UNIVERSIDAD NACIONAL DE LOJA

UNIDAD DE EDUCACIÒN A DISTANCIA

CARRERA DE DERECHO

TÍTULO:

“DESAFÍOS Y PERJUICIOS LEGALES EN LA SOCIEDAD DE LA INFORMACIÓN POR LAS INFRACCIONES INFORMÁTICAS”

Tesis previa a optar el título de Abogado

Autor: **Héctor Roberto Gordon Quinche**

Director: **Dr. Mg. Augusto Astudillo Ontaneda**

Loja – Ecuador

2018

CERTIFICACIÒN

Dr. Mg. Augusto Astudillo Ontaneda CATEDRÀTICO DE LA UNIDAD DE EDUCACIÒN A DISTANCIA DE LA UNIVERSIDAD NACIONAL DE LOJA

CERTIFICA

Que la presente tesis con el tema "**DESAFÍOS Y PERJUICIOS LEGALES EN LA SOCIEDAD DE LA INFORMACIÓN POR LAS INFRACCIONES INFORMÁTICAS.**", ha sido desarrollada bajo mi dirección la misma que, responde plenamente a las exigencias legales de fondo y de forma por lo que autorizo su presentación, sustentación y defensa.

Loja, Noviembre 2017

Dr. Mg. Augusto Astudillo Ontaneda

DIRECTOR DE TESIS

AUTORÍA

Yo, Héctor Roberto Gordon Quinche declaro ser autora del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el repositorio Institucional-biblioteca Virtual.

AUTOR: Héctor Roberto Gordon Quinche

FIRMA: .....

CÉDULA: 0102116662

FECHA: Loja, febrero de 2018

CARTA DE AUTORIZACION DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCION PARCIAL O TOTAL, Y PUBLICACION ELECTRÒNICA DEL TEXTO COMPLETO

HÉCTOR ROBERTO GORDON QUINCHE declaro ser autor de la tesis tema "DESAFÍOS Y PERJUICIOS LEGALES EN LA SOCIEDAD DE LA INFORMACIÓN POR LAS INFRACCIONES INFORMÁTICAS", como requisito para optar el Grado de Abogado; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad,

la Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 22 días del mes de febrero de 2018, firma el autor.

Firma:.....

Autor: Héctor Roberto Gordon Quinche
Cedula: 0102116662
Dirección: Cuenca, calle Pedro Vicente Maldonado y Jorge Juan
Correo electrónico: hectorgordon@yahoo.com
Teléfono: 0998168196

DATOS COMPLEMENTARIOS

Director de tesis: Dr. Mg. Augusto Astudillo Ontaneda

TRIBUNAL DE GRADO:
Presidente: Dr. Felipe Neptali Solano Gutierrez Mg. Sc.
Vocal: Dr. Gonzali Ivan Aguirre Valdivieso Mg. Sc.
Vocal: Dr. Marco Ortega Cevallos Mg. Sc.

DEDICATORIA

Dedico este trabajo de Investigación a mi Esposa e hijos, a mi Madre que desde todo el infinito del Universo me llena de bendiciones y amor, a mi Padre que con su ejemplo de perseverancia ha sabido guiarme por los caminos de la responsabilidad y del bien, a mis hermanos que con su ejemplo de superación han sido una fuente de inspiración.

Gracias a todos

AGRADECIMIENTO

Quiero primero agradecer al Supremo por todas las bondades y bendiciones recibidas, a mi Esposa, Compañera y Amiga Adriana Sigüenza, a mis hijos Milena, Francisco, Agustín y Grecko por ser pilares de mi vida y por permitirme robarles su tiempo en todos estos años de estudio, también quiero un agradecer de forma especial a todos los Profesores y personal administrativo de la Unidad de Educación a Distancia de la Universidad Nacional de Loja

Héctor Roberto Gordon Quinche

a. Título

“DESAFÍOS Y PERJUICIOS LEGALES EN LA SOCIEDAD DE LA INFORMACIÓN POR LAS INFRACCIONES INFORMÁTICAS”

b. Resumen

Los delitos informáticos pueden ser considerados como crímenes electrónicos, tan graves que pueden llegar a ser un problema para el avance de la informática. Sin embargo este puede tener consigo delitos tan graves como el robo, falsificación de documentos, fraudes, chantajes y malversación de caudales públicos. Un ejemplo muy común es cuando una persona llega a robar información y a causar daños de computadoras o servidores que pueden llegar a ser absolutamente virtuales porque la información se encuentra en forma digital y el daño cada vez se vuelve más grande.

Muchas de las personas que cometen este tipo de delitos informáticos tienen diferentes características tales como la habilidad del manejo de los diferentes sistemas informáticos o la realización de tareas laborales que le facilitan el acceso de carácter simple. La investigación sobre “El problema de la falta de conocimiento sobre el proceso que se debe seguir en los casos de delitos informáticos tiene como propósito reflexionar sobre la aplicación del sistema de justicia actual en todos los casos.

La propuesta servirá para mejorar el sistema de administración de justicia en lo concerniente a garantizar los derechos que el Estado asiste a todos los individuos y para garantizar el debido proceso en este caso específico. La propuesta en si consiste en la inclusión de delitos informáticos en el

Código Orgánico Integral Penal, la intención es de coadyuvar a que se respete y garantice los derechos y obligaciones de los ciudadanos, y se desarrollen de acuerdo a las Leyes Nacionales, Convenios y Pactos Internacionales.

ABSTRACT

Computer crimes can be considered as electronic crimes so serious that they can become a problem for the advancement of computer. However this can have with it such serious crimes as theft, forgery, fraud, racketeering and embezzlement of public funds. A common example is when a person comes to steal information and damage computers or servers that can become quite virtual because the information is in digital form and the damage becomes increasingly larger.

Many of the people who commit this type of cybercrime have different features such as the ability of handling different computer systems or performing work tasks that will facilitate access to simple character. Research on "The problem of lack of knowledge about the process to be followed in cases of cybercrime is intended to reflect on the implementation of the current system of justice in all cases for this research was conducted through surveys Provincial Judges, Members of the Court and judges of penal guarantees of Cotopaxi, prosecutors and lawyers in the free exercise of the Province, of which results were obtained for carrying out a feasible proposal is the inclusion of computer crimes in the Penal Code. The proposal will improve the system of administration of justice with regard to guaranteeing the rights that the State attends to all individuals and to ensure due process in this specific case. The proposal itself is the inclusion of computer crimes in the Penal Code, the intention is

to contribute to respect and ensure the rights and obligations of citizens, and conducted in accordance with national laws, international conventions and covenants.

c. Introducción

A nadie se nos escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones tanto públicas como privadas, la importancia que tiene su progreso para el desarrollo de un país los sistemas de información y el crecimiento de la economía digital. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, entre otros, son aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática, todo esto junto al avance de la informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos[1].

Para lograr una investigación completa de la temática se establece la conceptualización respectiva del tema, generalidades asociadas al fenómeno, estadísticas mundiales sobre delitos informáticos o infracciones informáticas, el efecto de éstos en diferentes áreas, como poder minimizar la amenaza de los delitos a través de la seguridad, la parte importante en los aspectos de legislación informática, y por último se busca unificar la investigación realizada para poder establecer el papel de la Ley Penal frente a las infracciones informáticas.

[1] Como en la mayor parte de los hechos delictivos interesa saber acerca del criminal, así mismo en el ciber-criminalidad, es menester estudiar los perfiles delictivos de las personas que cometen este tipo de conductas a través de las TIC, desde el punto de vista criminológico. Maestría de Ciencias Penales

Al final del documento se establecen las conclusiones pertinentes a la investigación en la que se busca destacar situaciones relevantes, comentarios, análisis, entre otros; la revolución tecnológica ha transformado profundamente la realidad del mundo entero, permitiendo a los seres humanos en la actualidad alcanzar lo inimaginable y conseguir nuevos objetivos hasta hace poco inalcanzables.

Estos cambios increíbles ha servido en su mayor para el bienestar de todos los individuos, facilitando la comunicación, los negocios, el acceso a la información entre otros, pero también ha existido quienes han sabido sacar provecho de este avance, hoy en día ya no hace falta el control, porque existen las herramientas para delinquir y el arma del nuevo delincuente es un teclado alfanumérico con código para proceder a atacar a las información de terceros; por ello solo un cabal conocimiento de la aplicación de las nuevas tecnologías y de sus métodos de protección, otorgarían al navegante seguridad al acceder a un ilimitado mundo de nuevas tecnologías.

Los efectos totalmente negativos que producen las infracciones informáticas dentro de la sociedad de la información son muchas veces desastrosas para quienes nos ha facilitado la creación, distribución y manipulación de la información particular o corporativa, tomando en cuenta que al momento de accionar alguna infracción informática la

investigación previa o posterior de la infracción requiere de conocimientos y procesos claros al establecer el peritaje informático forense que muchos casos o casi todos de ellos con delitos informáticos quedan en investigación porque no se detalla las evidencias eficaces y no se juzga efectivamente a los infractores. Nos enfrentamos a un gran problema social ya que estas conductas inapropiadas no pueden ser investigadas de forma clara, los problemas que se dan en todas sus etapas, la gran mayoría es por falta de evidencia digital probatoria en algunos casos y lo que es aún más grave en otros por falta de conocimiento, experiencia y un aparente vacío en la Ley pertinente que dificulta la aplicabilidad por parte de las autoridades encargadas de la administración de justicia para este tipo de delitos, que en nuestro País es una forma de delinquir sumamente incipiente.

Para respaldar esta investigación es importante mencionar que base legal está incluida en varios Capítulos referente a los delitos, infracciones informáticas en el Código Orgánico Integral Penal vigente actualmente en el Estado Ecuatoriano, COIP[2].

Debemos tomar cartas sobre el incumplimiento de las normas establecidas dentro de la sociedad ecuatoriana, están siendo porcentualmente un hecho que actúa como factor multiplicador de la

[2] El Código Orgánico Integral Penal, a veces simplemente referido por sus siglas **COIP**, es un conjunto sistematizado y organizado de normas jurídicas de carácter punitivo, es decir un compendio legislativo que establece delitos y penas conforme al sistema penal ecuatoriano.

impunidad en los casos sobre las infracciones informáticas, dejando un vacío por la falta de aplicabilidad de la Ley en los casos judiciales, por tal particularidad las infracciones quedan como procesos investigativos extrajudiciales.

Para garantizar el pleno ejercicio de los derechos de todas las personas y la seguridad jurídica dentro de la Sociedad que debe ofrecer el Estado Ecuatoriano, es necesario el análisis profundo de las infracciones informáticas, su modus operandi y tratarlo de plasmar con el Código Orgánico Integral Penal, garantizando una administración de justicia eficiente para resolver este tipo de casos tan incipientes en nuestra Sociedad de la Información.

d. Revisión de literatura

Marco Conceptual

El Dr. TÉLLEZ VALDÉS[3], Julio menciona en su obra titulada Derecho Informático, (2010) "dos clasificaciones del Delito Informático para efectos de conceptuación, que parten de lo típico y lo atípico.

El concepto típico, los Delitos Informáticos son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin". El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos.

Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos o infracciones informáticas del resto. Partiendo de esta compleja situación y tomando como referencia el **"Convenio de Ciberdelincuencia del Consejo de Europa[4]"**, podemos definir las infracciones y 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, redes y datos". En el Ecuador así como en los demás países, todos los principios jurídicos, legales y procesales, así como doctrinarios,

[3] Doctorado en Informática Jurídica y Derecho de la Informática por el Instituto para la Investigación y Tratamiento de la Información Jurídica, Francia 1981. Coordinador del Observatorio Electoral 2.0. Miembro Honorario de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI)

[4] Budapest, 23.XI.2001 Preámbulo Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio; Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros; Reconociendo el interés de intensificar la cooperación con los Estados Partes en el presente Convenio; Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional.

están presentes en el tratamiento del delito informático, su investigación y juzgamiento, sin embargo las características propias de este delito que pertenece a una nueva era, a la era de la información y el conocimiento, trasciende al ordenamiento jurídico vigente, constituyendo un elemento de inflexión o quiebre del tradicional sistema jurídico.

Tipos de Delitos Informáticos

CAMACHO LOSA[5], en un artículo publicado en el internet señala que el único límite 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 DON 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, se ponemos a consideración del lector en forma breve en qué consiste cada una de estas conductas delictivas.

Los Datos Falsos o Engañosos.

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.

Manipulación de Programas “Caballos de Troya”.

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática y

[5] https://www.iberlibro.com/buscar-libro/titulo/delito-inform%E1tico-el/autor/camacho-losa-luis/

en desarrollo de código. 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 que consiste en insertar instrucciones de computadora de forma encubierta en un programa para que pueda realizar una función no autorizada al mismo tiempo que su función normal sin ser detectado.

La Técnica del Salami o Gusanos de Morris

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.

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 víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos años, 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.

Bombas Lógicas

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 y Malware.

Son elementos informáticos, que como los microrganismos 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.

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.

Ataques de Denegación de Servicio.

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventana, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

El Espionaje Informático y el Robo o Hurto de Software.

Fuga de Datos.

También 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 del 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 supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

Apropiación de Informaciones Residuales

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 y Suplantación de Personalidad

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.

El Acceso no Autorizado a Servicios Informáticos.

Las Puertas Falsas

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

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

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 señaló 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.

Seguridad Informática y Normativa

La Seguridad Informática.

