener la empresa a su nombre (tanto capital como patrimonio).

Personas jurídicas de derecho público.

Son aquellas que han sido creadas mediante ley y legitima para actuar tanto pública como privadamente.

Personas jurídicas de derecho privado.

Aquellas que se crean por iniciativa privada ya sea por negocio o contrato, sometida en cada caso por una ley determinada. Reglas privadas.

Violación ilícita de comunicaciones.

Son aquellas conductas de sustracción, ocultamiento, extravío, destrucción, interceptación, control o impedimento de comunicaciones privadas

dirigidas a persona diferente de quien despliega esta conducta.

Adicionalmente tipifica el enterarse indebidamente del contenido de estas comunicaciones y la revelación de las mismas.

Espionaje

Es la obtención, el empleo y la revelación indebida de secretos políticos, económicos o militares relacionados con la seguridad del Estado. En este delito pueden encuadrarse todas las actividades informáticas o computacionales tendientes a obtener la información mencionada en el tipo penal. Pueden encuadrarse prácticamente todas las conductas descritos en los tipos penales anteriores, siempre y cuando el objeto material de los delitos sean secretos políticos, económicos o militares relacionado con la seguridad del Estado.

Difamar

La difamación es la comunicación a una o más personas con ánimo de dañar, de una acusación que se hace a otra persona física o moral de un hecho cierto o falso, determinado o indeterminado, que pueda causar o cause a ésta una afectación en su honor, dignidad o reputación.

Los orígenes en el derecho anglosajón de la difamación están en los agravios (declaración dañosa en una forma transitoria, sobre todo de forma hablada) y libelo (declaración dañosa en un medio fijo, sobre todo escrito pero también un cuadro, signo, o emisión electrónica), cada uno de los cuales da un derecho de acción.

La diferencia fundamental entre libelo y difamación está únicamente en la "forma" en la cual la materia difamatoria es publicada.

Si el material ofensivo es publicado en alguna forma efímera, como en forma hablada o sonidos, dactilología, gestos y otros por el estilo, entonces esto es difamación.

Si es publicado en una forma más duradera, por ejemplo en documentos, películas, discos compactos y otros por el estilo, entonces es considerado un libelo.

Divulgación y empleo de documentos reservados.

Son conductas punibles la divulgación y el empleo de documentos reservados en provecho propio o ajeno. En este delito se puede encuadrar la conducta del hacker que, habiendo accedido al sistema de su víctima, copia un archivo reservado de esa persona y lo publica e la Red o lo distribuye por cualquier otra vía. También se puede encuadrar el realizar maniobras no autorizadas de fuerza bruta con el ánimo de revelar las claves o las llaves con las que han sido encriptados documentos confidenciales.

Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas.

Es el ofrecimiento, la venta o la compra, no autorizados, de instrumentos aptos para interceptar la comunicación privada entre personas. Se podrán incluir como conductas encuadrables en este delito las actividades relacionadas con la comercialización de sniffers.

Esto tendrá lugar solamente cuando el Estado, actualizando la legislación, establezca la necesidad de obtener autorizaciones para la compra y uso de estos programas por razones de seguridad pública, debido al riesgo que implican para los usuarios desprevenidos de la Red.

Hipótesis

¿La ausencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos provoca la vulnerabilidad de la intimidad en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado del cantón Quito durante el período 2009?

Determinación de Variables

- **Variable Independiente**

La ausencia de normativa jurídica respecto a la Interceptación de Comunicaciones y Abuso de Dispositivos**.**

- **Variable Dependiente**

La vulnerabilidad de la intimidad en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado del cantón Quito durante el período 2009.

CAPÍTULO III

METODOLOGÍA

Enfoque de la Investigación

La investigación se desarrollará a través del paradigma cualitativo, que se revela por medio de las propiedades del objeto de estudio, lo que a su vez se expresa de un concepto global del objeto, es decir de un conjunto de propiedades que constituyen su cualidad.

Modalidad de la Investigación

De Campo

El paradigma de la investigación cualitativa de campo, permite que se describa el fenómeno de estudio. Esta ubicación paradigmática de la lógica de la investigación implica la necesidad de:

- Utilizar la inferencia inductiva de los datos que van a ser recolectados en las encuestas.

- Utilizar los criterios de credibilidad, transferibilidad y confirmabilidad como formas en el análisis y verificación de los resultados.

- Por el lugar es de campo, ya que el estudio se desarrollará en el lugar donde ocurren los acontecimientos.

Para la interpretación de los resultados a ser obtenidos requieren un tratamiento estadístico, lo cual nos permite el análisis y la descripción del objeto de estudio.

Para el desarrollo de esta investigación se usará del método deductivo, como método general, por cuanto se parte de una hipótesis que se comprobará durante el desarrollo del trabajo para llegar a las conclusiones y generalizaciones.

Bibliográfica – documental

Es de vital importancia y por ende se constituye en un valiosísimo aporte para determinar la influencia del cometimiento de ciertas conductas delictivas aun no reconocidas en nuestra normativa jurídica.

Las modalidades especiales

Proyecto de intervención social; se empleará para desarrollar el trabajo investigativo de manera holística la cual permitirá interpretar y evaluar la situación la elaboración de un modelo viable.

Considerando la evolución y producción de nuevas tecnologías permitiendo de esta manera reconocer nuevas amenazas y formas de cometer delitos informáticos a través de un computador ya que nuestra sociedad necesita una atención urgente en este campo.

Tipo de la Investigación

Explicativo

Se podrá determinar y detectar las causas mismas del porqué el cometimiento de ciertos delitos informáticos aún no reconocidos en nuestra sociedad, basada en conocimientos informáticos existentes tanto físico como lógicos estudiada en el derecho informático con base a la realidad de la problemática de estudio podré elaborar la propuesta.

Descriptivo

Por su alcance la investigación objeto del estudio y de ésta manera se

comparará varias situaciones y estructuras clasificando de esta manera varios elementos permitiendo reconocer varios tipos de delitos informáticos aún no reconocidos que por su naturaleza servirá para la toma de decisiones, que se traducen en la elaboración y diseño de la propuesta.

Exploratorio

Nos permitirá desarrollar nuevos métodos y soluciones al problema planteado que responden a una necesidad de interés de tipo informático, jurídico - social ya que para muchos la criminalidad informática es un problema desconocido en nuestra sociedad.

Asociación de Variables

El tipo de Investigación que el Trabajo logrará es en base a la Asociación de variables porque permitirá analizar y valorar el grado de correlación y comportamiento de las variables de estudio.

Población y Muestra

La población motivo de nuestra investigación la componen la Fiscalía General del Estado (Departamento de Investigación y Análisis), la Policía Judicial (Departamento de Criminalística); y, Abogados especializados en Informática Jurídica.

Unidades de Observación	Número
Fiscalía General del Estado (Departamento de Investigación y Análisis Forense)	8
Policía Judicial (Departamento de Criminalística)	2
Profesional del Derecho, Estudiantes	20
TOTAL	30

Cuadro Nº 01
Fuente: Investigador
Elaboración por: César E. Naranjo Mesías

Muestra:

Partiendo de la importancia que tiene la vulnerabilidad de las comunicaciones en nuestro país y el abuso indiscriminado de dispositivos se aplicarán las técnicas e instrumentos de investigación adecuados.

De ésta manera permitirán el registro exclusivo y preciso de los hechos o fenómenos que intervienen en la investigación.

Por considerar que el número de elementos de la población a ser investigada es inferior a cien se trabajará con todo el universo sin que sea necesario sacar una muestra representativa.

Operacionalización de Variables

VARIABLE INDEPENDIENTE: La ausencia de normativa jurídica respecto a la Interceptación de Comunicaciones y Abuso de Dispositivos

CONCEPTUALIZACIÓN	CATEGORIAS	INDICADORES	ITEMES BÁSICOS	TÉCNICAS INSTRUMENTOS
Interceptación de Comunicaciones y Abuso de Dispositivos se conceptúa como: Operaciones ilícitas realizadas por cualquier medio de comunicación especialmente a través de dispositivos Informáticos o del Internet; que tienen como objetivo, duplicar, destruir y vulnerar la información, medios electrónicos y redes de comunicación.	Daños	• Físicos • Lógicos	¿Cree usted que debería existir policía especializada en informática? ¿Cree usted que se debería incluirse nuevas normas para detectar los diferentes tipos de daños informáticos?	Cuestionario estructurado al departamento de investigación Análisis Forense de la Fiscalía General del Estado del universo de investigación.
	Procedimientos	• Materiales • Tecnologías de Información	¿La destrucción de un computador o la ocultación de información de un sistema informático son realizadas por terceras personas o trabajadores de una misma empresa? ¿Cree que la Auditoría Informática controlaría de mejor manera el ocultamiento o destrucción de documentos electrónicos?	Entrevista focalizada a personas que trabajan en la Policía Judicial, Abogados y Sociedad en la ciudad de Quito.

Cuadro Nº 02
Fuente: Investigador
Elaboración por: César E. Naranjo Mesías

VARIABLE DEPENDIENTE: Vulnerabilidad de la Intimidad.

CONCEPTUALIZACIÓN	CATEGORÍAS	INDICADORES	ITEMES BÁSICOS	TÉCNICAS INSTRUMENTOS
Vulnerabilidad de la intimidad se conceptúa como: El tener acceso ilegal o deliberado de la información para ocasionar daños materiales o morales en contra de otro individuo.	INSEGURIDAD JURÍDICA DAÑOS ALTERACIÓN DE INMFORMACIÓN	• Desprotección de información. • Morales • Materiales • Mecanismos • Transmisión	¿Cree usted que mediante el uso de nuevas tecnologías es aprovechada con fines delictivos? ¿Cree usted que se necesita regular urgentemente este tipo de acciones? ¿Cree usted que la alteración de información ser produce por la falta de control? ¿Cree que las defraudaciones como la alteración de información afectan a la sociedad o al Estado?	Cuestionario estructurado al departamento de investigación Análisis Forense de la Fiscalía General del Estado del universo de investigación. Entrevista focalizada a personas que trabajan en la Policía Judicial, Abogados y Sociedad en la ciudad de Quito.

Cuadro : Nº 03
Fuente : Investigador
Elaboración por: César E. Naranjo Mesías

Técnicas e Instrumentos

Entrevista:

Dirigida al Director Nacional de Investigación y Análisis Forense de la Fiscalía General del Estado del Cantón Quito, mediante preguntas planificadas previamente, a fin de alcanzar fidelidad en el total de la información obtenida.

Encuesta:

Destinada a obtener datos de los sujetos relacionados con el problema que es materia de investigación, cuyas opiniones impersonales, serán observadas y evaluadas, mediante un listado de preguntas escritas.

Fichas de observación:

Servirán de apoyo al investigador; en las que se registrará en forma ordenada los datos que se vayan obteniendo, de la investigación observada; para su posterior análisis.

Validez y confiabilidad:

La validez de los instrumentos empleados vendrá dada por la técnica llamada "Juicio de expertos", a fin de llegar a la esencia del objeto de estudio.

Plan para la recolección de la Información.

PREGUNTAS BÁSICAS	EXPLICACIÓN
1.- ¿Para qué?	Para alcanzar los objetivos de investigación
2.- ¿De qué personas u objetos?	Departamento de Análisis Forense, Departamento de Criminalística, Estudiantes, Profesionales del Derecho.
3.- ¿Sobre qué aspectos?	Interceptación de Comunicaciones, Abuso de Dispositivos y Vulnerabilidad de la Intimidad.
4.- ¿Quién? ¿Quienes?	Investigador
5.- ¿Cuándo?	Año 2009.
6.- ¿Dónde?	Departamento y Análisis Forense de la Fiscalía General del Estado
7.- ¿Cuántas veces?	Una sola vez.
8.- ¿Qué técnicas de recolección?	Entrevista y Encuesta.
9.- ¿Con qué?	Cuestionario
10.- ¿En que situación?	Directores y Funcionarios: Fiscalía General del Estado. Investigadores: Policía Judicial. Estudiantes: Carrera Derecho. Profesionales: Abogados

Cuadro Nº 04
Fuente : Investigador.
Elaborado por: César E. Naranjo Mesías

Plan de Procesamiento de la Información

Los datos recogidos (datos en bruto) se transforman siguiendo ciertos procedimientos:

- Revisión crítica de la información recogida; es decir limpieza de información defectuosa: contradictoria, incompleta, no pertinente, etc.

- Repetición de la recolección, en ciertos casos individuales, para corregir fallas de contestación.

- Tabulación o cuadros según variables de cada hipótesis: cuadros de una sola variable, etc.

- Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente, que no influye significativamente en los análisis)

- Estudio estadístico de datos para presentación de resultados.

- Análisis de las encuestas e entrevistas para mejorar nuestro estudio respecto a la informática jurídica.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Análisis de los resultados

El arte de análisis de datos seleccionada, se denominada análisis de contenido que es una técnica que permite el examen metódico, sistemático y objetivo del contenido de ciertos textos con vistas a clasificar e interpretar sus elementos constitutivos.

El procedimiento para codificar las preguntas abiertas, constantes en las entrevistas efectuadas, consistirá en establecer patrones generales de respuesta (respuestas similares o comunes), y después formular conclusiones.

Para el procesamiento de la información obtenida de las encuestas aplicadas a la población seleccionada, se empleará fundamentalmente la matriz de vaciado de datos, que permite el conteo y organización adecuada de los mismos.

Se realizará una descripción e interpretación de cada categoría y luego del total de ellas, lo que permitirá realizar un cierre conclusivo que comprende las principales observaciones que contiene la investigación.

Análisis de Procesos

El poder como tal siempre ha sido problemático y peligroso; problemático puesto que la libertad y el destino del individuo deben ceñirse a una estructura política donde su independencia debe transformase en obediencia exigible incluso por la fuerza; y peligroso ya que, por naturaleza el poder tiende a la arbitrariedad, al abuso. Para contrarrestar la tensión existente, surge el Debido Proceso, como garantía constitucional de todo individuo para ejercer su derecho de defensa y

obtener de los órganos judiciales y administrativos un proceso justo, pronto y transparente, siendo este el punto de partida del análisis siguiente.