Es el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya sean estos individuales o conectados a una red frente a posibles ataques accidentales o intencionados.

La seguridad Informática a su vez está dividida en cinco componentes a saber:

- **Seguridad Física:** Es aquella que tiene relación con la protección del computador mismo, vela por que las personas que lo manipulan tengan la autorización para ello, proporciona todas las indicaciones

técnicas para evitar cualquier tipo de daños físicos a los equipos informáticos.

- **Seguridad de Datos:** Es la que señala los procedimientos necesarios para evitar el acceso no autorizado, permite controlar el acceso remoto de la información, en suma protege la integridad de los sistemas de datos.

- **Back Up y Recuperación de Datos:** Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back Up de los sistemas informáticos. Permite recuperar la información necesaria en caso de que esta sufra daños o se pierda.

- **Disponibilidad de los Recursos:** Este cuarto componente procura que los recursos y los datos almacenados en el sistema puedan tener acceso rápidamente por la persona o personas que lo requieren. Permite evaluar constantemente los puntos críticos del sistema para así poderlos corregir de manera inmediata.

- **La Política de Seguridad:** Conjunto de normas y criterios básicos que determinan lo relativo al uso de los recursos de una organización cualquiera.

- **Análisis Forense:** El Análisis Forense surge como consecuencia de la necesidad de investigar los incidentes de Seguridad Informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales.

- **Seguridad Normativa:** Derivada de los principios de legalidad y seguridad jurídica, se refiere a las normas jurídicas necesarias para la prevención y sanción de las posibles conductas que puedan ir en contra de la integridad y seguridad de los sistemas informáticos.

En definitiva para que exista una adecuada protección a los sistemas informáticos y telemáticos se deben conjugar tanto la seguridad informática como la seguridad legal y así poder brindar una adecuada protección y tutela tanto técnica como normativa. En resumen la Seguridad Informática y Normativa debe usarse para impedir los ataques ya sean fuera del sistema (virus, spyware, adware, entre otros) y dentro del mismo, exigiendo políticas claras y precisas sobre el nivel de acceso a cierta información de carácter confidencial y una debida protección a esta.

Según el ilustre penalista CUELLO CALON[6], los elementos integrantes del DELITO son: - El delito es un acto humano, es una acción (acción u omisión). - Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido. Debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.

El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona. La ejecución u omisión del acto debe estar sancionada por una pena. Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

[6] Eugenio **Cuello Calón**. (Salamanca, 1879-Santander, 1963) Jurista español. Fue catedrático de derecho penal en las universidades de Barcelona y de Madrid. Escribió diversas obras, entre las que destacan Derecho penal: Penología (1920) y La nueva penología (1958).

Infracciones Informáticas.[7]

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta. A nivel internacional se considera que no existe una definición propia de la Infracción informática, aunque muchos estudiosos han intentado investigarlo desde diferentes puntos de vista puntos de vista como son el criminógeno, formal, típico y atípico.

Una primera idea al respecto la señala el profesor mexicano Julio Téllez Valdés, quien lo conceptualiza desde dos ópticas. Nos dice que desde un punto de vista atípico son "actitudes ilícitas en que se tiene al computador como instrumento o fin", y desde uno típico son "conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como medio o fin". Esta primera idea es común en los textos del área, así por ejemplo, Nidia Callegari define al delito informático como "aquél que se da con la ayuda de la informática o de técnicas anexas".

Rasgos.

- Son conductas criminógenas de cuello blanco, en tanto que solo un determinado número de personas, en este caso ingenieros de sistemas o técnicos, pueden llegar cometerlas.
- Son acciones ocupacionales, ya que generalmente se ejecutan cuando el sujeto se encuentra en pleno trabajo.
- Son acciones de oportunidad, en cuanto se aprovecha la ocasión presentada.
- Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a quienes los realizan.

[7] http://app.ute.edu.ec/content/3254-42-10-1-6-7/Infracciones%20Informaticas.pdf

- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundos y sin una necesaria presencia física del ejecutante pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias debido a la falta o escasa regulación por parte del Derecho.
- Debido a su carácter técnico presentan grandes dificultades para su comprobación.
- 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.

Sujeto Activo

Las personas que cometen los “Delitos Informáticos” son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, 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, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Sujeto pasivo

En primer término tenemos que distinguir que sujeto pasivo o 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 personas naturales o jurídicas, instituciones crediticias, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

MARCO DOCTRINARIO

Reseña histórica de los delitos informáticos en el Ecuador

En el mundo moderno, el acceso a la información es un derecho que puede ejercerse libremente por cualquier persona, salvo cuando con él puedan afectarse otros como la intimidad, el patrimonio económico, la libre competencia o la seguridad de un Estado. "La tecnología de la información", como la denomina Vittorio Frosini[8], ha traído consigo una criminalidad a la cual la doctrina ha llamado genéricamente "delincuencia informática".

El profesor Francisco Bueno Aruz, citando al profesor Davara, define el delito informático como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software". El autor realiza una descripción general de lo que es acto delictivo, puntualizando que para el delito informático lo que cambia es el instrumento con el que se delinque,

[8] https://it.wikipedia.org/wiki/Vittorio_Frosini

especificando que tiene que ser una herramienta tecnológica (hardware y software).

"Para Tiedemann (citado por Quiñones, 1997) '...los delitos de informática serían cualesquiera que se realicen contra los bienes ligados al tratamiento automático de datos'". Para este autor los delitos informáticos son aquellos únicamente que están en contra de los datos y su tratamiento automatizado y no señala la posibilidad de que con estos mismos datos se puedan realizar fraudes, porque en la actualidad la tecnología ataca de cierta manera a la tecnología misma.

"Lima (citada por Téllez, 1998) dice que el delito electrónico en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel como método, medio o fin. Pues bien en el caso de Lima trata de ampliar el uso de la computadora mirándolo como método y herramienta para ejercer un acto delictivo; como medio para a través de él realizarlos y como fin para que sean estos mismos atacados.

"Quiñones (1997) define a los delitos informáticos como 'cualquier acto violatorio de la ley penal para cuya comisión exitosa es esencial el conocimiento y utilización de la tecnología de las computadoras'". En esta definición el autor trata de escoger los tipos de delincuentes informáticos, haciendo referencia al conocimiento, pues recalca la importancia del estudio de las ciencias de la informática.

"Zabale y otros (2000) definen los delitos informáticos como 'toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable y atente contra el soporte lógico de un sistema de

procesamiento de información, y el cual se distingue de los delitos computacionales o tradicionales informatizados".

"Parker (citado por Cuervo, 1999) define los delitos informáticos como todo acto intencional asociado de una manera u otra a los ordenadores; en los cuales la víctima ha, o habría podido sufrir una pérdida; y cuyo autor ha, o habría podido obtener un beneficio". Este concepto se trata de centrar más en el objetivo de los delitos, los resultados de los ilícitos en algo material tangible.

María Cinta Castillo y Miguel Ramallo entienden que "delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas". El concepto de estos dos autores es un poco más general al describir a estos actos como cualquier acto doloso en el que intervengan equipos informáticos.

Actualmente una ingente cantidad de datos personales de los usuarios del internet son recogidos sin el consentimiento previo del dueño de los datos, gracias al proceso invisible de los datos. Las compañías de publicidad a través de internet procesos estos datos que se van acumulando a través de distintos procedimientos como las cookies o los enlaces invisibles y generan publicidad individualizada según el perfil previamente elaborados. Fernández Esteban da a conocer que "una sola de estas compañías puede generar hasta un billón de banners personalizados al día y a través de estos sistemas, obtienen toda nuestra información, la que nos permite rastrearnos todo el tiempo".

Viendo este tipo de actos desde el plano laboral, y tomando en cuenta que este tipo de hechos realizan una transformación social significativa como lo considera Sanz Larruga, "tratando de hacer que las actividades

laborales sea progresiva y automatizada (robótica), y esto de cierta manera ha hecho incrementar empleo en el área informática, y así facilitar los trabajos de diferentes áreas en cualquier lugar del mundo e incrementando actividades laborales incluso a domicilio, que adicionalmente traerá algunos beneficios, como por ejemplo: el des congestionamiento vehicular, el ahorro de energía, etc. Sin embargo el tratar de regular este tipo de actividades, demanda un gran esfuerzo a nivel de estado". Por su parte Borrajo Dacruz, mira a la tecnología como un esclavo servidor, y a su vez como un amo tirano. El peligro de desarraigo del trabajados respecto de su ambiente laboral y el potencial reforzamiento del autoritarismo tecnocrático en la empresa son amenazas que se ciernen sobre estas nuevas formas laborales.

En cuanto tiene que ver con los virus, Martínez Cantón, plantea en este caso específico, "que la cuestión que surge en primer lugar es preguntarse por el autor de los daños. El que dolosamente lo ha puesto en circulación o el que imprudentemente ha continuado la cadena de reenvío. Este hecho conocido como delito de daños informáticos, castiga los daños producidos por los virus".

Cabe recalcar que en el Manual de las naciones Unidas para la Prevención y Control de delitos informáticos, recalca que cuando el problema se eleva a la escena internacional, igualmente se magnifican los inconvenientes y las insuficiencias para poder sancionar estos delitos, por cuanto estos delitos constituyen una nueva modalidad de delito transnacional y su combate requiere de una eficaz cooperación internacional concertada.

Adelantándose, a las tendencias futuras del cibercrimen, McAfee Labs, predice la continuación de los fraudes y engaños a través de la red, y cada día estos actos se vuelven más sofisticados y personalizados,

tomando en cuenta que los usuarios siguen cada vez más compartiendo información privada y personas por vías electrónicas.

Entrando en materia jurídica haré un breve recorrido por las legislaciones internacionales, para poder centrarnos en la nuestra y realizar un análisis doctrinario de la misma. En la página web de la Biblioteca Nacional del Congreso de Chile, con respecto a un análisis hecho sobre las legislaciones Europeas con respecto al tema de delitos informáticos se refiere a lo siguiente: “Que en Francia la Ley Nº 88-19, que es relativa al fraude informático de 1992, introdujo el capítulo II, al libro II del título II del Código penal, bajo la denominación ”De ciertas infracciones en materia informática”, esta ley que hablaba de los atentados a los sistemas de tratamiento de datos automatizados”.

Carlos Parma en el Código Penal de Argentina, comentado en su tomo II, en la página 542, nos trae jurisprudencia en la materia de virus informático, en el que básicamente se recalca, “que frente a un ataque a través de mensajes electrónicos infectado con virus efectivamente haber sido afectada de manera grave a una empresa, logrando impedir su línea de producción , lo que conjuntamente lleva a una pérdida de tiempo y de dinero, pero que de ninguna manera se verifica un daño de tipo tutelado, y la reparación de este debe ser por medio civil, tatamente diferente al derecho Penal”.

Continuando con el análisis de las legislaciones damos un paso a la de Chile que tiene una ley a los delitos informáticos que la van renovando de manera constante, y en la cual el delito informático es considerado toda acción típica, antijurídica y culpable realizada por medios informáticos, o cuya acción busque modificar los datos un dispositivo informático, este concepto trata de hacer una descripción general de estos delitos, incluyendo el uso de los medios informáticos y su modificación, y engloba

las dos acciones que se ejecutan al cometer este tipo de delitos; se utiliza el medio o se busca modificar (cualquier aspecto de alteración, o transformación de algo).

Por su parte Perú también cuenta con su propia Ley de delitos informáticas, en cambio Colombia tiene dos años de contar con un tipo de Ley de esta índole. Díaz García, opina al respecto, que se excluyeron tipos tan importantes como la falsedad informática, el espionaje informático, el spam, y le modificaron el epígrafe a la estafa informática por transferencia no consentida de activos.

“En algunos países se ha hecho seguimiento de manera específica en este sentido y por esta razón se ha logrado obtener equipos especializados y experiencia como es el caso de La Oficina de Investigaciones especiales de las Fuerzas Aéreas de Estados Unidos lo afirma Cristina Vallejo”, a este le agrega otro, que es el Centro de Investigaciones de la Internet de Australia, integrado por oficiales de la Ley y peritos con avanzados conocimientos de la informática.

El Continente Europea específicamente España, se dispone de un marco legal, regulado para los ámbitos, civil, penal y laboral. En su Código Penal, citado por Cifuentes Mateos, “en que hace referencia que pese a no tener un título específico para Delitos Informáticos, en las categorías de tipos penales se ubica la utilización de medios informáticos y contra medios informáticos y se describe los delitos contra:

La confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (hacking)

- Delitos Informáticos (falsificación y fraudes)
- Delitos relacionados con el contenido (pedofilia, amenazas, y racismo)

- Delitos relacionados con infracciones de la propiedad intelectual y derechos ajenos".

Por otro lado Hernández Delgado describe que la protección de datos personales sin duda, constituye una prioridad jurídica, que esta estructura bajo el derecho fundamental denominado Habeas data, que funciona para que no se comparta la información íntima, y para que la misma pueda corregirse, actualizarse o modificarse en todo momento.

"Por otra parte en el Congreso de la Naciones Unidas, cuyo objetivo fue el establecimiento de acciones más eficaces más coordinadas y concertadas entre los Estados miembros de la Naciones Unidas, en el cual se trató el tema de «Estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo" en un mundo en evolución», según decisión de la Asamblea General de las Naciones Unidas; de donde tomamos el considerado III, que nos manifiesta lo siguiente:

"Actualmente, la elaboración de leyes sobre el delito cibernético tiene lugar principalmente a nivel nacional y regional. A diferencia de lo que ocurre con las normas técnicas utilizadas en los procesos de transferencia de datos, que son las mismas en todas partes del mundo, hasta la fecha no se ha hecho nada para armonizar la legislación sobre el delito cibernético a nivel mundial".

Es por este motivo de la transnacionalidad de estos delitos que se convierten en difíciles de investigar y a la vez de realizar diligencias jurídicas fuera de nuestra nación. Como consecuencia fundamental de soberanía nacional, por el cual no se puede realizar investigaciones dentro de territorios diferentes a los nuestros, sin previa autorización de las autoridades locales, se deduce que una cooperación mutua entre

países es sumamente importante para combatir ese tipo de delitos cibernéticos. Otro de los aspectos relevantes de delitos que de cierta manera frenan las investigaciones, es la rapidez con la que se los comete, pues en el caso de un correo electrónico, tarda unos pocos segundos en llegar a diferencia de los delitos comunes que por su tiempo de ejecución, pueden dar la oportunidad de detectarlo e impedirlo.

Luego de haber profundizado de cierta manera en campo del delito informático, podemos citar la definición que nos da Hernández Díaz en la que nos dice: no ha resultado fácil; por ello en la actualidad niega un sector de la doctrina la existencia de este concepto; y, con ello, esta tipología delictiva, se prefiere utilizar para abarcar todo este conjunto de comportamientos que tienen que ver con la informática, de uno u otro modo: “Delincuencia informática”, “Criminalidad Informática” o, simplemente, en plural “Delitos Informáticos”.

Para Pérez Peña “el hecho de entrar en la llamada Sociedad de la Información, las modernas tecnologías que se utilizan para las telecomunicaciones ha sido la principal amenaza a la hora de proteger la vida íntima de las personas. Este amplio desarrollo de las TIC’S, además de erigir “la información” como un nuevo valor económico o bien de capital, ha incentivado el uso de nuevas herramientas para cometer infracciones tradicionales en formas “no tradicionales”. A través de ello se han afianzado los graves rezagos de seguridad informática en el país, transformando las antiguas conductas delictuales en la ahora llamada “ciber-delincuencia” y revelando la incapacidad experimentada por las normas establecidas en el derecho clásico”.

En cuanto a los términos utilizados para definir la problemática, en la literatura en lengua española se ha ido imponiendo la expresión de delito informático, que, según el Profesor Casabona: “…tiene la ventaja de su

plasticidad, al relacionarlo directamente con la tecnología sobre o a través de la que actúa. Sin embargo en puridad no puede hablarse de un delito informático, sino de una pluralidad de ellos, en los que encontramos como única nota común su vinculación de alguna manera con los computadores, pero ni el bien jurídico protegido agredido es siempre de la misma naturaleza ni la forma de comisión del hecho delictivo o merecedor de lo que presenta siempre características semejantes... el computador es en ocasiones el medio o el instrumento de la comisión del hecho, pero en otras es el objeto de la agresión en sus diversos componentes (el aparato, el programa, los datos almacenados). Por eso es preferible hablar de delincuencia informática o delincuencia vinculada al computador o a las tecnologías de la información."

Jacopo Gamba los generaliza y los agrupa bajo otras denominaciones más amplias "la delincuencia informática se puede definir en un sentido amplio, como todo delito que implique la utilización de las tecnologías informáticas." Pérez Luño, en cambio los define como "conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistema informáticos."

Cámpoli, diferencia entre delito informático y delito electrónico, definiendo los primeros como aquellos realizados con el autor o con el auxilio o utilizando la capacidad de los sistemas informáticos para garantizar su anonimato o impunidad territorial, pero se puede tener tipos penales específicos en algunas legislaciones, definidos con anterioridad en la aparición de nuevos sistemas de información y telecomunicaciones; y a los electrónicos, como aquellos que sufren de las nuevas tecnologías aplicadas y tienen como objeto material el delito expresamente de las mismas, por regla general no posee definiciones de tipos posibles de ser aplicables por estar referidos a bienes y conceptos inexistentes a la sanción de las leyes penales.

Stephanie Perrin nos ayuda a aclarar, en un artículo escrito por esta especialista canadiense en el 2006, el concepto de delito informático. El término se logró acuñar a finales de los años noventa a medida que crecía la Internet. Al fundarse el ya bien conocido G-8 (actualmente sustituido por el G-20), se utilizó el término de manera muy imprecisa, para describir los tipos de delitos perpetrados mediante utilización de Internet o de las nuevas redes de telecomunicaciones. Obando en cambio nos dice que: “En general se considera delito informático aquellas conductas ilícitas susceptibles de ser perseguidas efectivamente, en sede judicial, con base en tipos previamente definidos por la normativa penal, general o especial, que hacen uso inadecuado de cualquier medio informático”. Repetimos que es un delito complejo, el cual en un primer momento los países iberoamericanos intentaron ajustar a figuras penales conocidas como el robo, hurto, fraude, estafa.

En el código penal Ecuatoriano, la Ley de Comercio Electrónico, firmas electrónicas y Mensajes de Datos, extiende la justificación en el sentido del uso de sistemas de información y de redes electrónicas, incluida la importancia para el desarrollo del comercio, de los servicios electrónicos que se generan por y a través de los medios electrónicos; de la necesidad de normarlos, de regularlos y controlarlos mediante la expedición de una ley especializada y de la urgencia de contar con herramientas jurídicas que le permitan el uso de servicios electrónicos, incluido el comercio electrónico, no menciona el concepto de delito informático, más bien, pueden ser una especie de bumerang para la parte actora, porque bien puede argumentarse contrariamente que se ha violado ciertos derechos fundamentales. “Pese a que la Ley de Comercio Electrónico recoge algunas disposiciones sobre el manejo de información electrónica, en el Ecuador los delitos informáticos no están tipificados ni sancionados en el Código Penal, según indicó Santiago Acurio, Ex director de tecnologías de la información de la Fiscalía.”

Explicó que en casos de interceptación de datos existe la opción de recurrir a preceptos constitucionales que rechazan la violación al derecho de la intimidad de la persona, incluida la correspondencia virtual.

El derecho Informático cumple un rol muy importante en la prevención del problema y en la solución de los mismos, generado por el uso de los medios electrónicos. También facilita la incorporación de nuevas instituciones jurídicas que permitan crear confianza a quienes son usuarios de los medios electrónicos. “La problemática que representa el ciber-crimen, haciendo referencia a todo lo que tiene que ver con delito informático y sus nocivos efectos como lo afirma Landa Durán”, y pueden llegar incluso devastadores para la economía de cualquier país del mundo, tomando en cuenta que la delincuencia en la actualidad cuenta con la tecnología más moderna y sofisticada, razón por la cual constituye una amenaza latente para la humanidad.

El campo de Derecho es extenso y complejo, debido a que en la actualidad se produce demasiada información diaria que es difícil tratar de controlarla. Según Verónica Cepeda, para quien la toma “como una decisión jurídica, sea que esta se exprese como una norma jurídica, sentencia judicial, informe en derecho, investigación jurídica o sea respuesta a una consulta legal, requiere largas horas de recopilación de información utilizando herramientas informáticas adecuadas, sin las cuales crecerá de validez y eficacia, además que son difíciles de conseguirlos”.

“Los problemas jurídicos que se plantean a raíz de las actividades técnicas, tecnológicas y en el ciberespacio, son de variada naturaleza, aclara la Academia de Ciencias Policiales de los Carabineros de Chile, y menciona que muchos de ellos, al orientarse exclusivamente al espacio, proviene del uso de nombres identificatorios de los servidores que chocan

con derechos de propiedad industrial previamente adquiridos, como las marcas comerciales registradas". Otros problemas descritos pueden ser al publicar información por la red que puede afectar la honra de personas, derechos de la propiedad intelectual o que apoye actividades absolutamente prohibidos como la pornografía, apuestas, actividades bancarias sin consentimiento, etc.

Por último toda la problemática que proviene del comercio electrónico realizado a través de estos medios, tales como la formación del consentimiento, la prueba de los contratos, la legislación y la jurisdicción aplicable a dicha actividad, las consecuencias fiscales, etc.

Criminalización.

Si hablamos de criminalización debemos tomar en cuenta que para la mayoría de personas está tarea no es muy compleja y que se va perfeccionando, sin antecedente alguno. Sin embargo es necesario aclarar que esta labor desde sus inicios, cuando el hombre comenzó a limitarse para el buen convivir en grupo, ha traído consigo un sin número de conflictos. Está razón nos hace centrarnos y afirmar que la criminalización no puede ser un producto histórico, ni mucho menos, improvisaciones de inspiraciones de un momento específico.

"Entonces podemos afirmar un gran problemática que presenta la criminalización la ausencia de reglas obligatorias de criminalización y al mismo tiempo la necesidad de reglamentar ciertos principios orientados de la criminalización." La criminalización no debe servir con pretexto de la solución de un problema, es por esta razón que debemos tener en cuenta lo siguiente.

¿Qué debemos criminalizar?

En este concepto lo que se puede sintetizar que lo que se puede llegar a criminalizar es el comportamiento humano, aclarando que no todo

comportamiento tiene que ser susceptible de criminalización; para lo que se debe tomar en cuenta los siguientes factores:

- El hombre exige un mínimo de seguridad jurídica para supervivir y desarrollar sus actividades en beneficio de la sociedad y de él mismo.
- Tener cuidado en criminalizar los comportamientos que pueden lesionar los bienes jurídicos, debido a que el Estado no puede atomizar la criminalización de forma tal que provea hasta la última y más íntima conducta que pueda afectar al indicado bien.

¿Cuándo se debe criminalizar?

Aquí afrontamos un problema difícil de resolver, cuando se debe determinar la criminalización; entonces podemos decir, que la intervención de leyes penales debe surgir cuando por las circunstancias sociales imperantes, sea necesaria. Las mismas que pueden ser de carácter objetivo subjetivo; en las primeras el Estado se ve obligado a criminalizar conductas que en tiempos normales no requieran su criminalización, mientras que en las segundas se refieren a las conductas que las sociedades adoptan, principios de vida diferentes, culturas distintas y nuevas reglas de conductas.

¿Cómo se debe criminalizar?

Este aspecto comprende el origen Institucional de la Ley penal y la forma como debe surgir, en las cuales además de las leyes penales se han involucrado los reglamentos y ordenanzas que contienen descripciones de comportamientos antijurídicos. Estas leyes deben surgir del criterio democrático, con la finalidad de que no sean atentatorias a los derechos humanos, tampoco se debe criminalizar una conducta en forma retroactiva.

¿Para qué se debe criminalizar?

Esto se refiere a la finalidad de la criminalización, tratando de garantizar a la sociedad un mínimo de seguridad jurídica, para el desarrollo y progreso de la misma.

La Penalización.

La penalización no debe jamás fundarse exclusivamente sobre el deseo de hacer dominante una concepción moral determinada al sujeto de un comportamiento determinado; La penalización no debe jamás tener por objeto primordial la creación de un cuadro dirigido a ayudar o a tratar a un delincuente (en potencia) en su propio interés."

En cuanto a lo que tiene que ver con la penalización en nuestro País con respecto a los delitos informáticos, por ser conductas de la nueva generación, se encuentran en un proceso de evolución y estudios social, ya que algunas de éstas penalizaciones no están a la par o no son proporcionales con el daño que hoy causan a los derechos de los ciudadanos.

Judicialización

Al referirnos a este término, tratamos de adentrarnos al tema de cómo aplicar las leyes, y el momento en que debe intervenir el órgano jurisdiccional penal, es decir se debe prever el largo proceso de la judicialización de la conducta criminalizada, ya que se puede afirmar que es el único camino previsto para la legal imposición de la pena.

El Tipo Penal.

ENRIQUE BACIGALUPO: "El tipo penal es la descripción de la conducta prohibida por una norma". Y agrega "el tipo penal es el conjunto de elementos que caracteriza a un comportamiento como contrario a la norma.

LA AUTORA SOVIETICA N. Kusnetsova, citada por el profesor Baquero Vernier, “la mayoría de los penalistas entiendo al tipo penal como los rasgos objetivos y subjetivos que según la ley penal caracterizan la conducta socialmente peligrosa como delito.”

Es la descripción de los elementos objetivos y subjetivos del delito, en donde el legislador toma de las conductas humanas sus elementos los mismos que pueden producir daño o peligro quedando este descrito en la norma penal para ser sancionado.” Es un poco difícil describir un tipo penal informático, pues estas conductas no cuentan un patrón que las identifique plenamente, por lo se tiene que acudir a técnicas informáticas que puedan generar el comportamiento de este tipo de individuos llamados cyber-delincuentes, y se los pueda identificar de manera segura.

Funciones del Tipo Penal.

Francisco Muñoz Conde y García Arán, para estos estudiosos el tipo tiene tres funciones:

a) Selecciona los comportamientos humanos penalmente relevantes

b) Función de garantía en la medida que sólo los comportamientos subsumibles pueden ser sancionados penalmente.

c) Función motivadora general: por cuanto con la descripción de los comportamientos en el tipo penal el legislador indica a los ciudadanos que comportamientos están prohibidos y espera que con la conminación penal contenidos en los tipos, los ciudadanos se abstengan de realizar estas conductas.

Elementos del Tipo Penal.