En la actualidad surgen varios problemas como es el cómo detectar si está siendo o no vulnerado su intimidad, un sistema informático, el principal objetivo es obtener información para de esta manera extorsionar, cometer fraudes, estafas e inclusive sacar dinero de cuentas bancarias, la delincuencia organizada.

De igual forma opta por los diferentes avances tecnológicos para cometer delitos como el terrorismo, narcotráfico, lo peor del caso es la pornografía infantil, tráfico de órganos y en sí muchos delitos que verdaderamente atentan contra la integridad de las personas.

Por esta razón mi investigación va encaminada a que se reconozca la interceptación de comunicaciones y principalmente que se controle el uso de dispositivos para mayor seguridad y protección de nuestro derecho a la intimidad reconocida en nuestra Constitución.

Conclusiones del Proceso

- Existen muchas denuncias que no se han dado el tratamiento adecuado para una verdadera identificación de los sujetos que cometen este tipo de delitos, los cuales al no existir las sanciones adecuadas en nuestra legislación penal quedan en la impunidad.
- De esta forma necesitamos un verdadero control acerca del uso de las comunicaciones y sus dispositivos, estos son los principales blancos de personas inescrupulosas para apoderarse de información confidencial para atentar de esta manera contra la privacidad e intimidad de las personas.
- Queda demostrado la necesidad concientización a nuestra sociedad del peligro que día a día corremos al no tener una verdadera cultura informática y tecnológica globalizada que existe hoy en día.
- De igual forma la inseguridad informática evoluciona y propone nuevos retos a la sociedad ecuatoriana.

- Retos que se manifiestan en variables humanas, técnicas o procedimentales que logran generar importantes niveles de incertidumbre, que de manera definitiva impactan uno de los activos más importantes de las organizaciones modernas: la información.
- El derecho clásico puede servir en un primer momento para soportar una legislación híbrida y resolver los desfases en los ritmos de crecimiento, desarrollo como de adaptación de la informática en la producción de bienes y servicios - altamente movibles en los sectores de punta productivos frente a su lentitud en los servicios, principalmente el sector judicial.
- En un segundo momento, será necesaria la actualización, adaptación o creación de nuevas nociones jurídicas. Normas que tengan en cuenta las características y funciones de las nuevas tecnologías y la evolución del derecho.Es importante dimensionar este problema de acuerdo a las entrevistas y encuestas realizadas convirtiéndose así en una problemática dura para nuestra sociedad.
- De todas formas hay que ser cuidadoso cuando alguien, a través de cualquier medio, pide información personal o bancaria, de esta manera ayudar a concientizar a nuestra sociedad de los peligros que corremos al mal utilizar la tecnología y los diferentes medios de comunicación.
- Por los considerandos anteriores se establece que al no estar reconocida las figuras jurídicas como la interceptación de comunicaciones y abuso de dispositivos, sin lugar a dudas existe un desamparo total al derecho a la intimidad y de esta manera cada uno de los usuarios de los distintos tipos de comunicaciones estemos desprotegidos.

Análisis de Entrevistas

1.- ¿De acuerdo a su experiencia que realmente le preocupa respecto a la vulnerabilidad de la intimidad?

En relación a esta interrogante los entrevistados, manifiestan por un lado que lo verdaderamente preocupante es la manipulación de datos; por otro lado

dicha información es mal canalizada para obtener resultados delictuosos de graves consecuencias que no sólo atentan al derecho de la intimidad, sino vulneran también la propiedad intangible o comúnmente conocida como derechos de autor, reservas industriales y comerciales, etc.

Conclusión

De la opinión vertida por los entrevistados es lógico concluir, que la ausencia de normativa respecto a la interceptación ilegal de comunicaciones y el abuso indiscriminado de dispositivos por el sujeto activo del delito, se constituye en la principal causa en el retardo de una sanción oportuna, hasta en ocasiones este tipo de delitos quedan impunes.

2.- ¿Hay hechos que verdaderamente empeoran esta situación?

Con respecto a esta pregunta las personas entrevistadas responden, es la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, la ausencia de la equiparación de éstos delitos en los tratados internacionales de extradición; además de la falta de una verdadera cultura informática en nuestra sociedad, sumado a ello el aspecto que no existe un estudio informático - jurídico previo, a fin de que no estandarice a las personas, que en la mayoría de casos son los mismos empleados, uno de los entrevistados manifiesta que lo que empeora la situación es la apropiación ilícita de comunicaciones.

Conclusión

La situación jurídica-informática por la que a traviesa la sociedad ecuatoriana, con el paso de los días va en decadencia, circunstancia que provoca a la par el desconocimiento, dificultad y aprovechamiento del crimen organizado y de muchas personas inescrupulosas que acceden a servicios de vital importancia

para las personas, no solo para las personas sino también para el Estado que resultan ser los más perjudicados.

3.- ¿Quién considera usted que debería asumir el control referente a las comunicaciones, el uso de dispositivos para que se proteja el derecho a la intimidad? ¿Por qué?

En referencia a esta pregunta los entrevistados exponen, que al no existir quien asuma este tipo de control manifiestan que se debería crear un organismo corrector de manera independiente de los ya existentes, además de contar con personas especializadas tanto el ámbito jurídico como el informático en la Policía Judicial, sea directa o indirectamente. Es el Estado también el encargado de crear mecanismos que permitan un verdadero control, canalizando de la mejor manera las nuevas tecnologías que en nuestra sociedad estamos totalmente al descubierto y vulnerables al plagio de información con fines inescrupulosos.

Conclusión

Si bien los responsables del cometimiento de este tipo de delitos y al no existir una norma que realmente los sancione realmente queda en la impunidad, ya que no se puede suplantar con otras figuras jurídicas, es de vital importancia que se reforme nuestro Código Penal y el Estado es el encargado de garantizar que se tome medidas drásticas de manera urgente porque a medida que evoluciona la tecnología la sociedad ecuatoriana sigue siendo vulnerada y en muchos de los casos el blanco perfecto de la delincuencia organizada.

4.- ¿Cómo debería asumir esta responsabilidad la institución o persona señalada por usted?

Con respecto a esta pregunta las personas entrevistadas, manifiestan que el Estado debería designar un fondo y dotar de nuevas tecnologías a las personas encargadas de investigar, indagar y descubrir este tipo de delitos, estableciendo un rubro en el presupuesto del Estado, encaminado al control de los diferentes tipos

de comunicaciones.

Conclusión

La responsabilidad en cuanto al promover una reforma y revisión de nuestro Código Penal, debería ser asumida por el Estado, mediante la creación de un organismo independiente como así ocurre en países especialmente europeos, esto conlleva el propósito que las personas no sean víctimas de los diferentes ataques informáticos acorde al desarrollo evolutivo de la tecnología, desde luego previa una concientización a nuestra sociedad.

5.- ¿De qué modo la falta de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos afecta a la intimidad?

La mayoría de los entrevistados manifiesta, que al no existir una norma que sancione evoluciona de manera impresionante la vulnerabilidad de los diferentes mecanismos tecnológicos, se establece el escenario ideal para que la inseguridad desarrolle todo su potencial.

Conclusión

Es una labor que demanda más que un control de los dispositivos de acceso a los medios de comunicación, sino adelantar una gestión de seguridad de la información, que exige regular el uso de los mismos, adaptarse a las condiciones cambiantes de la sociedad y el avance tecnológico, los negocios y las distintas organizaciones, y aprender de la inseguridad que es propia al proceso de creación, uso, registro, transporte, recuperación y disposición de la información., quedando clara la necesidad de crear un organismo de control y a la brevedad posible de reformar nuestra legislación penal.

6.- ¿Qué cambios propondría para remediar esta situación?

Los entrevistados responden a esta interrogante, en el sentido de que se

efectué un estudio o investigación social previa para establecer la verdadera situación y difundir el cómo se da el cometimiento de estos delitos a través del uso de nuevas tecnologías que los delincuentes usan. Además proponer reformas en lo referente a la inclusión completa de un capítulo a nuestra legislación penal acerca de los delitos informáticos que hoy en día son muchos.

Conclusión

De esta manera también se obliga a los desarrolladores de la tecnología a estar enterados de la normatividad, legislación y recomendaciones que tienen que ver con su buen uso. La colaboración entre especialistas de disciplinas tan distantes requiere de comprensión mutua y mucha paciencia. Los usuarios están expuestos a riesgos que casi todos desconocen, y su mejor defensa es el conocimiento de la tecnología que los pone en riesgo y de la normatividad que se puede aplicar.

7.- ¿Cómo el Estado cumple su función de protección hacia el derecho a la intimidad?

En relación a esta pregunta las personas entrevistadas expresan, que el Estado cumple su función de protección a través de la creación de normas, leyes a favor de la sociedad, que en ciertos casos resultan utópicas, de aplicación compleja en la práctica; esta función también es cumplida a través de los diferentes organismos como la Función Judicial, Fiscalía General del Estado y Policía Judicial.

Conclusión

Si bien el Estado cumple su función de protección esta no es cumplida a carta cabal, como debería ser y mucho más al no contar con una legislación penal acorde con los avances tecnológicos, se crean y expiden leyes, sin embargo, estas no responden a la realidad que vive la sociedad, son simplemente sanciones parche que tiende a mitigar el problema pero no a erradicarlo de raíz.

8.- ¿Cree Ud. que el derecho a la intimidad esté plenamente amparado por la ley?

Todos los entrevistados manifiestan, es de vital importancia que no se permita la vulnerabilidad de la intimidad y que este derecho esté plenamente amparado por la ley, pues, de esta forma se cuida la confidencialidad de la información de cada uno de nosotros, se busca una sanción que permita resarcir de alguna manera el daño causado, derechos que se encuentran estipulados en las normas ecuatorianas e internacionales para cumplir con el Plan Nacional de Desarrollo Integral para el Buen Vivir.

Conclusión

Resulta sumamente importante que la sociedad se encuentren plenamente amparada por la ley, partiendo del respeto a sus derechos y garantías establecidas en instrumento nacionales como internacionales, de alcanzarse el respeto pleno como seres humanos que somos, de ésta manera se formará una sociedad segura en la cual tengan la una verdadera seguridad jurídica de la información.

Una gravísima operación de espionaje estalló en los últimos días y con las horas parece ir creciendo.

Detalles de la vida privada, incluyendo fotos y otros datos, de un altísimo funcionario del Ejecutivo, un ministro, un integrante de la Corte Suprema, un ex gobernador, un intendente, un ex secretario de Estado y un colaborador de la Presidencia de la Nación fueron develados a través de correos electrónicos enviados desde direcciones que pertenecen a varios conocidos periodistas.

Es decir que a éstos les entraron a sus casillas de correo electrónico utilizando sus claves secretas y desde allí les mandaron los datos sobre la vida privada de los funcionarios a toda la libreta de direcciones de los periodistas.

Análisis e Interpretación de resultados de Encuestas

Una vez examinados los datos obtenidos a través de la encuesta planteada se hace necesario especificar y expresar los resultados del modo siguiente:

INTERROGANTES PLANTEADAS A LAS UNIDADES DE OBSERVACIÓN	ALTERNATIVAS					
	SI	**%**	**NO**	**%**	**Tot.**	**Tot. %**
1.- ¿Considera que la interceptación de comunicaciones y abuso de dispositivos vulneran los derechos fundamentales de las personas?	15	75	5	25	20	100
2.- ¿Cree que la interceptación de comunicaciones y abuso de dispositivos provoca la vulnerabilidad de la intimidad?	19	95	1	5	20	100
3.- ¿Comprobada la inexistencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos existe otras normas sancionadoras para este tipo de delitos?	3	15	17	85	20	100
4.- ¿Cree usted que el desconocimiento acerca de este tipo de delitos es una de las razones para que no se reconozca en nuestra legislación penal?	18	90	2	10	20	100
5.- ¿Cree usted que el Estado debe garantizar el derecho a la intimidad?	20	100	0	0	20	100

Cuadro Nº 05
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

6.- ¿Cree usted que la falta de control provoque la difamación, espionaje, violación de reservas industriales o comerciales, divulgación y empleo de documentos reservados, violación ilícita de comunicaciones; y, el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas?	14	70	6	30	20	100
7.- ¿Cree usted que mediante el aprovechamiento de nuevas tecnologías de comunicación y dispositivos vulneran directamente la intimidad?	16	80	4	20	20	100
8.- ¿Considera usted que al no contar con una normativa respecto a la interceptación de comunicaciones y abuso de dispositivos este tipos de delitos queden en la impunidad?	18	90	2	10	20	100
9.- ¿Cree usted que el acceso no controlado a nuevas tecnologías de información y comunicación vulneran la intimidad?	17	85	3	15	20	100
10.- ¿Considera usted oportuno que se reforme el Código Penal vigente para que se reconozca la interceptación de comunicaciones y abuso de dispositivos que atentan la intimidad?	20	100	0	0	20	100

Cuadro Nº 06
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

1.- ¿Considera que la interceptación de comunicaciones y abuso de dispositivos vulneran los derechos fundamentales de las personas?