Dentro de los elementos del tipo penal se encuentran los siguientes:

Tomando un ejemplo en el ámbito de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; identificaré a continuación los elementos de tipo penal informático:

“Art. 62.- A continuación del Art. 553, añádanse los siguientes artículos innumerados: "Art. ....- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. ....- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

- Inutilización de sistemas de alarma o guarda;
- Descubrimiento descifrado de claves secretas o encriptadas;
- Utilización de tarjetas magnéticas o perforadas;
- Utilización de controles o instrumentos de apertura a distancia; y,
- Violación de seguridades electrónicas, informáticas u otras semejantes."

Objetividad jurídica o bien protegido

Son los bienes jurídicos que se protegen como son la vida, estado, la integridad corporal de las personas, patrimonio, agrupando los delitos en el Código Orgánico Integral Penal. En el artículo citado como primer elemento del tipo penal que está sancionado por esta ley y el Código Orgánico Integral Penal es el patrimonio.

Marco Jurídico

El derecho a la comunicación e información en la Constitución de la República del Ecuador

En nuestra Constitución de la República existen derechos y garantías que son protegidos, a estos les llamamos derechos fundamentales establecidos en nuestra carta magna, por lo que en el tema que estoy tratando se encuentran varios derechos tipificados de los cuales el más alto deber del Estado es respetar y hacer respetar los derechos garantizados en la Constitución.

Ambiente Sano Art. 15
Comunicación e información Art. 16. Nº 1, 3, 5; Art. 17 Nº 1, 2, 3; Art. 18. Nº 1, 2; Art. 19; Art. 20.
Cultura y ciencia Art. 23; Art. 25.
Niños, Niñas y Adolescentes Art. 46. Nº 4, 7
El legislador se refiere a las medidas que el estado debe tomar frente a programas de difusión que atenten contra la integridad psíquica y física de los niños, niñas y adolescentes, con la finalidad de que los mismos no vayan a influenciar en un futuro en la forma de ser, en cómo deberían actuar o que decisiones deberían tomar.

Personas con discapacidad

Art. 47. Nº 11… Aquí se refiere las medidas que se adoptaran para proteger a las personas discapacitadas que tengan algún problema de comunicación para lo cual el estado coordinara con algunos sectores u organismos para facilitar la comunicación y como se habla de la tecnología en el futuro existirán algunos procedimientos con mayor avance para comunicarnos entre todos y poder entender al discapacitado.

Derechos de las comunidades, pueblos y nacionalidades

Art. 57. Nº 11, 21. La mejor forma de que se conozcan todas las costumbres de una nacionalidad, pueblo, comunidad es dándolo a conocer por medio de los avances tecnológicos en este caso a través de los sistemas de redes quienes son los encargados de transportar y difundir las costumbres de cada grupo social, en este caso tenemos ya información en la red como es en las páginas web como google, youtube, altavista etc. los cuales en la actualidad poseen información e historia de varios grupos sociales de cómo fue su creación y evolución.

Derechos de Libertad

Art.66. Nº 4, 6, 7, 13, 21. Aquí me centraré de manera fundamental, porque los derechos que se mencionan en la constitución, en este caso en el artículo mencionado, son de total trascendencia, ya que en estos últimos tiempos hemos sido testigos de varias denuncias que llegaron a ser noticia nacional e internacional, todas estas denuncias propuestas en los diferentes organismos de control a nivel mundial, en nuestro caso en la Fiscalía, llegaron a establecer un antecedente por cuanto las informaciones vertidas por varios medios de comunicación no fueron probadas conforme a derecho, ya que no se podían dar con sus autores por la razón de que se trataba de delitos cometidos por medio de los instrumentos tecnológicos que hoy en día están al alcance de todos, esto con lleva perjuicios al estado y en especial a las personas quienes son víctimas de estos ciberdelincuentes y que también por la falta de preparación o capacitación técnica de los administradores de justicia dejaron impunes algunas denuncias, también fue producto de que nuestra sistema de leyes carecía de la tipificación de algunas conductas contrarias al buen vivir, ahora en nuestro anteproyecto de código penal, se está reformando y tipificando algunas conductas que se cometen con las tecnologías de la información y comunicación “TIC”, por lo que es deber

de los asambleístas adecuar las conductas realizadas por el hombre a través de los herramientas tecnológicas a estos tipos penales, caso contrario la honra de las personas, el patrimonio se vería afectado y más aún quedaría esto impune.

Medios alternativos de solución de conflictos Art. 190.
Soberanía alimentaria Art. 281. Nº 3, 8, 9.
Sectores estratégicos, servicios y empresas públicas Art. 313; Art. 314; Art. 317.
Tipos de propiedad Art. 321; Art. 322
Formas de trabajo y su retribución. Art. 326. Nº 15

Delito informático en la Declaración Universal de Derechos Humanos

La Declaración Universal de Derechos Humanos son normas que se encuentran establecidas por acuerdo de los países que suscribieron convenios para garantizar la efectiva práctica de los derechos fundamentales de las personas, en donde los firmantes están en la obligación de responder cuando los derechos establecidos sean vulnerados por cualquier institución ya sea en el orden público o privado, es que así fue creado este instrumento, para garantizar su fiel cumplimiento por los estados, fue instituida el diez de diciembre de mil novecientos cuarenta y ocho, por la Asamblea General, reunida en París – Francia.

Debo aclarar que ahora con el origen de nuevas conductas delictivas hace falta hacer reformas para adecuar varias conductas creadas por el hombre, y así queden ya tipificadas para prevenir su impunidad, tomando en cuenta que estos delitos se han convertido en figuras delictuosas trasnacionales y que cada vez es más difícil su prevención y erradicación por su acentuación en el mundo de la tecnología e información, entre los derechos a los que me refiero están los llamados delitos informáticos, que

en algunos articulados de la DDHH, se encuentran pero no en la magnitud con la cual se cometen los delitos en la actualidad. Uno de los delitos que se encuentran en este cuerpo de leyes son los siguientes:

Art. 12. CRE. ART.66 Nº 18, 19, 20, 21, 22
La Declaración de Derechos Humanos es muy clara en el sentido de que nadie podrá ser objeto de injerencias arbitrarias en lo que tiene que a cualquier medio de comunicación e información, por los que los estados firmantes están en la obligación de respetar y hacer prevalecer estos derechos, salvo que sea a petición de autoridad judicial, y que no vulnere ningún otro derecho protegido en las legislaciones internas como en este convenio. Art. 17. Nº1, 2. CRE. ART. 66 Nº 26.

Este es un derecho por el cual todas las personas tienen la garantía de adquirir cualquier beneficio y hacer propietarios del mismo conforme estén regulados las normas internas y políticas públicas de cada estado miembro, tan solo se podrá cambiar esta situación cuando estén afectando al medio, y no estén cumpliendo la función social para la cual se creó.

Declaración Americana de los Derechos y Deberes del Hombre

Art 4; Art 5. CRE. ART.66 Nº 18, 19, 20, 21, 22; Art 10; Art 13.
Toda persona tiene el derecho de participar en la vida cultural de la comunidad, gozar de las artes y disfrutar de los beneficios que resulten de los progresos intelectuales y especialmente de los descubrimientos científicos.

Tiene asimismo derecho a la protección de los intereses morales y materiales que le correspondan por razón de los inventos, obras literarias, científicas y artísticas de que sea autor. CRE. ART. Nº 24

Los estados firmantes del convenio garantizan la propiedad en todas sus formas, y dan la oportunidad a que todos los miembros de la sociedad participemos de manera libre y responsable de los beneficios científicos en este caso tecnológicos lleguen a cada sector en forma equitativa.

El Pacto Internacional de Derechos Civiles y Políticos

El Pacto Internacional de los Derechos Civiles y Políticos fue adoptado en el seno de las Naciones Unidas el 16 de diciembre de 1966 junto al Pacto Internacional de los Derechos Sociales, Económicos y Culturales, bajo la finalidad de hacer de estos derechos una obligación jurídica vinculante para todos los estados, puesto que la Declaración Internacional de los Derechos Humanos no era respetada por las naciones y se la tenía como un mero enunciado, sin embargo en 1976, estos dos Pactos entraron en vigor tras la ratificación de un número suficiente de Estados.

Art 19.- Nº 1, 2, 3 a), b) El Pacto Internacional de los Derechos Civiles y Políticos, con llevó a que se instituya las normas jurídicas internacionales que describan afirmativamente los elementos integrantes del derecho a la libertad de expresión y de opinión, en la cual, se garantice a que este derecho sea respetado por el Estado y por los particulares para su máxima expresión y únicamente se aplican algunas restricciones dirigidas a garantizar la buena reputación de las personas, la seguridad nacional y el orden público.

Los tipos penales que criminalizan el delito informático en el Código Penal.

Para empezar nuestro país es un Estado independiente, democrático y sobre todo soberano, con las capacidades y las facultades plenas de sancionar delitos de cualquier índole, incluidos en los mismos estos actos delictivos de la rama de la informática; con la finalidad de garantizar a todos sus ciudadanos seguridad, como también al derecho de vivir en una

sociedad democrática y ante todo libre de corrupción, siendo estas razones suficientes para incluir en estos derechos, los de utilizar las herramientas tecnológicas que están a nuestro alcance, respetando los límites del uso de los mismos, respetando a su vez el derecho de los demás.

Sin embargo nuestros Códigos necesitan de una reestructuración que sea capaz de abarcar algunas de estas conductas que aún no están tipificadas, o de alguna forma tienen falencias que no permiten garantizar los derechos de las personas de manera eficaz.

Principios básicos del peritaje.-

a) Objetividad.- al observar el código de ética profesional para cualquier investigación.

b) Autenticidad y Conservación.- todos los medios que obtienen evidencias digitales tiene que ser conservados y mantener su autenticidad e integridad, caso contrario no tendrían valor probatorio.
c) Legalidad.- la actuación del perito está basada en el conocimiento de la legislación pericial, para poder observar, opinar y dar resultados.
d) Idoneidad.- las evidencias probatorias tiene que ser auténticos, relevantes y suficientes para el caso.
e) Inalterabilidad.- obligación de los peritos o los encargados de conservar las evidencias cumplir con lo dispuesto al principio de cadena de custodia.
f) Documentación.- toda pericia practicada deberá constar por escrito y en físico los pasos dados en el procedimiento pericial. Reconocimiento de la evidencia digital.- el rol que desempeña cada sistema informática determina: DONDE DEBE SER UBICADA Y

COMO DEBE SER USADA LA EVIDENCIA DIGITAL, para lo que se han aclarado anteriormente.

HARDWARE

Hardware (elementos físicos), está es una mercancía ilegal: por no estar autorizada por la ley como los decodificadores. Fruto del delito: cuando se lo obtiene por medio de robo, hurto; Hardware es un instrumento: cuando es usado para interceptar comunicaciones;

Hardware es evidencia: porque es un elemento físico cuando se constituye como prueba en la comisión de un delito por ejemplo scanner cuando se utiliza en la comprobación de algunas características, las que posee son únicas.

INFORMACIÓN

La información es mercancía ilegal: cuando su posesión no es permitida por la ley, ejemplo, Pornografía infantil. La información es fruto del delito: cuando es el resultado de la comisión de una infracción, ejemplo: Copias pirateadas de un programa de ordenador, secretos industriales robados.

La información es un instrumento: cuando es usada como medio para cometer una infracción penal, ejemplo, programas de ordenadores para romper las seguridades de un sistema informático, romper contraseñas o para brindar acceso no autorizado.

Su papel es importante en el cometimiento de un delito.

La información es evidencia: es la más grande y nutrida de todas las anteriores, por la razón de que nuestras acciones diarias dejan un rastro digital, se consigue mucha información como evidencia, ejemplo, la

información ISP´s, de los bancos, y de las proveedoras de servicios las cuales pueden revelar actividades particulares de los sospechosos.

Clases de equipos informáticos y Electrónicos

a) Sistemas de computación abiertos, son las llamadas computadoras personales y todos sus elementos como son los ratones, teclado, portátiles monitores y los servidores. Lo que los convierte en una fuente digital de gran almacenamiento.

b) Sistemas de computación, están compuestas por las redes de telecomunicaciones, inalámbrica, internet, contiene gran información y evidencia digital.

c) Sistemas convergentes de computación, son los que están formados por los teléfonos celulares llamados inteligentes o Smartphones, los asistentes personales digitales PDAs, las tarjetas inteligentes y cualquier otro aparato electrónico que posea convergencia digital y que pueda contener evidencia digital.

Un investigador entrenado puede identificar a los delincuentes por sus actuaciones ya sea en su conducta, haciendo un perfil, identificando las actividades que realiza y cuáles son sus víctimas.

Ejemplos de aparatos electrónicos o informáticos:

Computador de escritorio, portátil, estación de trabajo, Hardware de red, Servidor (aparato que almacena o transfiere datos electrónicos por el internet), teléfono celular, inalámbrico, identificador de llamadas, localizador o beeper, “GPS” aparato que ubica geográficamente a la persona o vehículo que lo opera, cámaras, videos, sistemas de seguridad, memoria flash (pequeño dispositivo que puede conservar hasta 128 gigabytes de información); impresora, copiadora, grabadora, videograbadora, DVD, duplicadora de discos decodificadores, aparatos

que capturan número de celulares cercanos para después copiarlos en otros teléfonos, etc. aparatos electrónicos: teléfonos inalámbricos, celulares, Smartphones.

Incautación de Equipos informáticos o electrónicos.- todo agente investigador que presumiera que con un aparato informático o electrónico existe evidencia digital con la que se cometió un delito, tiene que pedir la autorización judicial para su incautación como para acceder a los datos guardados y generados por el aparato, teniendo en cuenta:

- La hora en que debe realizar: esto con la finalidad de que no se pueda destruir los equipos, datos por parte del sospechoso, y para tener mayor seguridad de los investigadores.
- Entrar sin previo aviso: con la finalidad de utilizar seguridad, evitar destrucción y alteración de los equipos, o la evidencia contenida en ésta.
- Materiales previamente preparados (cadena de custodia): embalajes de papel, etiquetas, discos y disquetes vacíos, herramienta, cámara fotográfica.
- Realizar simultáneamente los allanamientos e incautación en diferentes sitios: por la razón de que los datos pueden estar en más lugares, sistemas de red, conexiones remotas; examen de equipos, aparatos no especificados en la orden de allanamiento.
- Creación de respaldos en el lugar, creación de imágenes de datos: Autorización para duplicar, reproducir datos encontrados por ejemplo, un aparato contestador, fijar/grabar la escena, cámaras, videos, etiquetas, códigos, claves de acceso/contraseñas, buscar documentos que contienen información de acceso, conexiones en redes, y cualquier otro tipo de consideración especial (consideraciones de la persona involucrada: médicos, abogados información privilegiada).

La falta de la autorización judicial puede terminar con la exclusión de los elementos probatorios por violación a las Garantías Constitucionales.

En la escena del delito y la responsabilidad de los investigadores.-

- OBSERVE Y ESTABLEZCA LOS PARÁMETROS DE LA ESCENA DEL DELITO: tiene que establecer si el delito está todavía en progreso, tomar nota de las características físicas del área circúndate, extendida a todo sistema de información o red que se encuentre dentro de la escena.
- **INICIE LAS MEDIDAS DE SEGURIDAD:** tomar todas las prevenciones necesarias para evitar cualquier riesgo eléctrico, químico o biológico, como las actividades criminales, por la razón de correr algún peligro las personas encontradas en la escena.
- **FACILITE LOS PRIMEROS AUXILIOS:** precautelar la vida de las posibles víctimas del delito como es el cuidado médico adecuado al personal de emergencias y el de preservar las evidencias.
- **ASEGURE FÍSICAMENTE LA ESCENA:** retirar a todas las personas extrañas a la misma, el objetivo principal es prevenir el acceso no autorizado de personal a la escena, evitando la alteración de la evidencia o su posible contaminación.
- **ASEGURE FÍSICAMENTE LAS EVIDENCIAS:** aquí aplican los principios de recolección de evidencias de una forma práctica, como también cumplir con el principio de cadena de custodia, el cual es realizado por personal entrenado en manejar, guardar y etiquetar evidencias.

- **ENTREGAR LA ESCENA DEL DELITO:** una vez cumplidas las etapas enunciadas deben entregarse a las respectivas autoridades para su cargo, dependiendo si éstas son administradoras de las redes o quedarán a cargo de la fiscalía, esto una vez que se determine la naturaleza del delito.

- **ELABORAR LA DOCUMENTACIÓN DE LA EXPLOTACIÓN DE LA ESCENA:** esto con la finalidad de tener una bitácora de todas las etapas que se siguieron para determinar y tener un respaldo de todos los hechos que se siguieron durante la investigación y recolección de evidencias.

La reconstrucción de la escena del delito.- ésta permite que el investigador comprenda todos los hechos relacionados con el cometimiento de la infracción, usando evidencias disponibles, permitiendo tres formas de reconstrucción a saber:

1. Reconstrucción Relacional, se hace en base a indicios que muestran la correspondencia que tiene un objeto con la escena del delito y su relación con los otros objetos presentes. Se busca su interacción en conjunto o entre cada uno de ellos.
2. Reconstrucción Funcional, se hace señalando la función de cada uno objeto dentro de la escena y la forma en que estos trabajan y como son usados.

3. Reconstrucción temporal, se hace con indicios que nos ubican en la línea temporal del cometimiento de la infracción y en relación con las evidencias encontradas.

Qué hacer al encontrar un dispositivo informático o electrónico.

- Usar guantes de hule, caso contario desaparece las huellas dactilares o adánicas existentes en el equipo o en el área donde se encuentra residiendo el sistema informático.
- Asegurar el lugar, los equipos de cualquier tipo de intervención física o electrónica hecha por extraños.
- Si no está encendido, no lo encienda (para evitar el inicio de programas de autoprotección).

- Si esta encendido, no lo apague inmediatamente (para evitar la pérdida de información volátil).
- Si se cree que el equipo electrónico o informático está destruyendo las evidencias desconectarlo inmediatamente.
- Si es posible llamar un técnico.

En caso de no existir técnico:

- Si está encendido no apagarlo inmediatamente.
- Si tiene “Mouse” moverlo cada minuto para evitar que la pantalla se cierre o se bloqueé.
- Si el aparato está conectado a una red anote los números de conexión IP.
- Fotografié la pantalla, las conexiones y cables.
- Si la computadora portátil no se apaga cuando es removido el cable de alimentación, localice y remueva la batería, situada debajo del equipo, tiene un botón para liberar la batería, guardar en otro lugar para prevenir el incendio de la misma.
- Usar bolsas especiales antiestáticas para almacenar diskettes, discos rígidos, y otros dispositivos de almacenamiento informáticos que sean de electromagnéticos (bolsas de papel, madera). No usar bolsas plásticas, porque puede causar una descarga de electricidad estática que puede destruir los datos. Etc.
- Si está en una estación de trabajo (conectado en red) al desconectar asesorarse de un técnico ya que puede acarrear responsabilidad, para la policía judicial, y la fiscalía o puede producir un daño permanente, una interrupción ilegal del negocio.
- En los teléfonos celulares se puede encontrar evidencia como: números llamados, guardados en la memoria del teléfono, direcciones, números personales de identificación (PIN) ETC.

Rastreo del correo electrónico (permite el envío de cartas escritas a través del computador a otras personas que tengan acceso a la red en todo el mundo).

- La computadora identifica una serie de números al sistema del proveedor de servicio de internet conocidos como (ISP).
- Enseguida se asigna la dirección (IP), y
- Es divido en paquetes pequeños de información a través del protocolo (TCP/IP)
- Los paquetes pasan por una computadora especial llamada servidor (server),
- Que los fija con una identificación única (mesage - ID)
- Posteriormente los sellan con la fecha y hora de recepción (sello de tiempo)
- Más tarde al momento del envío se examina su dirección de correo para ver si corresponde la dirección IP de algunas de las computadoras anotadas en una red local (dominio)
- Si no corresponde, envía los paquetes a otros servidores, hasta que encuentra al que reconoce la dirección como una computadora dentro de su dominio, y los dirigen a ella, es aquí donde los paquetes se unen otra vez en su forma original a través del protocolo TCP/IP. (Protocolo de transferencia y protocolo de internet)
- Siendo visible su contenido a través de la interface gráfica del programa de correo electrónico instalado en la máquina destinataria.

Hay que tomar en cuenta que los correos electrónicos se mantienen sobre un servidor de correo, y no en la computadora del emisor o del destinatario, a menos que el operador las guarde allí.

- Al redactarlos se transmiten al servidor de correo para ser enviados.
- Al recibirlas, nuestra computadora hace una petición al servidor de correo, para que los mensajes sean transmitidos luego a la computadora del destinatario, donde el operador puede guardar, leer o cerrar.
- Al cerrar sin guardar, la copia de la carta visualizada en la pantalla del destinatario desaparece, pero se mantiene en el servidor, hasta que el operador solicita que sea borrada.
- Los rastros se graban en el encabezamiento del email recibido, la cual está determinada por el proveedor de servicios de internet utilizado por nuestra computadora o la de quien recibe el correo electrónico, algunos ejemplos TO, FROM, CC, FÁCILES O SINO OTROS MÁS DIFÍCILES COMO ESTOS: IP 148.235.52.34 o messge-id:

El delito informático en la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos.

DE LAS INFRACCIONES INFORMÁTICAS

Art 58.....- 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, será sancionada 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 realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, estas 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.

Art. ....- 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".

Este delito en específico lo encontramos en el capítulo V que se refiere a los delitos contra la inviolabilidad del secreto, dentro del Título II de los delitos contra las garantías constitucionales y la igualdad racial, comprendido a su vez en el libro II de los delitos en particular. El secreto protegido es el secreto, garantizado en nuestra Constitución de la República en el artículo 66 nº21 esta es una característica de carácter ideológico y estructural, ayuda a que la vigencia de este derecho reconocido por los legisladores en la actualidad sea de inmediata y directa aplicación por parte del estado y todas las autoridades al servicio público y privado, en este caso ya se ve concebida en el destino de nuestro derecho penal, como tiene su incidencia y como va afectando a nuestros derechos a través de las tecnologías de la información y comunicación, y el uso no autorizado por parte de las personas de información privada, y

como tienen la obligación las instituciones de cumplir y acatar las normas constitucionales, sin alegar falta de norma para vulnerar derechos y garantías constitucionales.

En el primer inciso de las reformas artículo 202.1 el sujeto activo del delito es cualquier persona; el sujeto pasivo son las personas naturales o jurídicas; su núcleo es violentar claves o sistemas de seguridad; su objeto es vulnerar el secreto, confidencialidad, y reserva; el medio empleado puede ser cualquier máquina electrónica, informática o afín poniendo en peligro información reservada.

En el segundo inciso el sujeto pasivo es el estado o mejor dicho las instituciones estatales porque ya lo realiza con intención de causar daño o perjudicar a todo un estado cuya sanción por su alto riesgo es mayor.
El tercer inciso trata sobre su divulgación de secretos comerciales aquí se hace más rigurosa la pena, por la razón de que conocimientos propios pueden perjudicar la situación económica de una empresa y más aun llegando a poner en conocimiento de la competencia.

En cambio en el cuarto inciso el sujeto activo solo es la persona encargada de guardar secretos claves o que se hallan en lugares estratégicos para el uso y control de una red siendo él, el único responsable por el perjuicio causado, ya que no estaría cumpliendo con el código de ética que todo funcionario público y profesional debería manejar. Esta es la diferencia con que el legislador sanciona a los que delinquen contra empresas y los que actúan de manera fraudulenta contra el estado.

"Art. ....- Daños Informáticos.-Concordancias: Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o

procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica".

El bien protegido es la intangibilidad de la información protegida que se encuentra dentro de los programas informáticos, tanto el sujeto activo como pasivo que es cualquier persona, su núcleo es la destrucción o alteración de la información protegida y su objetivo es desaparecer o alterar los datos contenidos en esta información, los medios empleados son virus, fuerza física, incendios; en el segundo inciso del artículo 415.1 los bienes protegidos son el servicio público y la seguridad y defensa nacional.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Entendamos primeramente qué significado tiene el comercio electrónico; según Lorenzetti “La comisión de la Unión Europea, en la comunicación denominada Una iniciativa Europea en materia de comercio electrónico, lo define como el desarrollo de actividad comercial y de transacción por vía electrónica y comprende actividades diversas: la comercialización de bienes y servicios por la vía electrónica; la distribución on-line de contenido digital, la realización por vía electrónica de operaciones financieras y de bolsas, la obra pública por vía electrónica y todo procedimiento de este tipo celebrado por la administración pública”. Con la definición clara de comercio electrónico se puede llegar a una breve conclusión de que la ley de comercio electrónico no es más que una ley especial que trata de controlar estas actividades on-line, las mismas que actualmente se encuentran en continua modificación debido a los avances tecnológicos que se dan. Está ley da pautas para poder sancionar algunos actos delictivos mediante el código penal. Las firmas electrónicas por su parte consisten en cualquier símbolo o proceso electrónico que

permita al receptor de un documento electrónico identificar, formalmente a su autor.

Mensajes de datos involucra a la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o similares (correos electrónicos, telefax, telegramas).

COIP Código Orgánico integral Penal

SECCIÓN TERCERA

Delitos contra la seguridad de los activos de los sistemas de información y comunicación.

Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Artículo 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1) La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el

interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2) La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3) La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4) La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar

de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Artículo 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1) Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2) Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Artículo 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer

gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

Legislación Comparada

Para poder dar más alternativas o soluciones de los delitos informáticos, que actualmente se cometen a nivel global, es necesario analizar y comparar varias legislaciones de otros estados en el cual ya tipifican estas conductas, y ven la posibilidad de erradicar y prevenir las mismas, por eso voy a tomar leyes de países que tengan un común denominador en las tecnologías de la información y comunicación como también hare uso de legislaciones que tengan un enfoque más desarrollado que el nuestro, entre las legislaciones a compararse tenemos el Código Penal de España, Francia, y Chile.

Las leyes se pueden enmarcar en tres tipos

- Normas que incorporan los tipos penales al código penal, es decir, reformas hechas al código penal agregando el concepto de Delito

Informático. Solución adoptada por Francia, Italia, España, Alemania y Austria, entre otros.

- Tratar los tipos penales dentro de una Ley General de Derecho Informático o una Ley de Protección de Datos Personales. Solución elegida por Australia, Canadá, Estados Unidos, Reino Unido, Japón. Crear una Ley Especial que aisladamente solo tipifique las figuras delictivas. Es el caso de Venezuela y Chile.