Cuadro Nº 07

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	15	75%
No	5	25%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

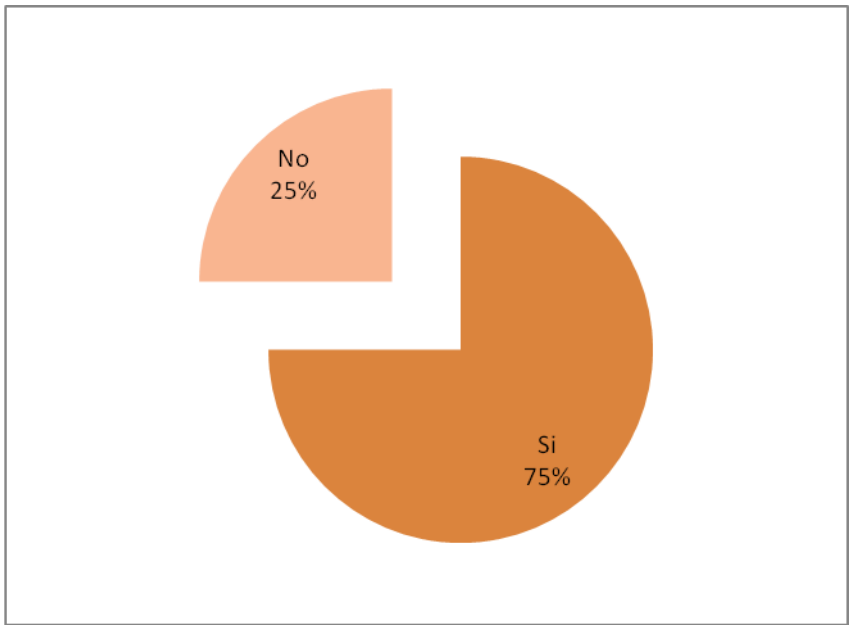

Gráfico Nº 05
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

Un 75% de los encuestados contestan que si se vulnera los derechos fundamentales de las personas, mientras que el 25% responden que no atentan contra los derechos fundamentales de las personas.

Es importante que en nuestro país se proteja un derecho tan elemental como es la intimidad ya que hoy en día el avance tecnológico abre muchas brechas para que se filtre información y sean objeto de injerencias arbitrarias en la vida privada, familia, correspondencia y atentados directos contra la honra, reputación de las personas como se manifiesta en la declaración fundamental de los Derechos humanos en su Art. 12 adoptada por la Asamblea General de las Naciones Unidas el 10 de diciembre de 1948.

Un derecho fundamental jurídicamente tiene la estructura normativa de un derecho subjetivo, es decir, que los derechos fundamentales son instituciones jurídicas que tienen la forma del derecho subjetivo.

Se considera además un conjunto de derechos subjetivos y garantías reconocidos en la Constitución como propios de las personas y que tienen como finalidad prioritaria garantizar la dignidad de la persona, la libertad, la igualdad, la participación política y social, el pluralismo o cualquier otro aspecto fundamental que afecte al desarrollo integral de la persona en una comunidad de hombres libres.

Tales derechos no sólo vinculan a los poderes públicos que deben respetarlos y garantizar su ejercicio estando su quebrantamiento protegido jurisdiccionalmente, sino que también constituyen el fundamento sustantivo del orden político y jurídico de la comunidad.

2.- ¿Cree que la interceptación de comunicaciones y abuso de dispositivos provoca la vulnerabilidad de la intimidad?

Cuadro Nº 08

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	19	95%
No	1	5%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

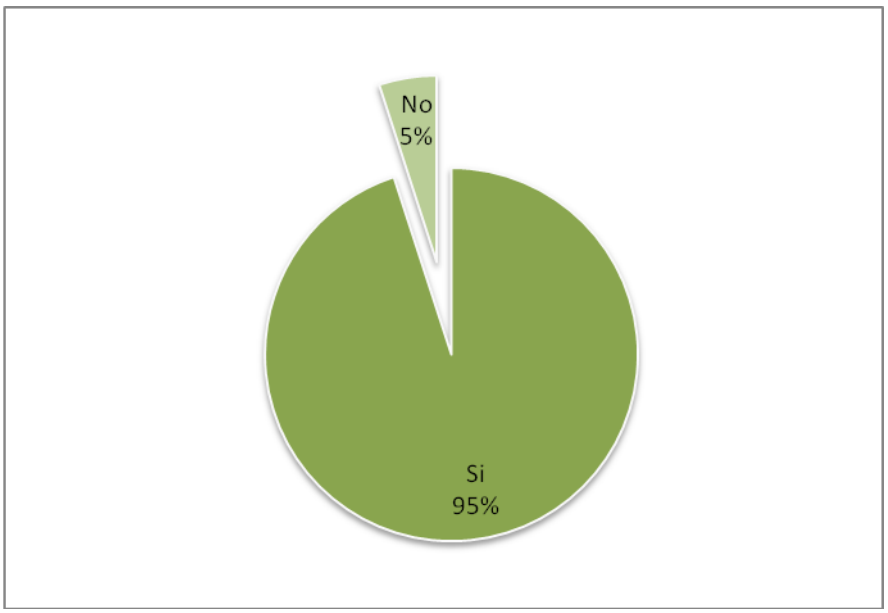

Gráfico Nº 06
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

El 95% de los encuestados contestan que la interceptación de comunicaciones y abuso de dispositivos si provoca la vulnerabilidad de la intimidad, mientras que un 5% contestan que la interceptación de comunicaciones y abuso de dispositivos no provoca la vulnerabilidad de la intimidad.

Es alarmante la cifra de inseguridad que cada día surge a través de la tecnología y nuestro país debería incentivar una verdadera concientización del riesgo que cada uno de nosotros corremos al ser vulnerados nuestra intimidad.

Numerosas reflexiones aparecen en la doctrina sobre la necesidad de modificar los esquemas jurídicos con la intención de dar protección legal a los derechos que puedan ser dañados a partir de los nuevos inventos de reproducción de la imagen y la voz; y, la creciente posibilidad de comunicación de los mismos.

Comienza así la necesidad de protección de los datos que revelen la personalidad de un individuo.

La controversia jurídica nace precisamente, del deseo de reforzar las garantías que los derechos del hombre conceden a la persona y a su vida privada. Poder y libertad no deben estar en lucha, al constituir la base y existencia para el hombre y su libertad. Sin duda, uno de los bienes jurídicos más susceptibles de ser lesionado o puesto en peligro por el uso de las nuevas tecnologías es la intimidad.

La violación del derecho a la intimidad es un delito que consiste en el apoderamiento de papeles, cartas, mensajes de correo electrónico o cualquier otro documento o efectos personales, interceptación de telecomunicaciones, utilización de artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o imagen, o de cualquier otra señal de comunicación, con intención de descubrir secretos o vulnerar su intimidad, sin que medie en consentimiento del afectado. Es un delito reconocido por la ONU.

3.- ¿Comprobada la inexistencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos existe otras normas sancionadoras para este tipo de delitos?

Cuadro Nº 09

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	3	15%
No	17	85%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

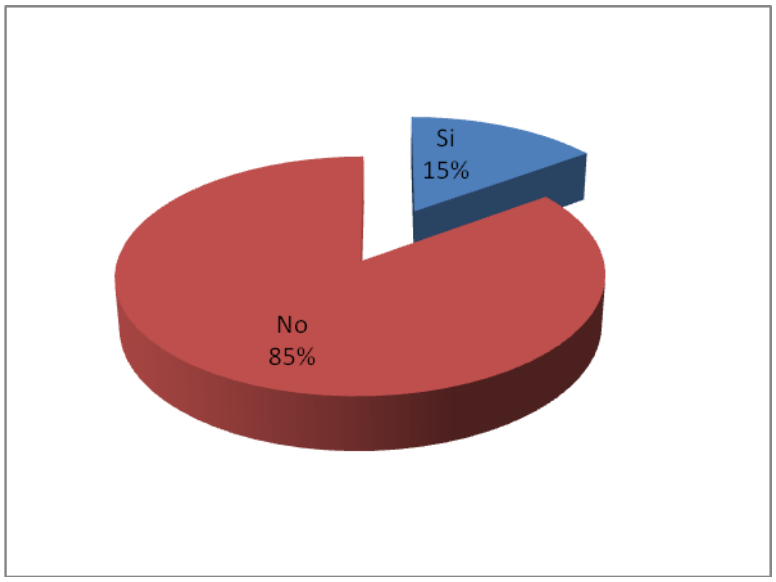

Gráfico Nº 07
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

El 85% de los encuestados manifiesta que, no existe otras normas sancionadoras para este tipo de delitos; el 15% responden que si existe normas que sancionen este tipo de delitos.

En la actualidad que vivimos en nuestro país no existe una verdadera tipificación para que estas conductas delictivas sean sancionadas por múltiples factores muchos de ellos de índole socio cultura lo que a corto plazo desencadena conflictos en los cuales se ven involucrados sectores de la sociedad al no existir una normativa que corrija estas conductas punitivas incluso al sector público y el más perjudicado el sector privado por la manipulación y alteración de información diaria y siempre que estos se vean amenazados, transgredidos o desconocidos en el procesamiento, almacenamiento, registro, utilización o uso o en la tele transmisión de datos de carácter personal y se realicen por medios informáticos, telemáticos o electrónicos.

El derecho a la intimidad personal se entiende como aquella facultad que tenemos las personas de poseer un espacio de nuestra existencia para la soledad y quietud, de ese modo desarrollar nuestra personalidad sin la interferencia de terceros.

Mientras que intimidad familiar se entiende como aquel derecho que posee todo grupo de personas que conforman una familia de tener una esfera o ámbito privado para desarrollar sus relaciones familiares sin la intervención de terceros ajenos a la familia.

Nadie tiene derecho a saber los internos de una familia si uno o varios de sus integrantes no lo revelan. Sin duda, toda persona que trabaja para otra, tiene la obligación de guardar los aspectos o situaciones íntimas de aquellas o su familia, que ha conocido por efectos propios del desempeño de sus labores.

4.- ¿Cree usted que el desconocimiento acerca de este tipo de delitos es una de las razones para que no se reconozca en nuestra legislación penal?

Cuadro Nº 10

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	18	90%
No	2	10%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

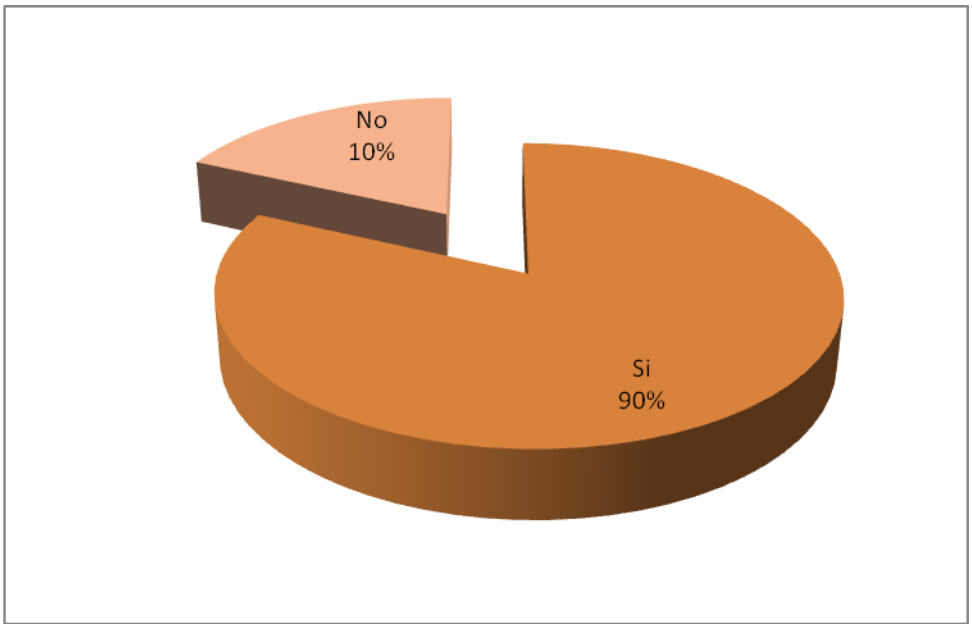

Gráfico Nº 08
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

Un 90% de lo encuestados responden que, el desconocimiento de este tipo de delitos no se ha propuesto varias reformas al Código Penal ecuatoriano vigente; el 10% responde que no es una razón para que no se legisle este tipo de delitos en nuestra legislación penal vigente.

Muchas veces por el desconocimiento de los serios problemas que implica la interceptación de comunicaciones y abuso de dispositivos lesiona gravemente la intimidad de las personas situación en la que está inmerso nuestro país y se necesita urgentemente que se tome medidas para controlar y mejorar la cultura tecnológica que vive el mundo entero.

La información que puede ser esta relacionada con:

- La raza, origen nacional o étnico, color, religión, edad o estado civil de la persona.
- Información relacionada con la educación, historial médico, delictivo, laboral de la persona, o información relacionada a las transacciones financieras en las que el individuo ha estado involucrado.
- Cualquier número o símbolo que identifique o se le asigne a una persona.
- Dirección, huellas digitales o tipo sanguíneo de la persona.
- Opiniones o ideas personales, excepto aquellas vertidas sobre otra persona, o sobre una propuesta de subvención, recompensa o un premio otorgado por una institución gubernamental, sección, departamento o Ministerio, según lo estipulen sus reglamentos.
- Correspondencia enviada a una institución gubernamental por una persona que es implícita o explícitamente de naturaleza privada o confidencial, así como las contestaciones a la misma en la medida que revelen un contenido que corresponda a la envida originalmente.
- Ideas u opiniones de otra persona sobre él.
- Ideas u opiniones de otra persona sobre una propuesta de subvención, recompensa o premio otorgado por una institución gubernamental,

sección, departamento o Ministerio, según lo estipulen sus reglamentos y referida en el parágrafo (e), pero excluyendo el nombre de la otra persona sobre la cual dedicó sus ideas u opiniones.

- Nombre de la persona que aparece relacionada con otra información personal y que él sólo descubrimiento del verdadero nombre revelaría información sobre aquél.
- La información de una persona que es o fue funcionario, empleado de una institución gubernamental y relacionada con la posición o funciones del mismo. Esta información incluye: 1. el hecho de que el individuo es o era funcionario o empleado de la institución gubernamental; 2. el título, dirección comercial y número del teléfono de la persona; 3. la clasificación, rango y monto del sueldo y atribuciones según su cargo; 4. el nombre de la persona que figura en un documento preparado por éste en el ejercicio de su empleo; y, 5. las ideas u opiniones personales expresadas en el curso de su empleo.
- Información sobre una persona que desempeña o desempeñó los servicios bajo contrato con una institución gubernamental. Esta información incluye: los términos del contrato, el nombre del individuo y las opiniones o ideas expresadas en el transcurso del mismo.
- Información relacionada con cualquier beneficio discrecional de naturaleza financiera, incluida la concesión de una licencia o permiso, así como nominación del mismo, el nombre de quien la confirió y la naturaleza precisa de la misma.