Legislación Española

Las normas españolas a través de su sistema penal, ha calificado algunas conductas como contrarias al orden social, en si a lo que se refiere a los delitos informáticos que hoy en día se encuentran de manera masiva alrededor del mundo, estas tipificaciones realizadas por el gobierno español son graves como las previstas en nuestra ley penal y la ley de comercio electrónico, firmas electrónicas y mensajes de datos, de esta manera, analizaré las normas existentes en dicha legislación en las cuales, constan las descripción de las conductas típicas que son sancionadas por el Código Penal.

Este país reformó su código penal el 23 de noviembre de 1995, en el cual se han introducido nuevas figuras y modalidades referentes a los delitos informáticos. Se sanciona:

- El descubrimiento y revelación de secretos vulnerando la intimidad sin consentimiento.
- El espionaje empresarial y la estafa informática.
- Pornografía infantil.
- Calumnias e injurias hechas con publicidad a través de Internet y terminales móviles.
- La fabricación o tenencia de programas destinados a la falsificación de todo tipo de documento.

- El daño de datos perteneciente a software, programas o documentos electrónicos contenidos en redes, soportes o sistemas informáticos.

Art 186.- El que por cualquier medio directo, vendiere, difundiere, o exhibiere material pornográfico entre menores de edad, o incapaces, será castigado con la pena de prisión de seis meses a un año o multa de 12 a 24 meses

Esta norma se refiere a cualquier forma de información ilegal en donde los involucrados directamente son los menores de edad y los incapaces quienes por su mismo estado de conciencia no pueden identificar la agresión de la cual pueden llegar a hacer objeto por el uso del material pornográfico. Su criminalización se basa como conducta típica en vender, difundir, o exhibir material pornográfico.
Art 189.- (Artículo redactado de acuerdo con la modificación establecida por la Ley Orgánica 15/2003, de 25 de noviembre)

1. Será castigado con la pena de prisión de uno a cuatro años:

a) El que utilizare a menores de edad o a incapaces con fines o en espectáculos exhibicionistas o pornográficos, tanto públicos como privados, o para elaborar cualquier clase de material pornográfico, cualquiera que sea su soporte, o financiare cualquiera de estas actividades.
2. El que produjere, vendiere, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición por cualquier medio de material pornográfico en cuya elaboración hayan sido utilizados menores de edad o incapaces, o lo poseyere para estos fines, a o incapaz, será castigado con la pena de prisión de tres a seis meses o multa de seis a 12 meses.

3. El ministerio fiscal promoverá las acciones pertinentes con objeto de privar de la patria potestad, tutela, guarda o acogimiento familiar, en su caso, a la persona que incurra en alguna de las conductas descritas en el apartado anterior.
4. Será castigado con la pena de prisión de tres meses a un año o multa de seis meses a dos años el que produjere, vendiere, distribuyere, exhibiere o facilitare por cualquier medio material pornográfico en el que no habiendo sido utilizados directamente menores o incapaces, se emplee su voz o imagen alterada o modificada.

5. En los casos previstos en los apartados anteriores, se podrán imponer las medidas previstas en el artículo 129 de este Código cuando el culpable perteneciere a una sociedad, organización o asociación, incluso de carácter transitorio, que se dedicare a la realización de tales actividades.

Las conductas a las que se refiere este artículo y que es criminalizado son varias como por ejemplo: El que utilizare a menores de edad o a incapaces, el que produjere, vendiere, distribuyere, exhibiere o facilitare la producción, venta, difusión o exhibición, realicen los actos, haga participar a un menor o incapaz causando perjuicio a la personalidad del mismo, el que tuviere bajo su potestad, tutela, guarda o acogimiento a un menor de edad o incapaz y que no impida la realización de sus conductas, el empleo de la voz o imagen alterada o modificada del menor o incapaz, las encontramos de manera más amplia y sancionatoria, con el objeto mismo de impedir que por cualquier medio se perpetre estos ilícitos. Nuestro Código Penal se refiere a las diferentes formas de explotación sexual en su artículo 552.2, 528.7 y siguientes

Art 197.- 1.- El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

3.- Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

4.- Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

5.- Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.
6.- Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado 5, la pena a imponer será la de prisión de cuatro a siete años.

Las formas de participación de cada individuo en la perpetuación del delito se lo castiga conforme al grado de autoría y según las persona sea esta natural o jurídica que fueran objeto de violación o que sin su consentimiento se haga uso para difundir sus datos personales y que cause prejuicio a los mismos, dentro de las conductas a las que se refieren también las encontramos en nuestra legislación pero la forma de castigar no es proporcional al daño causado.

Art 198.-La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años. Aquí encontramos ya identificado de manera directa a quien es el responsable de la conducta típica, en este caso es “la autoridad o funcionario público” siendo este el sujeto activo y el sujeto pasivo el estado, y su sanción por obvias razones son más severas por que el interés de la administración pública está en peligro.

Art 199.- 1.- El que revelare secretos ajenos, de los que tenga conocimiento por razón de su oficio o sus relaciones laborales, será

castigado con la pena de prisión de uno a tres años y multa de seis a doce meses.

2.- El profesional que, con incumplimiento de su obligación de sigilo o reserva, divulgue los secretos de otra persona, será castigado con la pena de prisión de uno a cuatro años, multa de doce a veinticuatro meses e inhabilitación especial para dicha profesión por tiempo de dos a seis años.

Toda persona que por su cargo tenga acceso a claves y tenga la obligación de mantenerlas en reserva revele o divulgue secretos será sancionado según el grado de participación y los efectos causados. Estas conductas ya criminalizadas hacen que los técnicos o los especialistas conozcan sobre el uso indebido del mismo, el articulado tiene similitud con el artículo 201, 262 de nuestro Código Penal.

Art 200.-Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este código. La reputación de las personas jurídicas está en peligro por ende ya se ve la manera cómo prevenir el traspaso de datos que merezcan y sean acreditados como confidenciales o reservados.

Art 201.- 1.- Para proceder por los delitos previstos en este capítulo será necesaria denuncia de la persona agraviada o de su representante legal. Cuando aquélla sea menor de edad, incapaz o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

2.- No será precisa la denuncia exigida en el apartado anterior para proceder por los hechos descritos en el artículo 198 de este Código, ni cuando la comisión del delito afecte a los intereses generales o a una pluralidad de personas.

3.- El perdón del ofendido o de su representante legal, en su caso, extingue la acción penal o la pena impuesta, sin perjuicio de lo dispuesto en el segundo párrafo del número 4º del artículo 130.

Las denuncias las puede presentar cualquier persona; está en la obligación el ministerio público de acogerlas e investigarlas, dependiendo de la participación y que finalidad tiene, se puede extinguir la acción penal o la pena impuesta solo con el perdón de la parte ofendida o el representante legal, según la gravedad de la conducta típica pueden ser archivadas o tramitadas de oficio.

Art 211.-La calumnia y la injuria se reputarán hechas con publicidad cuando se propaguen por medio de la imprenta, la radiodifusión o por cualquier otro medio de eficacia semejante.

Art 212.-En los casos a los que se refiere el artículo anterior, será responsable civil solidaria la persona física o jurídica propietaria del medio informativo a través del cual se haya propagado la calumnia o injuria.
Al referirse a cualquier medio de difusión ya se hace alarde de las nuevas formas de comunicación e información por las cuales las personas pueden ser objeto de violaciones a sus derechos en lo referente a la honra, al buen nombre y a la intimidad. El mismo guarda relación con el artículo 64 de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; y el artículo 606 del numeral 19 en adelante del Código Penal.

Art 238.-Son reos del delito de robo con fuerza en las cosas los que ejecuten el hecho cuando concurra alguna de las circunstancias siguientes:

1. Escalamiento.
2. Rompimiento de pared, techo o suelo, o fractura de puerta o ventana.
3. Fractura de armarios, arcas u otra clase de muebles u objetos cerrados o sellados, o forzamiento de sus cerraduras o descubrimiento de sus claves para sustraer su contenido, sea en el lugar del robo o fuera del mismo.
4. Uso de llaves falsas.
5. Inutilización de sistemas específicos de alarma o guarda.

Art 239.- Se considerarán llaves falsas:
1. Las ganzúas u otros instrumentos análogos.
2. Las llaves legítimas perdidas por el propietario u obtenidas por un medio que constituya infracción penal.
3. Cualesquiera otras que no sean las destinadas por el propietario para abrir la cerradura violentada por el reo.

A los efectos del presente artículo, se consideran llaves las tarjetas, magnéticas o perforadas, y los mandos o instrumentos de apertura a distancia.
Los diferentes tipos penales se encuentran de manera detallada en cuanto a las circunstancias por las cuales se puede cometer el delito, y nuestra norma interna también las descifra y los modos o formas con las cuales se ejecuta esta operación, por lo que la legislación española la amplía en el sentido de las tecnologías de la información y comunicación que pueden llegar a realizar y así poder criminalizar todo acto cometido por medio de las herramientas tecnológicas. Se relaciona con el articulado 553.2 de nuestro Código Penal.

Art 248.- 1.- Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2.- También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de terceros.

Art 255.- Será castigado con la pena de multa de tres a doce meses el que cometiere defraudación por valor superior a cincuenta mil pesetas, utilizando energía eléctrica, gas, agua, telecomunicaciones u otro elemento, energía o fluido ajenos, por alguno de los medios siguientes:

1. Valiéndose de mecanismos instalados para realizar la defraudación.
2. Alterando maliciosamente las indicaciones o aparatos contadores.
3. Empleando cualesquiera otros medios clandestinos.

Art 256.-El que hiciere uso de cualquier equipo terminal de telecomunicación, sin consentimiento de su titular, ocasionando a éste un perjuicio superior a cincuenta mil pesetas, será castigado con la pena de multa de tres a doce meses.

Art 263.-El que causare daños en propiedad ajena no comprendidos en otros Títulos de este Código, será castigado con la pena de multa de seis a veinticuatro meses, atendidas la condición económica de la víctima y la cuantía del daño, si éste excediera de cincuenta mil pesetas.

Art 264.- 1. Será castigado con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses el que causare daños expresados en el artículo anterior, si concurriera alguno de los supuestos siguientes:

1. Que se realicen para impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones, bien se cometiere el delito contra funcionarios públicos, bien contra particulares que, como

testigos o de cualquier otra manera, hayan contribuido o pueden contribuir a la ejecución o aplicación de las Leyes o disposiciones generales.

2. Que se cause por cualquier medio, infección o contagio de ganado.
3. Que se empleen sustancias venenosas o corrosivas.
4. Que afecten a bienes de dominio o uso público o comunal.
5. Que arruinen al perjudicado o se le coloque en grave situación económica
6. La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

La legislación española como se ve en estos artículos se ve más desarrollada llegando incluso hasta los puntos donde se enmarcan las telecomunicaciones para causar el daño, realiza un estudio sobre la pérdida económica de las personas, descifra de manera detallada a los autores del delito y el lugar donde se encuentran para causar estos agravios, pero en fin las conductas descritas y tipificadas también se relacionan con nuestro sistema penal, la ley de comercio electrónico en su artículo 63 en concordancia con el artículo 563 de nuestro Código Penal igualmente sancionan, pero no de la misma gravedad.

Art 270.-Será castigado con la pena de prisión de seis meses a dos años o de multa de seis a veinticuatro meses quien, con ánimo de lucro y en perjuicio de tercero, reproduzca, plagie, distribuya o comunique públicamente, en todo o en parte, una obra literaria, artística o científica, o su transformación, interpretación o ejecución artística fijada en cualquier tipo de soporte comunicada a través de cualquier medio, sin la autorización de los titulares de los correspondientes derechos de propiedad intelectual o de sus cesionarios.

La misma pena se impondrá a quien intencionadamente importe, exporte o almacene ejemplares de dichas obras o producciones o ejecuciones sin la referida autorización. Será castigada también con la misma pena la fabricación, puesta en circulación y tenencia de cualquier medio específicamente destinada a facilitar la supresión no autorizada o la neutralización de cualquier dispositivo técnico que se haya utilizado para proteger programas de ordenador.

Art 27.- 1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

En cuanto se refiere a la propiedad intelectual, en la protección española existe las limitaciones para quienes pueden tomar como ejemplares las investigaciones realizadas por otras personas, pero se sanciona a quien interfiera de modo que quiera alterar los datos contenidos en los procesos de carácter personal, como también se castiga a quien teniendo o apoderándose de cualquier medio de información y comunicación quiera poner en riesgo cualquier clase de propiedad ya sea con la finalidad de perjudicar o favorecer a otros sin el consentimiento de su autor o creador

actuando en forma de distribución, transformación o llegando hasta el plagio.

En algo nuestra legislación ha intentado prevenir y sancionar pero cabe señalar que la misma ley española es más amplia y más profunda en el sentido de proteger a los innovadores.

Art 400.- La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

En este caso en particular no solo la sanción será para sus autores sino que llegará hasta el secuestro de estos mismos equipos y la prohibición de desempeñar las funciones para las que estaban destinadas.

Art 536.-La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación, con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años. Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

Aquí también se adaptan varios procedimientos como en nuestro sistema judicial, para poder tomar como prueba ciertos actos, pero siendo el caso de intersecciones ilegales o no pedidas por autoridad competente y que sus autores fueren representantes de la sociedad la responsabilidad y

sanción van hasta la suspensión de su trabajo, privándolo quien sabe según el delito hasta con el cese definitivo de su función o empleo y prohibiéndole a futuro desempeñar el mismo cargo. Respecto a estos delitos en España existen varias medidas de seguridad para prevenir estas conductas delictivas.