Su protección se basa en el no descubrimiento o divulgación de datos personales cuando no media consentimiento de la persona pero consagra una excepción para identificar la información y es cuando haya de por medio un procedimiento administrativo y sumario en las situaciones mencionadas anteriormente.

5.- ¿Cree usted que el Estado debe garantizar el derecho a la intimidad?

Cuadro Nº 11

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	20	100%
No	0	0%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

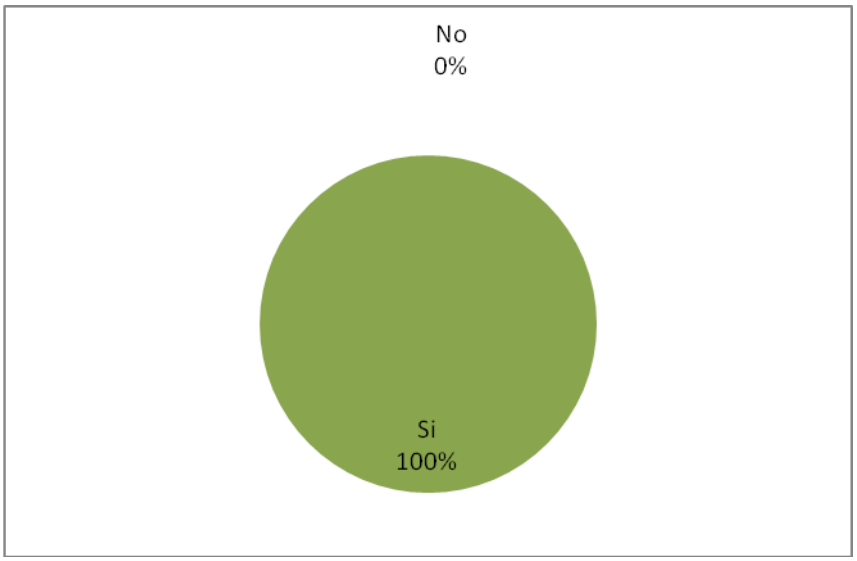

Gráfico Nº 09
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

El 100% de los encuestados responde que el Estado debe garantizar nuestro derecho que se encuentra reconocido en nuestra Constitución de la República del Ecuador a través de los diferentes entes del Estado.

Al no tener una verdadera regulación en nuestra legislación penal el Estado a través de los diferentes entes de justicia debería garantizar nuestro derecho a la intimidad para que no seamos víctimas de la delincuencia organizada que cada día aflora más y más.

La que más repercusión social ha tenido debido a la gran notoriedad que se le ha dado en distintos medios de comunicación escrita y oral; circunstancia que puede haber causado un mayor perjuicio al trabajador despedido, en cuanto a la violación del derecho a la intimidad que el hecho mismo del control empresarial efectuado en el correo electrónico, toda vez que por dichos conductos informativos se ha divulgado el nombre, la filiación sindical, la relación con compañeros de trabajo, su conducta laboral, etc., que son reveladores, en cierta medida de su intimidad por ende la falta de control inmediato de seguridad al momento de difundir nuestra información personal por internet o por cualquier medio de comunicación.

En consecuencia la falta de protección penal al derecho a la intimidad, se justifica hasta por dos circunstancias concretas: primero, porque se pretende evitar intromisiones de terceros en ciertos hechos y conductas que de ser conocidas y reveladas alteran la tranquilidad de la persona agraviada, en razón de encontrarse trabados con lo más recóndito de su ser; y segundo, porque los ataques contra la intimidad de una persona son altamente perjudiciales e intolerables para el que las sufre y a veces para la sociedad misma.

6.- ¿Cree usted que la falta de control provoque la difamación, espionaje, violación de reservas industriales o comerciales, divulgación y empleo de documentos reservados, violación ilícita de comunicaciones; y, el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas?

Cuadro Nº 12

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	14	70%
No	6	30%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

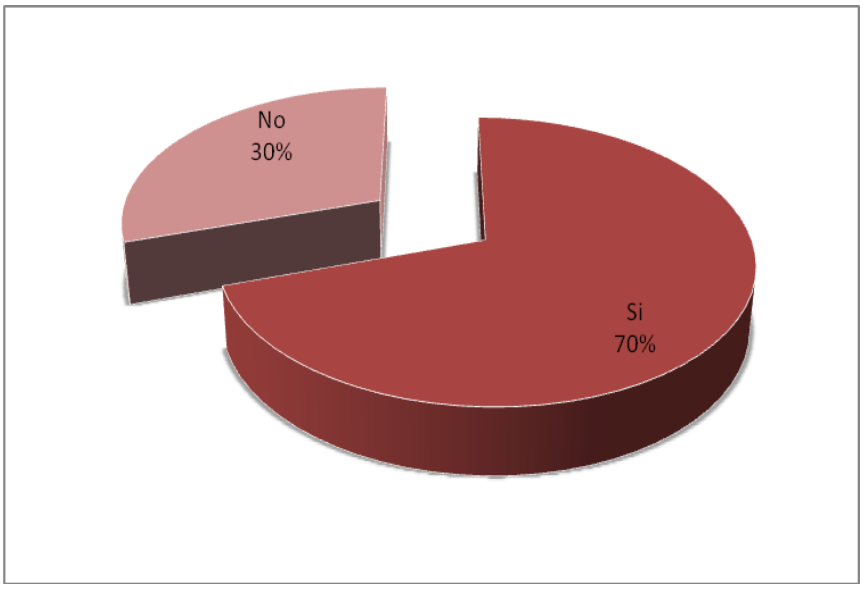

Gráfico Nº 10
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

El 70% de los encuestados responden que la falta de control provoca la difamación, espionaje, violación de reservas industriales o comerciales, divulgación y empleo de documentos reservados, violación ilícita de comunicaciones; y, el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas; mientras que el 30% responde la falta de control no provoca la interceptación de comunicaciones privadas.

La falta de control en nuestras comunicaciones provoca la divulgación, mal utilización de información, espionaje, violación de reservas industriales o comerciales que atentan directamente la intimidad de las personas provocando así graves `perdidas económicas y resultado de esto atentando directamente a la dignidad y moral de la sociedad en general.

Ahora bien, desde un punto de vista estrictamente técnico, el empresario, el empleado, los usuarios tienen la posibilidad de controlar y archivar todo el correo electrónico que circula por la red de comunicación de su empresa. Ello podría configurarse como una medida más de vigilancia y supervisión de los trabajadores que ofrecen las nuevas tecnologías, junto a otras como el control de la navegación por internet, el control de las llamadas telefónicas, la instalación de cámaras, el control médico, etc.

Se suele alegar que la vigilancia de las comunicaciones en la empresa puede tener una finalidad legítima de control de la calidad del trabajo, posibilitando la corrección de errores en el sistema productivo, así como una medida de protección y vigilancia ante posibles actuaciones desleales del trabajador o visitantes, como un uso particular de los elementos de la empresa, defraudaciones, introducción de virus, espionaje industrial e incluso, el acoso sexual.

7.- ¿Cree usted que mediante el aprovechamiento de nuevas tecnologías de comunicación y dispositivos vulneran directamente la intimidad?

Cuadro Nº 13

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	16	80%
No	4	20%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

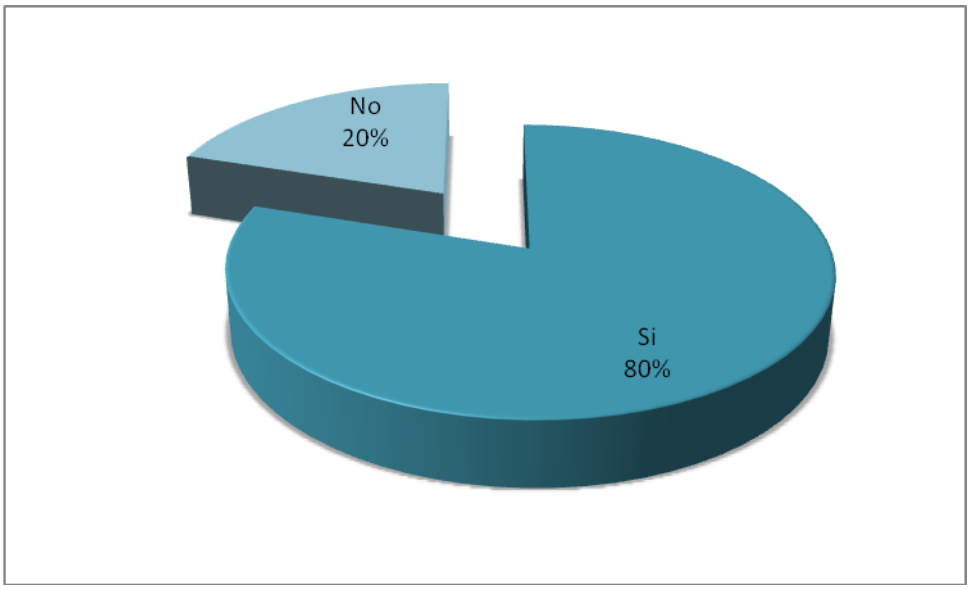

Gráfico Nº 11
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

De los encuestados el 80% afirman que, el aprovechamiento de nuevas tecnologías y dispositivos atentan directamente la intimidad de las personas mientras que el 20% afirman que no se atenta directamente la intimidad de las personas.

La información se ha convertido en el eje promotor de cambios sociales, económicos y culturales. El auge de las telecomunicaciones y sus dispositivos mejorados ha producido una transformación de las tecnologías de la información y de la comunicación, cuyo impacto ha afectado a todos los sectores de la economía y de la sociedad.

La expansión de redes informáticas y las comunicaciones ha hecho posible la universalización de los intercambios y relaciones, al poner en comunicación a amplios sectores de ciudadanos residentes en espacios geográficos muy distantes entre sí.

Los espacios nacionales se han visto superados por las tecnologías de la información que no tienen fronteras: informaciones políticas, militares, económicas especialmente financieras, sociales, empresariales, etc. se intercambian y se transmiten cada día por todo el mundo, de manera que nuestra vida está condicionada en cada momento por lo que está sucediendo a miles de kilómetros de distancia.

Cualquier acontecimiento político o económico ocurrido en un país puede tener una repercusión importante en la actividad económica de otras naciones. La subida de los tipos de interés en Estados Unidos, por ejemplo, afecta al precio del dinero en Europa y, consiguientemente, a la liquidez monetaria de los ciudadanos, y por tanto, a sus posibilidades de consumo y bienestar.

8.- ¿Considera usted que al no contar con una normativa respecto a la interceptación de comunicaciones y abuso de dispositivos este tipo de delitos queden en la impunidad?

Cuadro Nº 14

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	18	90%
No	2	10%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

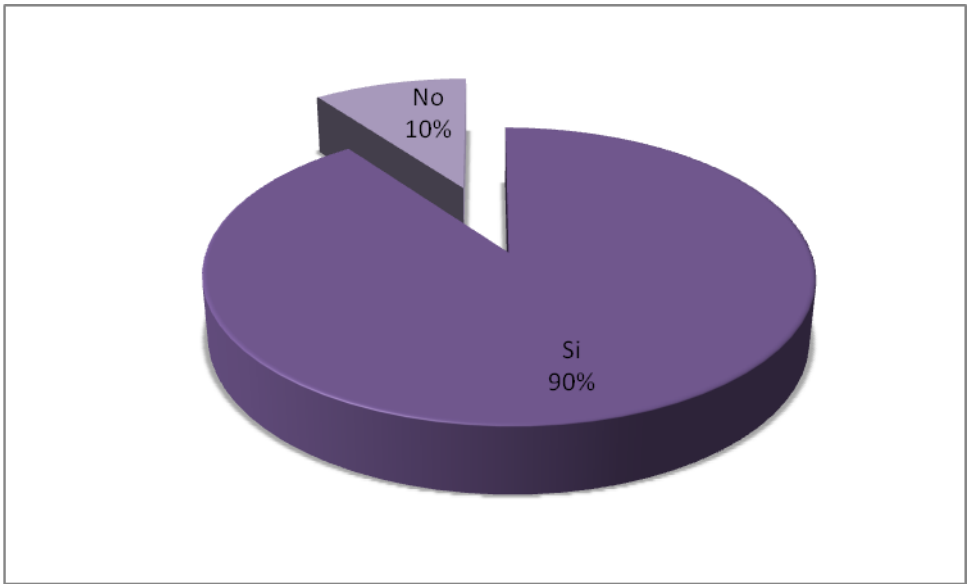

Gráfico Nº 12
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

De los encuestados el 90% aseveran que la falta de normativa provoca que no sean sancionadas las personas que comenten este tipo de delitos; mientras que el 10% niegan que la falta de normativa no se de una sanción correlativa al cometimiento de este tipo de delitos.

Si bien, cabe destacar que no existe un apartado específico donde se incluyan los denominados delitos informáticos e incluso no todos se encuentran debidamente especificados, entre los que cabe destacar la apología a la interceptación de comunicaciones y abuso de dispositivos.

Se puede entenderse como delito informático por tanto en cuanto tiene cabida en la acepción amplia de delito informático que tienen en los datos o sistemas informáticos el objeto o el instrumento de su delito atentan directamente a la intimidad de las personas.

Los delitos que atentan directamente a la intimidad, es el derecho a la propia imagen y la inviolabilidad de domicilio.

El descubrimiento y revelación de secretos, la interceptación de comunicaciones, siempre que no exista consentimiento y haya intención de desvelar secretos o vulnerar la intimidad de un tercero.

También sería un delito contra la intimidad, la usurpación y cesión de datos reservados de carácter personal. Siendo de vital importancia que se regule para proteger estos bines jurídicos.

Los medios de ejecución del comportamiento típico podrán ser instrumentos, procesos técnicos u otros. Al final se deja una cláusula abierta, donde tendría cabida el avance de las nuevas tecnologías, sobre todo de la informática.

9.- ¿Cree usted que el acceso no controlado a nuevas tecnologías de información y comunicación vulneran la intimidad?