Legislación de Francia

El tratamiento que le ha dado Francia a estos delitos no ha sido del todo bueno ya que en algunos artículos que tomaré, tratan este sistema delictivo de manera general y no en forma detallada pero se sabe que existen estudios que a futuro podrán tipificar conductas delictuales con más detalle y mayor sanción.
Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

Art 462-2.- Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
Se criminaliza las conductas de manera muy general, pero al momento de llegar a su comprobación se delimitarán varios procesos para justificar el hecho delictual, nuestro Código Penal en su artículo 553. 1 tiene relación en cuanto a las personas que de manera fraudulenta entran a redes informáticas sin autorización de su propietario causando transferencias de bienes o valores no consentidos por sus dueños o también que altere o modifique dichos datos contenidos en redes informáticas.

Art 462-3.- Sabotaje Informático. Falsear el funcionamiento de un sistema de tratamiento automático de datos.

Art 462-4.- Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

Este artículo tiene mucha relación con el Código penal ecuatoriano artículo 262 CP por cuanto ya califica el dolo para la ejecución de la acción pero la sanción se la califica según el grado de participación como las consecuencias que dieran lugar en esta ley francesa.

Art 462-5.- Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Art 462-6.- uso de documentos informatizados falsos. En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5, En estos dos artículos finales nuestro código los califica como pueden ser alterados los datos o modificados en su artículo 353 del CP, por lo general se dan estos casos por querer lucrar o causar un mal a un tercero ya sean éstas alteraciones de carácter formal o esencial de manera que induzca a error en cuanto al original o auténtico.

Legislación Chilena

En lo que tiene que ver a países del sur de América, quien tuvo mayor desarrollo y crecimiento en lo referente a la prevención de los delitos Informáticos fue Chile, por cuanto su ley abarca varias conductas que merecen sanción por parte del sistema penal Chileno, por las cuales se puede cometer fraudes, falsificaciones, sabotajes, espionajes y lo más grave la trata de personas, por lo que toda la ley que mencionaré tiene íntima relación con la Ley de Comercio Electrónico, Firmas Electrónicas y

Mensajes de datos. Las penas que se establecen en la legislación Chilena van desde un año y medio hasta cinco años de prisión. En este país existen dos leyes informáticas, una referente a la protección de los sistemas de información y sus datos y otra que regula los documentos electrónicos, firma electrónica y su certificación.

Por reforma del año 1993 se redactó una ley especial (ley 19.223), promulgada con fecha 28 de mayo de 1993 y publicada en el diario oficial N° 34.584, de fecha 7 de junio de 1993, que contempla las figuras del delito informático. Esta ley consta de cuatro artículos que se refieren a lo siguiente:

LEY RELATIVA A DELITOS INFORMATICOS.

Ley No.:19223

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

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

Art 3.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Art 4.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado

medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".

e. Materiales y Métodos

Materiales

Los materiales utilizados para la presente investigación fueron:

- Documentales y bibliográficos, relacionados con el derecho penal y su relación con la informática jurídica, además de legislaciones nacionales e internacionales.
- Material de Campo, a este tipo de materiales nos referimos a la utilización de herramientas tecnológicas como es el caso de software para la detección de pruebas en el caso de delitos informáticos, el uso de la red (INTERNET), para la consulta de métodos delictivos y la satisfacción de cumplir con los métodos planteados es este trabajo de investigación, además el empleo de recursos humanos para la elaboración de encuestas en instituciones jurídicas y demás, para poder concluir la investigación con datos reales y actuales al medio en el que estamos desenvolviéndonos.

Métodos

En la ejecución del presente trabajo de investigación empleé el método científico que me permitió seguir la secuencia pertinente para la obtención respectiva de la información, análisis e interpretación jurídica de los hechos establecidos en las diferentes doctrinas internacionales que hacen referencia al principio de mismidad. Además apliqué el método inductivo, deductivo, analítico-sintético y dialéctico, los mismos que me sirvieron para desarrollar el proyecto investigativo y concretamente a fin de obtener nuevos conocimientos de las ciencias penales.

Método Científico

Entendido como camino a seguir para encontrar la verdad acerca de la problemática planteada permitió de una manera lógica lograr la adquisición

organizada y sistemática de conocimientos en sus aspectos teóricos y doctrinarios acerca de la contratación informática y sus efectos en las relaciones mercantiles.

Método Inductivo y Deductivo

El primero que partiendo de los casos particulares permitió llegar al descubrimiento de los principios y leyes generales que los rigen; y el segundo a la inversa, partió de los conceptos principios y leyes para luego realizar el análisis correspondiente y permitió llegar a las conclusiones y recomendaciones.

Método Histórico

Se utilizó para realizar el análisis retrospectivo de la evolución del Derecho
Informático, de los contratos informáticos, hasta llegar a las actuales concepciones.

Método Descriptivo

Permitió observar y analizar en forma minuciosa aspectos relativos a la problemática planteada. Además empleé el análisis doctrinario que me sirvió para conocer profundamente la importancia del principio de mismidad y su significado para el proceso penal. Así mismo utilicé el análisis exegético jurídico que me ayudo a estudiar el problema enfocado, para determinar su importancia.

También recurrí al método comparativo, a través del cual efectué el estudio de la legislación procesal penal comparada en lo relacionado al principio de mismidad, evaluando las tendencias más eficaces. Para el desarrollo del trabajo de campo utilicé la técnica de la encuesta que será aplicada a Magistrados, Jueces de lo Penal del Distrito Judicial de algunas

ciudades del País en una muestra de treinta personas cuyos resultados me sirvieron para establecer criterios sobre la necesidad de encontrar una alternativa de solución.

Procedimientos

Fueron los procedimientos de observación, análisis y síntesis, los que fueron
utilizados y aplicados en la presente investigación, auxiliados de técnicas de
acopio teórico como el fichaje bibliográfico, nemotécnicas y documental; y de
técnicas de acopio empírico, como la encuesta y la entrevista, el estudio de
casos de contratos informáticos, reforzó la búsqueda de la verdad objetiva de la problemática desarrollada. Mediante el Fichero Bibliográfico, se procede a la selección de la Bibliografía Básica, la que constará del proyecto; esta bibliografía debe comprender libros, revistas, enciclopedias, diccionarios, complicaciones legales, compendios de jurisprudencia, informes monográficos y la Tesis; inclusive archivos informativos de literatura jurídica.

Técnicas

La investigación de campo se concretó a consultas de opinión a personas conocedoras de la problemática, previo muestreo poblacional de por lo menos treinta personas para las encuestas, las mismas que fueron dirigidas
a profesionales del derecho y personas dedicadas al comercio electrónico.

Las entrevistas fueron aplicadas a los profesionales del derecho, proveedores y consumidores de bienes y servicios informáticos, quienes

se encuentran directamente vinculados con la problemática. En ambas técnicas se plantearon cuestionarios derivados de la hipótesis, cuya operatividad partió de la determinación de variables e indicadores.

f. Resultados

Resultados en la aplicación de encuestas y entrevistas.

Para el análisis, tabulación e interpretación de resultados de los datos obtenidos mediante la aplicación de las encuestas, se tomó como muestra la cantidad de 30 personas, que están inmersas en el área del derecho, como también operadores y administradores de la función judicial.

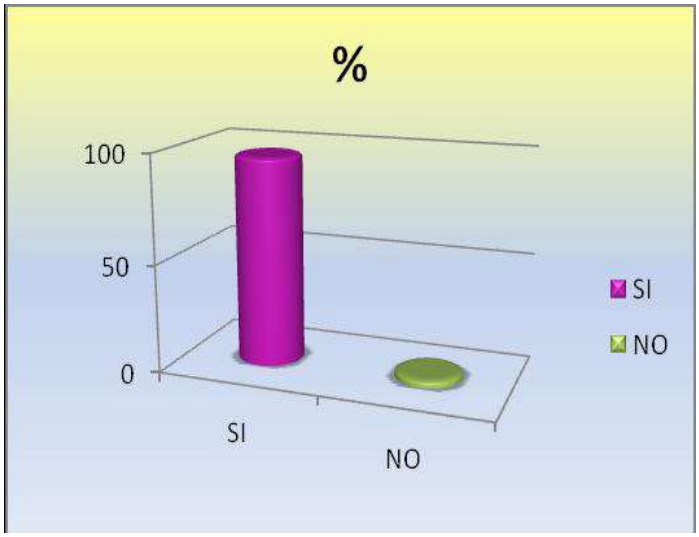
Pregunta Nro. 1

¿Usted sabe que existe una ley que protege a las personas de la Sociedad de la Información de los delitos informáticos?

Cuadro # 1

Indicador	Frecuencia	Porcentaje
SI	1	3.34
NO	29	96.66
TOTAL	30	100

Grafico # 1



Interpretación: De los encuestados veintinueve personas que corresponden al 96,66%, opinan que desconocen la ley que proteja a las personas de los delitos informáticos; y su respectivo proceso de investigación, mientras tanto que una persona que corresponde al 3,34% manifiesta que si existe.

Análisis: si existe una ley que protege a la sociedad de los delitos informáticos, pero la misma no es conocida por todos ya que en muy pocas ocasiones se han presentado denuncias o hechos que llamen la atención en cuanto al mal uso de las tecnologías de la información y comunicación, y todo los casos quedan o son analizados por expertos de forma extra judicial.

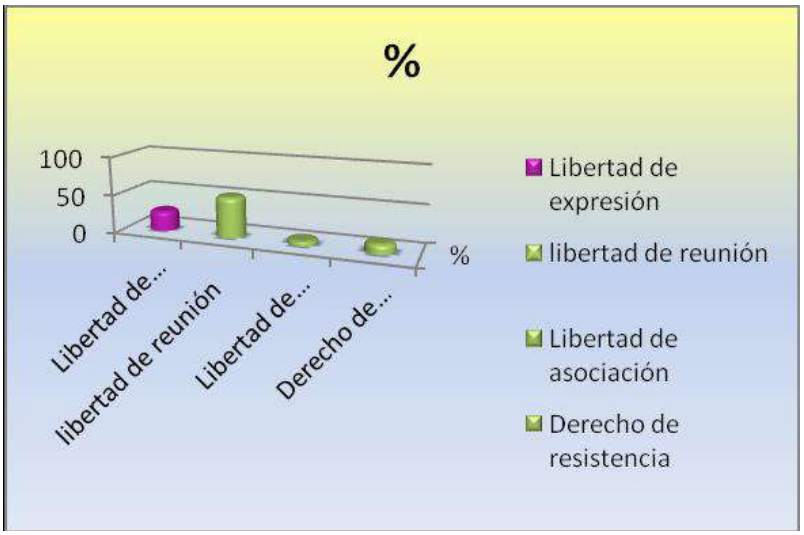
Pregunta Nro. 2

¿En Ecuador, quienes son las Autoridades Certificadoras del gobierno federal que actualmente expiden Firmas Electrónicas garantizando los derechos de la protección de datos, la intimidad y la falsificación de las firmas electrónicas?

Cuadro # 2

Indicador	Frecuencia	Porcentaje
COIP	16	53.34
No existe en el País	4	13.34
Ley de Comercio Electrónico, mensajes de datos.	2	6.66
Constitución	8	26.66
TOTAL	30	100

Grafico # 2



Interpretación: De los encuestados, ocho personas que corresponden al 26,66% opinan que los derechos se encuentran en la Constitución; dieciséis personas que forman parte del 53, 34% afirman que se encuentran en el Código Penal; dos personas que pertenecen al 6,66% sostienen que los derechos se encuentran en la ley de comercio electrónico; y finalmente cuatro personas opinan que los derechos mencionados no están regulados por ninguna ley.

Análisis: los derechos de: el honor, el buen nombre, la intimidad, la protección de datos, falsificación de firmas electrónicas, se encuentran garantizados por nuestra constitución pero no existe un procedimiento técnico legal para tipificar y sancionar los mismos cuando son vulnerados.

Estudio de Casos

CASO 1

El juicio se inició: 29 de marzo de 2006

País: Inglaterra, ante el Juez de la Corte Suprema.

“Apple Corps demando ha Apple Computer, en septiembre de 2003, Apple Corps demandó a Apple Computer, por incumplimiento de contrato,

en el uso del logotipo de Apple en la creación y el funcionamiento de la computadora de Apple iTunes Music Store, Apple Corps, que afirmó era una violación del acuerdo anterior. Algunos observadores especularon que si Apple Corps fue un éxito, Apple se vería obligada a ofrecer una población mucho más grande, tal vez como resultado de Apple Corps convertirse en un accionista mayoritario de Apple Computer, o tal vez en la división de iPod de Apple Computer y los negocios relacionados a una entidad independiente.