Cuadro Nº 15

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	17	85%
No	3	15%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

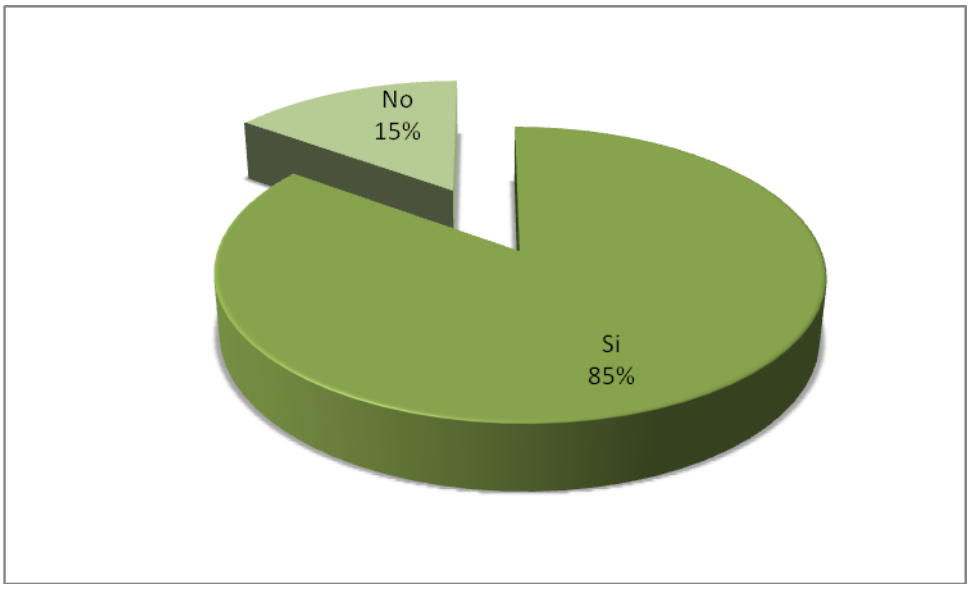

Gráfico Nº 13
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

Un 85% de los encuestados responden que si, por cuanto si no se cuenta con un verdadera control a las nuevas tecnologías vulneran la intimidad con mayor facilidad; un 15% que dice que no vulnera la intimidad el acceso no controlado a nuevas tecnologías de información y comunicación.

La información ha contribuido a que los acontecimientos que se suceden a escala mundial, continental o nacional nos resulten más cercanos, y que la idea de la "aldea global "de MacLuhan se vaya haciendo realidad. Nuestra visión del mundo está adquiriendo una nueva dimensión por encima de países, comunidades y localidades, lo mismo que le sucede a las empresas. Estamos ante un nuevo modelo social, la "sociedad globalizada", en el que las fronteras desaparecen en beneficio de los intercambios de ideas, mensajes, productos, servicios, persona, etc.

El espectacular desarrollo científico y tecnológico han abierto las puertas a nuevas posibilidades de delincuencia antes impensables. De esta manera se demuestra que la falta de cultura tecnológica en nuestro país es mayor. Sin embargo, como cualquier tecnología, se debe tener presente que son solamente un instrumento (eso sí, muy potente y flexible) para la gestión de las empresas. Por tanto, es evidente que las nuevas tecnologías son un elemento imprescindible y en continuo desarrollo dentro de cualquier empresa.

No obstante las tecnologías están mucho más presentes en las grandes empresas que en las medianas y pequeñas (PYME); esto se debe principalmente a la dimensión de la empresa y, como consecuencia, al ámbito de actuación de la misma y a su capacidad de inversión y gestión, aunque poco a poco esta diferencia se va acortando, ya que muchas PYME están empezando a ser conscientes de que es una cuestión clave para su expansión y supervivencia.

10.- ¿Considera usted oportuno que se reforme el Código Penal vigente para que se reconozca la interceptación de comunicaciones y abuso de dispositivos que atentan la intimidad?

Cuadro Nº 16

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
Si	20	100%
No	0	0%
Total	20	100%

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

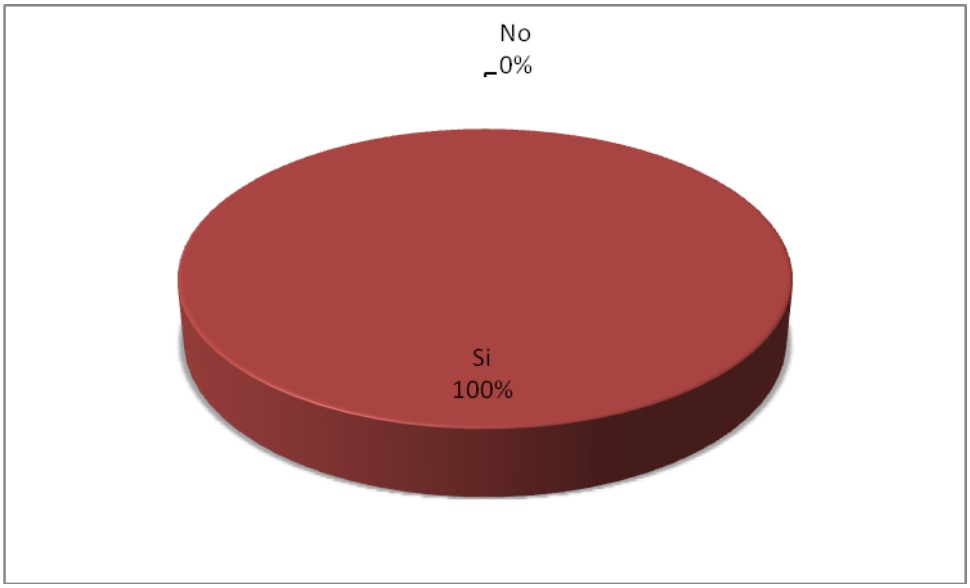

Gráfico Nº 14
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Análisis e Interpretación

Respuesta concluyente en este aspecto, cuando se reconoce en un 100% de los encuestados, su manifestación al estar de acuerdo con la creación de un proyecto de reforma a nuestra legislación Penal vigente reforma que sancionara este tipo de delitos y no se queden en la impunidad.

La creación del proyecto de reforma permitirá garantizar el bienestar social y económico de la sociedad en general cuidando y garantizando de esta manera el derecho a la intimidad consagrada en nuestra Constitución de la República del Ecuador y demás normas internacionales.

Para concluir con esta aproximación a un tema de gran interés y de preocupación, se puede señalar que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, dispositivos es conveniente establecer tratados de extradición o acuerdos de ayuda mutua entre los países, que permitan fijar mecanismos sincronizados para la puesta en vigor de instrumentos de cooperación internacional y así contrarrestar eficazmente la incidencia de la criminalidad informática.

La razón de aquella protección radica en la libertad del hombre, que se vería seriamente afectada por la invasión de su intimidad, violentando su propia conducta. Es natural la postura de ocultamiento de nuestras propias debilidades y de aquellos aspectos de nuestra personalidad que consideramos desagradables o que, en todo caso, queremos mantener bajo nuestro exclusivo dominio.

Al perder el control sobre estos datos íntimos se produciría ineludiblemente un cambio en nuestra actitud por la coacción de hechos revelados, atentando contra nuestra libertad constituyéndose así en una necesidad urgente que se reconozca en nuestro Código Penal vigente.

Cálculo de Chi Cuadrado

Enunciado.- La ausencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos provoca la vulnerabilidad de la intimidad en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado del cantón Quito durante el período 2009.

Ho= La ausencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos **no** provoca la vulnerabilidad de la intimidad en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado del cantón Quito durante el período 2009.

Hi = La ausencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos **si** provoca la vulnerabilidad de la intimidad en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado del cantón Quito durante el período 2009.

Para comprobar la hipótesis utilizaremos un nivel de aceptación que es igual 0,01 (99%) o igual 0.05 para la verificación de nuestra hipótesis vamos a utilizar la prueba del Chi Cuadrado.

Frecuencias Observadas

Cuadro Nº 17

ALTERNATIVAS	CATEGORIAS		
	SI	**NO**	**TOTAL**
¿Considera que la interceptación de comunicaciones y abuso de dispositivos vulneran los derechos fundamentales de las personas?	15	5	20
¿Comprobada la inexistencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos existe otras normas sancionadoras para este tipo de delitos?	3	17	20
¿Cree usted que el acceso no controlado a nuevas tecnologías de información y comunicación vulneran la intimidad?	17	3	20
¿Considera usted oportuno que se reforme el Código Penal vigente para que se reconozca la interceptación de comunicaciones y abuso de dispositivos que atentan la intimidad?	20	0	20
TOTAL	55	25	80

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Frecuencias Esperadas

Cuadro Nº 18

ALTERNATIVAS	CATEGORIAS		
	SI	NO	TOTAL
¿Considera que la interceptación de comunicaciones y abuso de dispositivos vulneran los derechos fundamentales de las personas?	13.75	6.25	20
¿Comprobada la inexistencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos existe otras normas sancionadoras para este tipo de delitos?	13.75	6.25	20
¿Cree usted que el acceso no controlado a nuevas tecnologías de información y comunicación vulneran la intimidad?	13.75	6.25	20
¿Considera usted oportuno que se reforme el Código Penal vigente para que se reconozca la interceptación de comunicaciones y abuso de dispositivos que atentan la intimidad?	13.75	6.25	20
TOTAL	55	25	80

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Cuadro Nº 19

O	E	O-E	(O-E)2	(O-E)2 / E
15	13.75	1.25	1.56	0.11
5	6.25	-1.25	1.56	0.24
3	13.75	-10.75	115.5	8.4
17	6.25	10.75	115.5	18.48
17	13.75	3.25	10.5	0.76
3	6.25	-3.25	10.5	1.68
20	13.75	6.25	39	2.83
0	6.25	- 6.25	39	6.24
80	80	0	333	38.74

Fuente: Investigador
Elaboración: César E. Naranjo Mesías

38.74% tope máximo de la campana de Gauss

gl = (grados de libertad)

gl =(fr - 1) (c - 1)

gl =(4 - 1) (2 - 1)

gl = (3) (1)

gl = 3

Grado de libertad **3** que corresponde al nivel de aceptación 0.01 corresponde al 99% de aceptación es de 8. 4

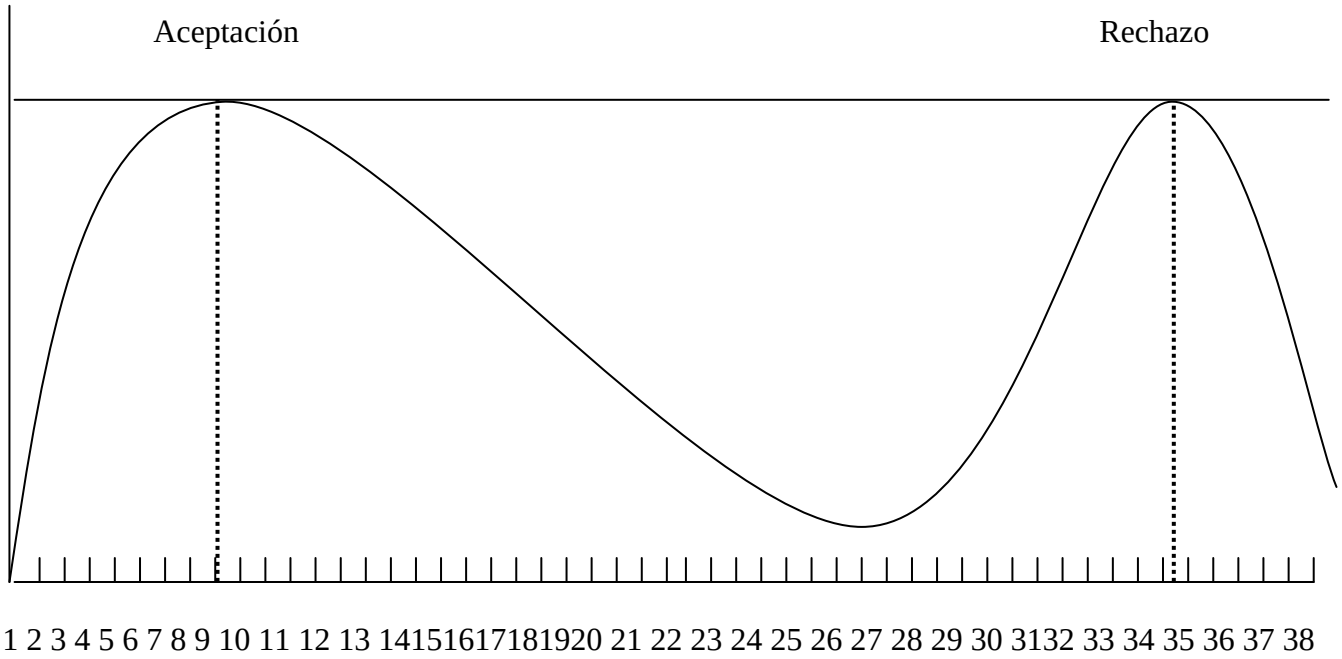

Gráfico Nº 15
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

De acuerdo al gráfico observado y de acuerdo a las regiones planteadas el ultimo valor X calculado es mayor que X tabulado se rechaza el **Ho** y se acepta el **Hi** que dice "La ausencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos **si** provoca vulnerabilidad de la intimidad en el Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado del cantón Quito durante el período 2009".

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Para la labor de prevención de estos delitos es importante el aporte de los damnificados que puede ayudar en la determinación del modus operandi, esto es de las maniobras usadas por los delincuentes informáticos.

Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción acerca de la interceptación de comunicaciones y abuso de dispositivos que generan nuevas formas de delitos informáticos.

Sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesionales dedicados a su investigación.

Luego de analizar la realidad de la interceptación de comunicaciones en el Ecuador y exponer sus mecanismos y herramientas existentes para su investigación, se recomienda considerar por sectores: Gubernamental, Marco Legal, Formación, Tecnología y Sociedad; los siguientes aspectos:

Gubernamental

1. Establecer y alinear una política de lucha en contra el cibercrimen.
2. Incentivar mecanismos de cooperación con otros países con el objetivo de prevenir y sancionar la interceptación de comunicaciones y abuso de dispositivos que traspasa las fronteras de las naciones.

Marco Legal

1. Proyecto de inclusión de los artículos innumerados 202.3 y 202.4 al art. 202 del código penal ecuatoriano acerca de la interceptación de comunicaciones y abuso de dispositivos.
2. Revisión de la Ley de Comercio Electrónico, Mensajes de Datos y Firma Digital.
3. Reformas al Código de Procedimiento Penal del Ecuador sobre penalizaciones a las infracciones acerca de las comunicaciones y dispositivos informáticos.
4. Establecer mecanismos de protección penal respecto de la delincuencia referente a los diferentes tipos de comunicaciones.
5. Implementación de mecanismos de mayor rigurosidad en los procedimientos de acreditación de peritos informáticos, en la que los profesionales acrediten además de sus conocimientos técnicos, procedimientos de manejo de evidencias, criminalística, e incluso respaldar sus conocimientos con certificaciones.
6. Convenios o suscripción de tratados internacionales.
7. Desarrollo de proyectos que permitan llevar a cabo las recomendaciones del Grupo de Expertos Gubernamentales – Delitos Cibernéticos de la OEA.

Formación

1. Desarrollo de programas de capacitación al órgano legal (Fiscales, Jueces, Policía Judicial, Abogados) sobre la interceptación de comunicaciones y abuso de dispositivos, delitos informáticos e informática legal.
2. Capacitación a los profesionales de tecnología en aspectos básicos de informática legal, forense, criminalística, manejo de evidencias digitales, etc.
3. Fomentar el desarrollo de programas que involucren la disertación del peritaje informático, legislación existente que atañen a la informática, criminalística.

4. Desarrollo de programas de especialización que contemplen profesionales en informática forense y/o legal que pueden darse en cooperación con organismos especializados o entre convenios universitarios.

Tecnología

1. Convenios institucionales (universidades, gremios, etc.)
2. Cooperación y transferencia de conocimiento con países vecinos, o con quienes se hayan establecido convenios internacionales, sobre la tecnología existente o el desarrollo de las mismas que permitan la persecución de los delitos informáticos.
3. Implementación de laboratorios especializados forenses informáticos.

Sociedad

1. Advertir a los usuarios sobre las posibilidades u probabilidad de ocurrencia de delitos informáticos
2. Difusión de medidas de salvaguarda tal como el cierre de brechas de seguridad, como medidas de prevención ciudadana ante delitos de índole tecnológico.
3. Concientización en las organizaciones de que las medidas de seguridad más que un gasto son una inversión que proveen mecanismo para evitar este tipo de delitos.
4. Concientización del efecto e impacto de la interceptación de comunicaciones y abuso de dispositivos sobre la sociedad.

Es indudable que los países latinoamericanos están tomando iniciativas que les permite desarrollar estrategias para el seguimiento de los delitos informáticos, hemos visto como Argentina y Colombia han elaborado y aprobado las respectivas regulaciones que protegen el bien jurídico: la información, entonces, Ecuador que cuenta ya con el entidad de certificación de las firmas electrónicas, la Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos e iniciativas que permiten el seguimiento de ciertos aspectos tecnológicos debiendo

embarcarse en un proyecto que permita delinear aspectos regulatorios sobre las tecnologías de la información.

Sin duda alguna, el avance tecnológico y la necesidad de establecer mecanismos que permitan la persecución de actos ilícitos cometidos utilizando medios tecnológicos generará una nueva generación de profesionales que darán respuesta a la creciente necesidad de la sociedad de contar con asesores entendidos, y capaces de brindar sustento y respaldo legal a cada una de las actividades que se desarrollan con soporte de las tecnologías de la información.

El aporte de los damnificados que puede ayudar en la determinación del modus operandi, esto es de las maniobras usadas por los delincuentes informáticos.

RECOMENDACIONES

1. La mejor forma de evitar situaciones engorrosas de fraudes, robo interceptación de comunicaciones, abuso de dispositivos y siniestros informáticos es estableciendo controles, pero por sobre todo, promover una cultura de seguridad e inviolabilidad de la intimidad en las organizaciones y sociedad en general.

2. Se deben desarrollar prácticas, procedimientos de programación y control que busquen disminuir los problemas de seguridad en los productos de software y hardware, dispositivos de comunicación, etc.

3. Previsibilidad, debido cuidado y diligencia son palabras claves de control en el entorno institucional público o privado, personal o la sociedad.

4. Definir prácticas y políticas de seguridad en comunicaciones, como pruebas preconstituidas para la organización.

5. Una de las normas legales es garantizar la confiabilidad de la información y por consiguiente los resultados obtenidos, debe ser una meta de los Jefes

departamentales.

6. Adecuar a la empresa con seguridades físicas y lógicas básicas.

7. Revisiones periódicas constituyen una buena práctica de control interno y deben aplicarse en las organizaciones incluso para el entorno informático.

8. Capacitar continuamente al personal de investigaciones del Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado y Policía Judicial Departamento de Criminalística a nivel nacional para fomentar y mejorar la cultura organizativa con el propósito de establecer objetivos de control para que a su vez esto contribuya a la obtención y cumplimiento de metas y objetivos institucionales.

9. Fomentar al personal la importancia de poseer y trabajar con información efectiva, oportuna y verdadera para adecuadas y acertadas toma de decisiones.

10. Los cambios tecnológicos y procesos globalizados demandan mayor rapidez, eficacia, efectividad y un mayor control, por lo cual los profesores y estudiantes vinculados a la investigación, así como los directivos de las instituciones educativas deben profundizar en estos temas de actualidad.

11. Difundir el uso de las herramientas, técnicas y mecanismos necesarios para evitar los posibles fraudes, robos y siniestros que se pueden cometer dentro de un sistema de información.

12. Concientizar sobre las responsabilidades jurídicas de estas situaciones a los colaboradores de la empresa.

13. Implantar Mecanismos de Seguridad como:
    a. Firmas digitales
    b. Certificados digitales

c. Algoritmos de encripción simétrica y asimétrica
d. Control de integridad de archivos
e. Aplicación de auditorías

14. Establecer enfoques de Seguridad de Comunicaciones de acuerdo a los aspectos legales del país incluyendo:

    a. Principios
        i. Confidencialidad
        ii. Integridad
        iii. Disponibilidad
    b. Servicios
        i. Autenticación
        ii. Autorización
        iii. No-repudiación
        iv. Auditabilidad

15. Ante los continuos cambios tecnológicos se recomienda que el analista esté constantemente actualizándose en el uso de herramientas y técnicas hasta ganar la experiencia requerida para resolver casos con mayor facilidad.

CAPÍTULO VI

PROPUESTA

PROYECTO DE INCLUSIÓN DE LOS ARTÍCULOS INNUMERADOS 202.3 Y 202.4 AL ART. 202 DEL CÓDIGO PENAL ECUATORIANO ACERCA DE LA INTERCEPTACIÓN DE COMUNICACIONES Y ABUSO DE DISPOSITIVOS.

Datos Informativos

Institución: Fiscalía General del Estado.

Beneficiarios: Departamento de Investigación y Análisis Forense

Ubicación: República del Ecuador.

Tiempo estimado para la ejecución: 9 meses.

Equipo técnico responsable:

- Asambleístas,
- Abogados,
- Economistas,
- Representantes de sectores sociales,
- Secretarias,
- Investigador.

Costo: Mil Cuatrocientos dólares americanos.

Antecedentes de la Propuesta

Hablar de interceptación de comunicación y abuso de dispositivos es referirse a los medios empleados y su mal uso, está involucrado la sociedad en general, el sector privado y especialmente el sector público

Han existido muchos casos de espionaje, interceptación de comunicaciones que han sido utilizados con fines políticos o lucrativos pero de una u otra manera se necesita su pronta regulación para que los medios de comunicación sea su utilización muy bien canalizada para no entorpecer la veracidad de la información. Estas razones son más que suficientes para conformar personal especializado la cual es una realidad constatada que este tipo de amenazas podría convertirse en un problema de dimensiones desproporcionadas.

Si el legislador no establece pronto medidas que permitan mejorar el control indispensable por parte de las autoridades correspondientes y que como consecuencia el no control de la comunicaciones y el uso indiscriminado de los dispositivos se la ve notoriamente agravada, pudiéndose incluso llegar a crear un riesgo en todos los ámbitos de la sociedad.

El retardo de una solución a lo que hoy es un problema grave, amenaza con incrementar el alto índice de interceptación de comunicaciones y el abuso de dispositivos de comunicación

Al no contar con personas especializadas tanto en el derecho informático como personas de la institución especializadas para realizar los distintos tipos de peritajes y reconocimientos que esta problemática conlleva provoca que el derecho a la intimidad sea vulnerada con mayor facilidad.

Justificación

Luego de haber realizado el trabajo investigativo y haber obtenido los

resultados es necesario la tipificación inmediata de la Interceptación de comunicaciones y abuso de dispositivos en nuestro Código Penal, protegerá de mejor manera a las personas que desconocen de este tipo de delitos que cada vez con el adelanto tecnológico operan con mayor facilidad pudiendo de ésta manera castigar sin tener que adoptar otras figuras jurídicas para sancionar este tipo de delitos.

La finalidad de esta propuesta es la de que se reconozca en nuestra legislación penal urgentemente, porque nuestra sociedad aun no tiene una verdadera cultura acerca del impresionante mundo tecnológico, y estamos expuesto al no tener reconocido este tipo de delitos que atentan no solamente la intimidad sino también la privacidad de la sociedad y sin la posibilidad de que la reclamación legal sea atendida oportunamente.

Actualmente, la sociedad ha sido espectadora de los avances tecnológicos que cotidianamente son empleados para efecto de investigación dentro de la averiguación previa, pues las herramientas de antaño ante el fortalecimiento de la delincuencia aparecen como ineficaces para un combate congruente, pues la delincuencia principalmente aquella que está organizada, acopia los instrumentos de mayor avance tecnológico existentes en el "mercado negro".

Aquellas herramientas con las que se lleva a cabo la investigación formal, son principalmente la intervención de comunicaciones, correos electrónicos, agente encubierto, de comunicaciones ambientales entre personas presentes y telecomunicaciones, que actualmente contempla la legislación penal ecuatoriana.

Requiere especial atención el hecho de que muchas de las comunicaciones son interceptadas ilegalmente mediante el empleo de dispositivos que atentan contra la intimidad se refleja los perjuicios que directa e indirectamente provoca este tipo de delitos violando de esta manera los derechos inculcados en nuestra Constitución Política del Estado y las diferentes tratados y convenios internacionales. Por otro lado, persiste la lentitud de la administración de justicia a la espera de eventuales reformas de las leyes de procedimiento que agilicen los

trámites de enjuiciamiento y ejecución correspondientes, lo que impide resolver y sancionar a las personas que cometen este tipo de delitos.

De ahí que sea necesario actualizar las instituciones jurídicas procesales que se emplean en la materia de interés, a efecto de auxiliar a los órganos encargados de la investigación. En el arduo compromiso de combate a la nueva criminalidad, que se ve favorecida por las barreras jurídicas del sistema de enjuiciamiento penal.

Por tal razón el Estado mediante esta propuesta requiere una actualización que no podemos pasar por alto ante la realidad que se vive no solo en nuestro Estado sino en el resto del país. Donde la delincuencia se muestra con avance y expansión en la utilización de medios sofisticados a modo de comunicación y demás herramientas que han sido incautadas por los órganos de investigación del país, lo que ha expuesto parte del poderío que detentan, al margen del Estado.

Esta propuesta tiene, por lo tanto, la finalidad de dar una respuesta desde el ámbito público y privado a la problemática planteada en numerosas grupos vulnerables e todos los sectores sociales, por parte de quien comete este tipo de delitos.

Objetivos

General

Identificar y sancionar a las personas que vulneran la intimidad mediante la interceptación de comunicaciones y abuso de dispositivos que causan graves perjuicios a la sociedad, el Estado y la familia.

Específicos

Dar cumplimiento al artículo 17 de la Constitución de la República del Ecuador, ponderando en cualquier caso la prevalencia del interés colectivo ya

sean estas naturales o jurídicas.

Garantizar el buen manejo de las comunicaciones y propender al correcto uso de los dispositivos mediante la aplicación de nuevos mecanismos de control acorde con el avance tecnológico que hoy en día se va presentando.

Garantizar que sólo al agraviado, ya sea en forma directa o por medio de representante legal que le sustituye, le está reservado acudir o recurrir ante la autoridad jurisdiccional y denunciar el hecho e iniciar un proceso en nuestro sistema jurídico.

Garantizar la difusión de estos nuevos delitos a toda la sociedad ecuatoriana.

Análisis de Factibilidad

A continuación se presenta una revisión de la factibilidad de reforma al Art. 202 del Código Penal Ecuatoriano, propuesto en relación con sus aspectos principales:

Factibilidad legal

Revisada la legislación y normatividad en particular la Constitucional vigente en el país esta posibilita:

Art. 61.- Las ecuatorianas y ecuatorianos gozan de los siguientes derechos:

3. Presentar proyectos de iniciativa popular normativa.

Art. 102.- Las ecuatorianas y ecuatorianos, incluidos aquellos domiciliados en el exterior, en forma individual o colectiva, podrán presentar sus propuestas y proyectos a todos los niveles de gobierno, a través de los mecanismos previstos en la Constitución y la ley.

Art. 134.- La iniciativa para presentar proyectos de ley corresponde:
5. A las ciudadanas y los ciudadanos que estén en goce de los derechos políticos y a las organizaciones sociales que cuenten con el respaldo de por lo menos el cero punto veinticinco por ciento de las ciudadanas y ciudadanos inscritos en el padrón electoral nacional.

Factibilidad política

En la Fiscalía General del Estado involucrado, se ha evidenciado interés en la por la creación de nueva figuras jurídicas como el propuesto, más aún cuando cobra mayor fuerza en el país el tema de los delitos informáticos y en especial de parte del Estado, la Sociedad y la Familia.

Este interés se evidencia en los compromisos de buscar las mejores articulaciones de operación de la Fiscalía General del Estado, Policía Judicial el Estado con las políticas respecto de proteger la intimidad de las personas y sociedad en general.

Fundamentación Científica Técnica

La propuesta planteada se la elaborado en base al enfoque Constructivista Social y Tecnológico, considerando que nada viene de nada, puesto, que todo conocimiento previo genera un conocimiento nuevo.

El conocimiento no solo se formar a partir de las relaciones ambiente - hombre, además es la suma del factor entorno social, es decir, se aprende con la ayuda de los demás, el origen de todo conocimiento es la sociedad, dentro de una cultura, dentro de una época histórica.

El individuo construye su conocimiento porque es capaz de leer, escribir y preguntar a quienes le rodena y de preguntarse a sí mismo sobre aquellos asuntos que le interesan.

Modelo Operativo de la Propuesta

Objetivo Específico.- Dar cumplimiento al artículo 17 de la Constitución de la República del Ecuador, ponderando en cualquier caso la prevalencia del interés de los demás.

Actividades	Contenidos	Recursos	Evaluación	Tiempo
Iniciativa.	Antecedentes. Importancia. Objetivos. Alcance del Proyecto. Organismos involucrados Beneficiarios.	Humanos: Ciudadanas/os, en goce de los derechos de intimidad. Materiales: Constitución de la República; Declaración de los Derechos Humanos, Convención de la Unión Europea acerca de delitos informáticos, Código Penal y Código de Procedimiento Penal	Asentimiento de la propuesta; impacto público o de ingresos que la medida pueda tener.	30 días.
Presentación del Proyecto.	Distribución del Proyecto por medio de la Secretaría General de la Asamblea a todos los Asambleístas.	Humanos: Personal de secretaría. Técnicos: Portal Web oficial de la Asamblea Nacional.	Difusión pública del extracto y remisión del Proyecto al Consejo de Administración Legislativa.	15 días.
Calificación del Proyecto.	Que se refiera a una sola materia; que contenga exposición de motivos y articulados, y; que cumpla los requisitos que establece la Constitución de la República.	Humanos: Miembros del Consejo de Administración Legislativa.	Prioridad para el tratamiento del Proyecto, por parte de la comisión especializada. Resolución.	60 días.
Tratamiento del Proyecto.	Conocimiento de todos los integrantes de la comisión, de la ciudadanía y de organizaciones registradas.	Técnicos: Portal Web oficial de la Asamblea Nacional.	Asentimiento de la propuesta. Impacto público	15 días.

Cuadro Nº 20
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Objetivo Específico.- Garantizar el buen manejo de las comunicaciones y propender al correcto uso de los dispositivos mediante la aplicación de nuevos mecanismos de control acorde con el avance tecnológico que hoy en día se va presentando.

Actividades	Contenidos	Recursos	Evaluación	Tiempo
Informe de la comisión especializada.	Presentación a la Presidenta/e de la Asamblea Nacional, el informe con las observaciones que sean necesarias introducir.	Humanos: Comisión de estudio correspondiente para el análisis respectivo.	Informe de conclusiones emitido por la comisión.	45 días.
Primer debate.	Inclusión del informe de la comisión especializada con las observaciones que juzgue necesarias.	Humanos: Presidenta/e de la Asamblea Nacional, Asambleístas. Materiales: Para presentación de observaciones.	Distribución del informe a los asambleístas y observaciones que sean necesarias introducir.	30 días.
Segundo debate.	Presentación a la Presidenta/e de la Asamblea Nacional, el informe de la comisión analizando y acogiendo las observaciones.	Humanos: Presidenta/e de la Asamblea Nacional, Asambleístas. Materiales: Para presentación de observaciones.	Distribución del informe a los asambleístas e incorporación de cambios al Proyecto de ley sugeridos en el Pleno.	45 días.
Remisión del Proyecto de ley a la Presidenta/e de la República.	Proyecto de ley aprobado por la Asamblea Nacional es enviado a la Presidenta/e de la República para su sanción u objeción.	Humanos: Presidenta/e de la República, para que sancione u objete el Proyecto de ley.	Promulgación u publicación en el Registro Oficial.	32 días.

Cuadro Nº 21
Fuente: Investigador
Elaboración: César E. Naranjo Mesías

Desarrollo de la Propuesta

Exposición de Motivos

El retardo de una solución a lo que hoy ya puede considerarse un problema grave, al no estar reconocida en nuestra legislación la interceptación de comunicaciones y el abuso de dispositivos son amenazas que con el pasar el tiempo provocarán daños incalculables al ser violentado el derecho a la intimidad, puesto que, en definitiva, se necesita urgentemente la regulación en nuestra legislación penal.

Es Increíblemente q los delincuentes hoy están utilizando la tecnología para facilitar el cometimiento de infracciones y eludir a las autoridades. Este hecho ha creado la necesidad que se tome en cuenta para que se legisle y se brinde especialización y capacitación en estas nuevas áreas en donde los Tics se convierten en herramientas necesarias en auxilio de la Justicia y la persecución de delito y el delincuente.

La obtención de Información (elementos de convicción) se constituye en una de las facetas útiles dentro del éxito de en una investigación criminal, aspecto que demanda de los investigadores encargados de la recolección, preservación, análisis y presentación de las evidencias digitales; una eficaz labor que garantice la autenticidad e integridad de dichas evidencias, a fin de ser utilizadas posteriormente ante el Tribunal Penal.

Este problema que nos afecta a todos suscitando de esta manera preocupación tanto en nuestro país como en el ámbito internacional. Es incuestionable que los poderes públicos deben dar cobertura y solución, dentro de sus posibilidades, a estas situaciones de desprotección y proporcionar una adecuada garantía para la protección del derecho a la intimidad de la sociedad y el Estado en general.

Este tipo penal se evidencia cuando el agente que tiene o ha tenido una

relación de dependencia laboral o personal con el sujeto pasivo, revela, expone, pública o divulga a terceras personas, aspectos o datos sensibles de la intimidad personal o familiar de aquél, a los cuales ha tenido acceso por razones del trabajo que realizó para aquel o para un tercero que conocía aquellos aspectos de la víctima por haberlos confiado.

En otras palabras, el comportamiento prohibido consiste en revelar o divulgar aspectos íntimos del agraviado que conociera el agente con motivo del trabajo que prestó a aquél o a la persona a quien éste le confió.

Considerando:

Que, de conformidad al artículo 1 de la Constitución de la República del Ecuador, publicada en el Registro Oficial No. 449 de 20 octubre de 2008 determina que El Ecuador es un Estado constitucional de derechos y justicia, social, democrático, soberano, independiente, unitario, intercultural, plurinacional y laico;

Que, al tenor del segundo inciso del artículo 1 de la Constitución, la soberanía radica en el pueblo, cuya voluntad es el fundamento de la autoridad, y se ejerce a través de los órganos del poder público y de las formas de participación directa;

Que, el artículo 61 de la Constitución establece los derechos de participación de los que gozan las ecuatorianas y los ecuatorianos.

PROYECTO DE INCLUSIÓN DE LOS ARTÍCULOS INNUMERADOS 202.3 Y 202.4 AL ART. 202 DEL CÓDIGO PENAL ECUATORIANO ACERCA DE LA INTERCEPTACIÓN DE COMUNICACIONES Y ABUSO DE DISPOSITIVOS.

Agréguese dos Artículos innumerados después del Art. 202.2 del Código Penal.

ART. 202.3. DE LA INTERCEPTACIÓN DE TELECOMUNICACIONES.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento procure la interceptación deliberada e Ilegítima de sus telecomunicaciones, por medios o artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será reprimido con reclusión menor ordinaria de tres a seis años y multa de quinientos a mil dólares de los Estados Unidos de América.

Se impondrá el máximo de la pena si quien cometiera la infracción fuera Funcionario Público.

ART. 202.4. ABUSO DE DISPOSITIVOS.- El que para cometer las infracciones determinadas en los Artículos. 202.1, 202.2 y 202.3 realice la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

1. Un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos señalados en el párrafo anterior.
2. Una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados Artículos. 202.1, 202.2 y 202.3.

   Será sancionado con una pena de prisión de seis meses a dos años y multa de quinientos a dos mil dólares de los Estados Unidos de América,

la posesión de alguno de los elementos contemplados en los numerales 1 y 2 del apartado anterior con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos. 202.1, 202.2 y 202.3., será reprimido con prisión de tres a seis meses y multa de doscientos cincuenta a quinientos dólares de los Estados Unidos de América.

No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 202.1, 202.2 y 202.3, como es el caso de las pruebas autorizadas o de la protección de un sistema Informático.

La presente Reforma al Código Penal entrará en vigencia a partir de su publicación en el Registro Oficial.

Administración

La reforma de inclusión de dos artículos innumerados al artículo 202 del Código Penal Ecuatoriano respecto a la Interceptación de Comunicaciones y Abuso de Dispositivos, funcionaría bajo el sistema de investigación establecido por la Fiscalía General del Estado a través de un sistema de investigación especializada por el Consejo Nacional de la Judicatura y sus dependencias en cada provincia, a los que podrían adherirse otras entidades; a fin de garantizar la adecuada operación y acceso a una justicia sin dilaciones; así como para evaluar y mejorar los servicios prestados, ampliando su esfera de acción cada vez a un mayor número de beneficiarios/as.

Previsión de la Evaluación

Inmediatamente después que se hayan realizado las actividades previas, a la presentación del Proyecto de Ley a la Asamblea Nacional, se verán los

resultados positivos o negativos referentes a la aplicabilidad de la propuesta planteada.

Se plantea la previsión de la evaluación posterior a la evaluación.

Instrumentos.- Los instrumentos de evaluación son indispensables tanto para los organismos involucrados y sus funcionarios como para los beneficiarios/as.

Técnicas.- Se deben aplicar las mejores técnicas para tener una mejor visión del proceso, aplicando entre ellas tenemos la que mejor se ha desarrollado conforme a nuestro tema es la encuesta y entrevista.

Criterios.- La evaluación debe ser diagnóstica, formativa, comprensiva y sumativa.

Evaluación Diagnóstica.- Se aplicara cuestionarios previamente elaborados con técnicas de acuerdo a los conocimientos anteriores, para detectar falencias existentes en ese medio.

BIBLIOGRAFÍA

- Business Software Alliance BSA, 5ta Estudio Anual Global de la Piratería de Software por BSA e IDC, 2007, http://global.bsa.org/idcglobalstudy2007/.

- Carlo Sarzana; Criminalista e Tecnología en Computer Crime Rasaggna Penitenziaria e Criminalitá – Roma 1979.

- CERT, Informe de Vulnerabilidades, 2007, http://www.cert.org/.

- Convenio de Cyber-delincuencia del Consejo de Europa Estados miembros del Consejo de Europa y otros Estados – Budapest 2001 http://www.coe.int.

- CSI. Computer Crime & Security Survey, 2007, http://www.gocsi.com/.

- Diario el Telégrafo, Edición N° 45119, Transparencia en la Información Pública, Página 4 y 5, Publicación Octubre 27 del 2008.

- DIJIN (Dirección Central de Policía Judicial), http://www.dijin.gov.com.

- Emilio del Peso Navarro, Peritajes Informáticos, Página 10, 2da Edición, Editorial Díaz de Santos S.A, 2001.

- Eoghan Casey E, Digital Evidence and Computer Crimen, Página 9, 2da Edición, Edit Elsevier Ltda, 2004.

- Gerberth Adín Ramírez, Informática Forense, Página 2 - 4, Publicación Universidad San Carlos de Guatemala, 2008.

- Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos, http://www.oas.org/juridico/spanish/cybersp.htm.

- Grupo Faro, Acción Colectiva para el Bienestar Público, Cumplimiento de la Ley Lotaip, 2007, http://www.grupofaro.org/.

- Hans Kelsen, General Theory of Law and State, Harvard University, Editorial Porruo 1945.

- Introducción a la Informática Forense. Dr. Santiago Acurio del Pino, Director Nacional de Tecnologías de la Información de la Fiscalía General del Estado.

- Jeimy J. Cano M, Introducción a la Informática Forense, Revista Sistemas N° 96, Publicado por Asociación Colombiana de Ingeniero de Sistemas (ACIS), 2006, http://www.acis.org.co/FBI, Computer Evidence Examinations at the FBI, 2nd International Law Enforcement Conference on Computer Evidence, 1995, http://www.fbi.gov/.

- Jeimy J. Cano M, Estado del arte del Peritaje Informático en Latinoamérica, 2005, http://www.alfa-redi.org/.

- Jeimy J. Cano M, Consideraciones sobre el Estado del arte del Peritaje Informático en Latinoamérica, Revista de Derecho Comunicaciones y Nuevas Tecnologías, Universidad de los Andes, 2007,http://derechoytics.uniandes.edu.co.

- Juan Carlos Riofrío – La Prueba Electrónica. Editorial TEMIS S.A. Edición 2004.

- Julio Téllez Valdés, Derecho Informático, 2da Edición, Mc Graw Hill – México 1996.

- Ley Modelo sobre Comercio Electrónico, CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 1996 complementada por la Comisión en 1998. http://www.uncitral.org/.

- Ley Modelo sobre Firmas Electrónicas, CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, 2001, http://www.uncitral.org/.

- María de la Luz Lima, Delitos Electrónicos Pág. 100, Ediciones Porrua – México 1984.

- Manual de Peritaje Informático. Maricarmen Pascale, Fundación de Cultura Universitaria. Uruguay. 2007.

- Miguel López Delgado, Análisis Forense Digital, Página 10 - 23, 2da Edición, 2007.

- Montiel Sosa, Criminalística Tomo III Página 86, Editorial Limusa 1997.

- Pedro Miguel Lollet R, Auditoria Forense, Publicado por ACGAF, http://auditoriaforense.net/

- Phil Williams, Crimen Organizado y Cibernético, Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon, http://www.pitt.edu/.

- Plan de Seguridad Ciudadana y Modernización de la Policía Judicial, http://www.policiaecuador.gov.ec/publico/img_policia/rendicion.pdf.

- Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público, http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf.

- Red IRIS, Informe de Evolución de Incidentes de Seguridad, 2007, http://www.rediris.es/.

- The Best Practices for Seizing Electronic Evidence, Version 3.0, Us. Department of Home Land Security, and the United States Secret Service.

Linkografía

- http://www.apsique.com/wiki/DesaPadre_ausente.
- http://institutoninezyadolescenciacam.blogspot.com/2009/11/para-bajar-libros-gratis-sobre.html
- http://www.iustel.com/v2/revistas/detalle_revista.asp?id_noticia=400354
- http://dragiocondabatres.com/descargas/Manual%20de%20Ninos%20que%20Abusan.pdf
- www.orientared.com

ANEXOS

Anexo Nº 01

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Entrevista Nº……

Fecha:…….....

Nombre:……

Cargo que desempeña:…….

Entrevista dirigida a los señores funcionarios del Departamento de Investigación y Análisis Forense de la Fiscalía General del Estado

La siguiente entrevista pretende recoger su opinión acerca de la falta de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos vulneran la intimidad del amparo de la ley. No hay respuestas mejores o peores, todas son igualmente válidas siempre que correspondan con su opinión, por lo que le ruego sea sincero/a y responda con toda libertad.

El principio de confidencialidad será absoluto, en virtud de que la información brindada se la utilizará estrictamente para los fines de esta investigación.

1.- ¿De acuerdo a su experiencia que realmente le preocupa respecto a la vulnerabilidad de la intimidad?

……

……

……..…..

2.- ¿Hay hechos que verdaderamente empeoran la vulnerabilidad de la intimidad?

……

……

……..……..

3.- ¿Quién considera usted que debería asumir el control referente a las comunicaciones, el uso de dispositivos para que se proteja el derecho a la intimidad? ¿Por qué?

……

……

……....

4.- ¿Cómo debería asumir esta responsabilidad la entidad o persona señalada por usted?

……

……

……..…..

5.- ¿De qué modo la falta de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos afecta a la intimidad?

……

……

……..…..

6.- ¿Qué cambios propondría para remediar esta situación?

……

……

……..……..

7.- ¿Cómo el Estado cumple su función de protección hacia el derecho a la intimidad?

……

……

……..……..

8.- ¿Cree usted que el derecho a la intimidad esté plenamente amparado por la ley?

……

……

……..……..

¡GRACIAS POR SU COLABORACIÓN!

Anexo Nº 02

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE JURISPRUDENCIA Y CIENCIAS SOCIALES

CARRERA DE DERECHO

Encuesta Nº……

Fecha:…….....

Encuesta dirigida al departamento de criminalística de la policía judicial y profesionales del derecho.

La siguiente encuesta pretende recoger su opinión acerca de la ausencia de normativa respecto a la interceptación de comunicaciones y abusos de dispositivos provoca la vulnerabilidad de la intimidad. A continuación encontrará una serie de interrogantes, únicamente debe marcar con una X en la opción con la que usted está de acuerdo o desacuerdo. El principio de confidencialidad será absoluto, en virtud de que la información brindada se la utilizara estrictamente para los fines de esta investigación.

1.- ¿Considera que la interceptación de comunicaciones y abuso de dispositivos vulneran los derechos fundamentales de las personas?

SI ( ) NO ( )

2.- ¿Cree que la interceptación de comunicaciones y abuso de dispositivos provoca la vulnerabilidad de la intimidad?

SI ( ) NO ( )

3.- ¿Comprobada la inexistencia de normativa respecto a la interceptación de comunicaciones y abuso de dispositivos existe otras normas sancionadoras para este tipo de delitos?

SI ( ) NO ( )

4.- ¿Cree usted que el desconocimiento acerca de este tipo de delitos es una de las razones para que no se reconozca en nuestra legislación penal?

SI ( ) NO ( )

5.- ¿Cree usted que el Estado debe garantizar el derecho a la intimidad?

SI ( ) NO ( )

6.- ¿Cree usted que la falta de control provoque la difamación, espionaje, violación de reservas industriales o comerciales, divulgación y empleo de documentos reservados, violación ilícita de comunicaciones; y, el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas?

SI ( ) NO ( )

7.- ¿Cree usted que mediante el aprovechamiento de nuevas tecnologías de comunicación y dispositivos vulneran directamente la intimidad?

SI ( ) NO ( )

8.- ¿Considera usted que al no contar con una normativa respecto a la interceptación de comunicaciones y abuso de dispositivos este tipos de delitos queden en la impunidad?

SI ( ) NO ( )

9.- ¿Cree usted que el acceso no controlado a nuevas tecnologías de información y comunicación vulneran la intimidad?

SI ( ) NO ( )

10.- ¿Considera usted oportuno que se reforme el Código Penal vigente para que se reconozca la interceptación de comunicaciones y abuso de dispositivos que atentan la intimidad?

SI ( ) NO ( )

¡GRACIAS POR SU COLABORACIÓN¡

GLOSARIO

- **Auditoria Forense:** es una alternativa para combatir la corrupción, porque permite que un experto emita ante los jueces conceptos y opiniones de valor técnico, que le permiten a la justicia actuar con mayor certeza, especialmente en lo relativo a la vigilancia de la gestión fiscal.
- **Base De Datos:** Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.
- **Browser (Buscador):** El software para buscar y conseguir información de la red WWW. Los más comúnmente usados son Microsoft Explorer, Firefox y Opera.
- **Caballo de Troya.-** Sirve para manipular software a través de un sistema difícil de localizar. Su función es modificar programas en el sistema de las computadoras de forma que cumpla con funciones no solicitadas.
- **Cracker.-** Es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo.
- **Comunicación Inalámbrica.-** Es la comunicación de un punto a otro por medios de transmisión sin la necesidades de un cableado estructurado.
- **Cookie**: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que está haciendo. Hay una variedad de "anticookie" software que automáticamente borra esa información entre visitas a su sitio.
- **Delito.-** Etimológicamente, la palabra delito proviene del latín delictum, expresión también de un hecho antijurídico y doloso castigado con una pena. En general, culpa, crimen, quebrantamiento de una ley imperativa.

- **Delito Informático:** Según María de la Luz Lima, dice que el "delito informático en un sentido amplio es cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin".
- **Dialup (Marcar)**: El método de conectarse con Internet vía la línea de teléfono normal mediante un modem, en vez de mediante una LAN (Red Local) o de una línea de teléfono alquilada permanentemente. Esta es la manera más común de conectarse a Internet desde casa si no ha hecho ningún arreglo con su compagina de teléfono o con un ISP. Para conexiones alternativas consulte con su ISP primero.
- **Digital Signature (Firma Digital)**: El equivalente digital de una firma autentica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma escribió o autorizo el Archivo.
- **Documento Electrónico:** Es la representación en forma electrónica de hechos jurídicamente relevantes susceptibles de ser presentados en una forma humanamente comprensible.
- **Fraude:** Engaño, inexactitud, consistente, abuso de confianza, que produce o prepara un daño, generalmente material.
- **Hacker.-** La palabra "hack" en inglés tiene varios significados en español, entre ellos "hacha". Como si fuesen taladores de árboles que usan su hacha, en forma infatigable hasta llegar a tumbarlos, su tesonero propósito les mereció este apelativo. La palabra hacker aplicada en la computación se refiere a las personas que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía.
- **Hallazgo:** Es la recopilación de información especifica sobre una operación, actividad, organización, condición u otro asunto que se haya analizado y evaluado y que se considera de interés o utilidad para los funcionarios del organismo.

- **Herramientas de la Auditoria Forense:** Son artículos u objetos que ayuda a resolver un problema que puede ser de cualquier clase, técnico, labora, penal, etc."
- **HTTP (HYPER TEXT TRANSPORT PROTOCOL). -** El conjunto de reglas que se usa en internet para pedir y ofrecer páginas de red y demás información.
- **Informe:** Comunica a las autoridades pertinentes los resultados de la Auditoría. Los requisitos para la preparación del informe son claridad y simplicidad, importancia del contenido, respaldo adecuado, razonabilidad, objetividad entre otros.
- **Infracciones electrónicas.-** son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y, culpables en que se tienen a las computadoras como instrumento o fin.
- **Internet.-** Red de ordenadores que permite intercambiar información con personas de todo el mundo.
- **Interceptación de las comunicaciones.-** Es una ofensa para cualquier persona que intencionalmente y sin autorización legal, para interceptar las comunicaciones en el curso de su transmisión a través de un sistema de telecomunicaciones públicas y salvo en determinadas circunstancias a través de un sistema de telecomunicaciones privadas.
- **Intranet.-** Es el conjunto de redes privadas que son usadas a través de puertas lógicos (Gateways) para transmitir información de un punto a otro.
- **Insiders.-** Según un reciente informe de la publicación estadounidense Information Week, un porcentaje sustancial de intrusiones en las redes de las empresas (ya sean chicas, medianas o grandes) proviene de ataques internos. Es decir, los mismos empleados hackean a su propia organización.
- **Interceptación de Comunicaciones.-** Es una ofensa para cualquier persona que intencionalmente y sin autorización legal, para interceptar las comunicaciones en el curso de su transmisión a través de un sistema de telecomunicaciones públicas y - salvo en determinadas circunstancias a

través de un sistema de telecomunicaciones privadas.

- **La Intimidad.-** Es al intrínseco, muy personal que generalmente son asuntos o afectos reservados de una persona o familia.
- **Manipulación de los datos.-** Este fraude conocido también como sustracción de datos, este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos.
- **Manipulación de programas.-**. Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas.
- **Manipulación informática.-** Es una alteración o modificación de datos, ya sea suprimiéndolos, introduciendo datos nuevos y falsos, colocar datos en distinto momento o lugar, variar las instrucciones de elaboración, etc.
- **Mensaje de Datos:** Es toda aquella información visualizada, generada enviada, recibida, almacenada o comunicada por medios informáticos, electrónicos, ópticos, digitales o similares.
- **Metodología:** Según el Diccionario, Método es el "modo de decir o hacer con orden una cosa". Asimismo define el diccionario la palabra Metodología como "conjunto de métodos que se siguen en una investigación científica". Esto significa que cualquier proceso cinético debe estar sujeto a una disciplina de proceso defina con anterioridad que llamaremos Metodología.
- **Modem**: Un aparato que cambia datos del computador a formatos que se puedan transmitir más fácilmente por línea telefónica o por otro tipo de medio.
- **Networks Scanners.-** Hacen un mapa de la red identificando: dominios, servidores, sistemas operativos.
- **Outsiders.-** El outsider es la persona con conoce muy bien la instalación de una organización pero no pertenece a ella. Son aquellos que ingresan a la red simplemente averiguando una password autorizada. El aprovechamiento ilícito de las vulnerabilidades da lugar al delito informático que pueden originar en muchos casos siniestros informáticos

- **Packet Sniffers.**- Permiten leer la información de los paquetes que pasan por la red donde están instalados.
- **Passwords crackers.**- Se usan para detectar la confinación de usuarios y passwords válidos.
- **Phreaker.-** Es una persona que con amplios conocimientos de telefonía puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general celulares. Construyen equipos electrónicos artesanales que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello. En Internet se distribuyen planos con las instrucciones y nomenclaturas de los componentes para construir diversos modelos de estos aparatos.
- **Ports Scanners.-** Scanean las máquinas para detectar puertos abiertos, a fin de identificar posibles exposiciones o vulnerabilidades a explotar. Sistemas activos, servicios a la escucha, sistemas operativos.
- **Sabotaje Informático.-** El acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema.
- **Sistemas de comunicación.-** Abuso de dispositivos informáticos.- Esta es otra forma de delincuencia informática, aunque se puede describir mejor como delitos informáticos. Esto implica el uso de activos de la empresa, en este caso los ordenadores, por los empleados para actividades no autorizadas.
- **Sistema Telemático.** Conjunto organizado de redes de telecomunicaciones que sirven para trasmitir, enviar, y recibir información tratada de forma automatizada.
- **Sistema de Información:** Se entenderá como sistema de información, a todo sistema utilizado para generar, enviar, recibir, procesar o archivar de cualquier forma de mensajes de datos.
- **Sistema Informático:** Conjunto organizado de programas y bases de datos que se utilizan para, generar, almacenar, tratar de forma automatizada datos o información cualquiera que esta sea.
- **Spam.**- El Spam o los correos electrónicos no solicitados para propósito

comercial, es ilegal en diferentes grados. La regulación de la ley en cuanto al Spam en el mundo es relativamente nueva y por lo general impone normas que permiten la legalidad del Spam en diferentes niveles. El Spam legal debe cumplir estrictamente con ciertos requisitos como permitir que el usuario pueda escoger el no recibir dicho mensaje publicitario o ser retirado de listas de email.

- **Soporte Lógico:** Cualquiera de los elementos (tarjetas perforadas, cintas o discos magnéticos, discos ópticos) que pueden ser empleados para registrar información en un sistema informático.
- **Soporte Material:** Es cualquier elemento corporal que se utilice para registrar toda clase de información.
- **TCP/IP: (TRANSMISIÓN CONTROL PROTOCOL/INTERNET PROTOCOL).-** Conjunto de protocolos que hacen posible la interconexión y tráfico de la Red Internet.
- **Telemátic (Telemática).-** Contratación de telecomunicación e informática.
- **Trojans.**-Permiten introducir back doors en las redes.
- **Vulnerabilidad**.- Consiste en la incapacidad de una comunidad para absorber, mediante auto ajuste, los efectos de un determinado cambio en su medio ambiente, o sea, su no flexibilidad o incapacidad para adaptarse a ese cambio, que para la comunidad constituye un riesgo.
- **Vulnerabilidad de un sistema informático.-** Es la cualidad que le hace susceptible de ser afectado, alterado o destruido por algún hecho o circunstancia indeseada, de recibir algún daño o perjuicio en cualquiera de las partes o componentes, que afecte al funcionamiento normal o previsto de dicho sistema informático.
- **War Dialers.-** Son los que permiten detectar módems en las líneas de teléfono.