El juicio se inició el 29 de marzo de 2006 en Inglaterra, ante el Juez de la Corte Suprema. En la apertura de argumentos, un abogado de Apple Corps declaró que en 2003, poco antes del lanzamiento de la tienda de Apple Computer demúsica en línea, Apple Corps rechazó una oferta de EE.UU. $ 1 millón de Apple Computer por usar el nombre de Apple en la tienda de iTunes. El 8 de mayo de 2006 el tribunal falló a favor de Apple Computer, con la Justicia Edward Mann sostiene que "no incumplimiento del acuerdo de marca había sido demostrada". El juez se centró en la sección 4.3 de este Acuerdo: Las partes reconocen que ciertos bienes y servicios en el campo de la informática de uso de Apple son capaces de entregar su contenido en el campo de Apple Corps de uso. En tal caso, a pesar de que Apple Corps tendrá el derecho exclusivo a utilizar o autorizar a terceros a utilizar las marcas de Apple Corps, o en relación con el contenido en el inciso 1.3 (i) o (ii) (el catálogo de Apple Corps y el futuro cualquier tipo de música), Apple Computers (sic) tendrá el derecho exclusivo a utilizar o autorizar a terceros a utilizar las marcas Apple Computer, o en relación con bienes o servicios dentro de la subsección 1.2 (Apple la informática de uso) (tales como servicios de software, hardware o radiodifusión) utilizado para reproducir, correr, jugar o no entregar el contenido, a condición de que no podrá utilizar o autorizar a terceros a utilizar las marcas Apple Computer, o en relación con los medios físicos entrega de contenido pregrabado en el inciso 1.3 (i) o (ii)

(ejemplo como un disco compacto de música de los Rolling Stones).” El juez sostuvo que el uso de Apple Computer fue cubierto por esta cláusula. La sentencia ordena Apple Corps a pagar los costos legales de Apple, estimado en 2 millones de Libras esterlinas.”

COMENTARIO Y ANÁLISIS

Apple Corps fundamenta su demanda en el no cumplimiento del contrato, por parte de Apple Computer, sin embargo el Tribunal que conoce del caso,
falló a favor del demandado (Apple Computer), demostrando que no hay incumplimiento del acuerdo de marcas, para lo cual se remite a la sección.

4.3 del Acuerdo Informático o Contrato informático, en donde claramente se
estipula que las partes reconocen que ciertos bienes y servicios en el campo de la informática de uso de Apple son capaces de entregar su contenido en el campo de Apple Corps de uso. Así mismo existe un Catálogo que forma parte del acuerdo entre las partes, en donde las partes se obligan a cumplir con ciertos requerimientos que tienen que ver con el campo de la informática de uso, como servicios de software, hardware o radiodifusión utilizado para reproducir, correr, jugar o no entregar el contenido.

Este caso se determina que los contratos informáticos como evidencia digital, estipulan cláusulas informáticas, catálogos de uso de bienes y servicios informáticos, que las partes están obligados a cumplir y en el caso de que una de las partes considere que hay incumplimiento de los términos contractuales, puede demandar sus derechos. Por esta razón creo que es necesario incorporar en nuestra Ley de Comercio Electrónico,

Firmas Electrónicas y mensajes de datos, los Contratos Informáticos como evidencia y se prueba la eficacia de los mismos[9].

CASO 2

“Klocek v. Gateway, Inc.Corte: Estados Unidos Tribunal de Distrito de Kansas (104 F. Supp .2 d 1332) Año: 2000 Página en el texto: 137-144 Historia de procedimiento: Demandantes: Demandar a Gateway y Packard Hewlatt en un caso de la diversidad en la corte federal. Movimientos de puerta de enlace para un juicio sumario. Hewlatt mociones de juicio sumario. Tribunal otorga movimiento Hewlatt, pero no los Gateways. El demandante afirma trae la acción individual y colectiva contra puerta de enlace alegando que loindujo y otros consumidores para comprar computadoras y paquetes especiales de apoyo, haciendo falsas promesas de apoyo técnico.

Puerta de entrada afirma que el demandante debe arbitrar sus reclamaciones en virtud de los Términos Estándar de Gateway y el Acuerdo de Condiciones, que se incluye en la caja que contiene los cables de la batería la energía del ordenador y manuales de instrucciones. Hechos del caso: Términos: "Al mantener el sistema Gateway 2000 equipo más allá de cinco (5) días después de la fecha de entrega, la aceptación de estos Términos y Condiciones." Problema jurídico: Si la cláusula de arbitraje de puerta de enlace en sus Términos y Condiciones Estándar es parte del contrato entre él y los demandantes. Regla: En cuanto a Hill c. Gateway 2000, afirman Inc. 's que la UCC § 2-207 no se aplica cuando hay una sola forma, el tribunal en este caso dice: "Por sus propios términos, § 2-207 se aplica a la aceptación o el escrito confirmación. Afirma nada de lo que requiere otra forma antes de la prestación se haga efectiva." "En las transacciones de consumidor medio,

[9] http://en.wikipedia.org/wiki/Apple_Corps_v_Apple_Computer#2003.E2.80.932006

el comprador es el oferente, y el vendedor es el destinatario." Explotación: Por lo tanto, ya que Gateway no ha aportado pruebas suficientes para apoyar una conclusión en la ley de Kansas o Missouri que el demandante de acuerdo con la cláusula de arbitraje contenida en Condiciones Estándar de Gateway, el Tribunal anula el movimiento de puerta de enlace para despedir. Razonamiento:

"Si bien es posible que el vendedor sea el oferente, Gateway no ofrece pruebas objetivas que respaldan esa constatación. El Tribunal por lo tanto, asume los efectos de la moción para desestimar que el demandante ofreció comprar el ordenador y puerta de enlace aceptó la oferta del demandante (ya sea por completar la transacción de venta en persona o por acuerdo de enviar y / o entregar el ordenador al demandante)." "Gateway proporciona no ninguna evidencia de que en el momento de la transacción de venta, informó al demandante de que la operación estaba condicionada a la aceptación del demandante de las condiciones generales."

"Debido a que el demandante no es un comerciante, términos adicionales o diferentes que figuran en las cláusulas no se convirtió en parte de acuerdo de las partes, salvo acuerdo expreso con ellos." Juicio: Anuló el movimiento de puerta de enlace de desestimar.[10]”

COMENTARIO Y ANÁLISIS

El Tribunal declara que el acto de mantener el equipo los últimos 5 días no fue suficiente para demostrar que el demandante ha aceptado expresamente las condiciones estándar.

[10] http://www.casebriefs.com/blog/law/contracts/contracts-keyed-to-murphy/the-bargain-relationship/klocek-vgateway/2011

Consentimiento expreso no se puede presumir por el silencio o la mera falta de objeto. Por lo tanto, ya que Gateway no ha aportado pruebas suficientes de que el demandante accedió a la cláusula de arbitraje, anuló el movimiento de puerta de enlace de desestimar.

Es este caso se confirma que es posible que las partes que intervienen en la generación de obligaciones y derechos, puedan ir más allá de la ley, siempre y cuando sus compromisos no sean contradictorios al derecho; lo cual significa que lo pactado entre las partes obliga. La inclusión de cláusulas particulares, el mismo objeto o alcance del proyecto o incluso en Anexos Técnicos que establezcan los criterios necesarios para una adecuada y pormenorizada definición del proyecto, están contemplados en la metodología jurídica de los contratos informáticos.

g. Discusión.

Verificación de objetivos

En el proyecto de investigación se plantearon algunos objetivos para ser verificados en el desarrollo del trabajo investigativo. Estos objetivos fueron los siguientes:

El Objetivo general

Realizar un estudio jurídico crítico sobre la legislación informática en relación con las evidencias digitales en materia de lo delitos informáticos, y en el Derecho Comparado. Este objetivo general fue desarrollado a partir del análisis del Marco Jurídico, en el cual se hizo un estudio de la Constitución de la República del Ecuador en relación con la ley de los delitos computacionales que otorga la constitución dentro de este análisis consta el estudio jurídico-crítico dentro del Código Orgánico Integral Penal y la Ley de Comercio Electrónico, Firmas Electrónicas. y Mensajes de Datos, y sus diversas disposiciones, análisis que comprendió el estudio evidencias digitales y la necesidad de su incorporación; también se realizó el estudio del Derecho Informático, y las concepciones en las diferentes legislaciones.

Objetivos específicos

- Demostrar que la insuficiencia jurídica de que adolecen tanto el COIP, el Código de Comercio Ecuatoriano y la Ley de Comercio Electrónico, Firmas Electrónicas, y Mensajes de Datos, en cuanto a la falta de normatividad de los Contratos Informáticos, perjudica las relaciones mercantiles y a los usuarios de esta rama del comercio.

- Revisar bibliografía especializada acerca de los Delitos Informáticos.
- Proponer un proyecto de Reformas a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, y COÏP, incorporando a su normatividad el manejo de la evidencia Digital.

Contrastación de la hipótesis

La carencia en la legislación informática en el manejo de la evidencia digital que regulen las actividades de las empresa que mantienen su información principal como patrimonio de las actividades comerciales y quienes requieren de éstos servicios, genera problemas graves y dificultad de este tipo de actos

Fundamentación jurídica para la propuesta de reforma legal

Nuestra Constitución vigente, garantiza la integridad de la información en un proceso digital en consecuencia se pueden considerar la tipicidad de los Delitos informáticos dentro de esta garantía, por consiguiente, las personas son libres para mantener integra la información verificando sus condiciones, limitaciones, modalidades, formalidades, plazos, y demás particularidades que regirán la relación jurídica creada por el tratamiento de la información digital.

Los resultados de la investigación ratifican que la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y el COIP adolece de
insuficiencia jurídica al no regular en su normativa legal a la evidencia digital.

Este tipo de tratamientos son instrumentos que demandan no solo de conocimientos jurídicos “tradicionales” para formular el tratamiento seguro y confiable de la Información, sino que adicionalmente requieren de conocimientos de Tecnologías de la Información, los cuales deben ser traducidos e incorporados en términos legales al contrato en sí como normas obligatorias entre ellas.

h. Conclusiones

Luego de la revisión teórica y con los resultados reales obtenidos en el proceso investigativo de campo he llegado a las siguientes conclusiones:

Los entrevistados coinciden en que las organizaciones que ofrecen bienes y trabajan con servicios informáticos enfrentan la problemática que la información sea vulnerada, y de ser así la garantía judicial de saber si la evidencia digital es tratada para llegar a la investigación de quien cometió el delito, la normatividad existente sin embargo es necesario mediante adecuar una metodología jurídica, crear soluciones adecuadas que puedan aportar elementos suficientes para regular en forma veraz y oportuna.

La metodología jurídica de los Delitos Informáticos, permite el conocimiento de la técnica del tratamiento de la información, la utilidad o aplicación concreto de un bien o servicio informático y deberes de los proveedores y usuarios; constituyen elementos claves para el mantenimiento de los activos de información y de la tecnología informática.

La mayoría de los abogados encuestados están de acuerdo que la Ley de Comercio Electrónico, los delitos establecidos en el COIP, Firmas Electrónicas y Mensajes de Datos, adolece de insuficiencia jurídica al no contemplar en su normativa la metodología jurídica - Informáticos.

El criterio unánime de los encuestados y entrevistados coincide en manifestar que el desarrollo de medios electrónicos han dinamizado la comunicación y el comercio informático, por lo que se hace necesario incorporar a la normativa existente, la doctrina del tratamiento de la evidencia digital, que por su naturaleza requieren de procesos, que

permitan que el comercio informáticos y los sistemas de información se desarrolle en condiciones seguras, oportunas, garantizando el debido proceso.

El auge del comercio electrónico y la firma digital, juegan un papel determinante en la recuperación de la confianza y seguridad de los usuarios, que sienten en las comunicaciones electrónicas una apertura al mundo actual.

El desarrollo tecnológico que se ha venido logrando en los países industrializados, permite agilitar y hacer mucho más operante la prestación de los servicios y el intercambio de bienes tangibles e intangibles, lo que hace necesario incorporar dentro de la estructura legal, el marco jurídico en temas de los sistemas de información.

i. Recomendaciones.

La experiencia obtenida al concluir el presente trabajo investigativo y luego de haber expuesto las conclusiones a las que he llegado, considero pertinente formular las siguientes recomendaciones:

Que Universidad Nacional de Loja, socialice las temáticas variadas que existen sobre la metodología de los Delitos Informáticos, que promueva jornadas académicas, a fin de que profesionales del derecho, estudiantes, los proveedores y usuarios, conozcan esta normativa y puedan acceder a los beneficios y seguridades informáticas.

Que se implemente en el pensum de estudio académico, la doctrina del derecho informático, por tratarse de una materia inequívocamente jurídica, con el propósito de que los estudiantes de derecho, conozcan las normas jurídicas relativas a lo que se conoce como la materia informática, que es, precisamente, todo lo concerniente a la informática.

Que, dicha reforma contenga la metodología jurídica de los Delitos informáticos, con el propósito de garantizar un eficiente análisis de los sistemas de información e informáticos.

Que, es indispensable que el Estado Ecuatoriano, cuente con herramientas jurídicas que le permitan acceder a la transferencia de tecnología, mediante el uso de las tecnologías de la información.

Propuesta de reforma jurídica asamblea nacional considerando

QUE, la actual Ley de Comercio Electrónico, COIP, Firmas Electrónicas y Mensajes de Datos, adolece de insuficiencia jurídica al no estar incorporados a su normatividad y la relevancia de los Delitos Informáticos.

QUE, los Delitos Informáticos constituyan instrumentos jurídicos de suma importancia para viabilizar las actividades mercantiles a través de los medios electrónicos y sus derivados como la evidencia digital y su tratamiento correcto en todos sus procesos.

QUE, la existencia de los delitos informáticos en otras legislaciones ha permitido que las actividades mercantiles relacionadas a la transferencia de tecnología informática se desarrollen en un marco jurídico adecuado dentro del cual las partes en sus transacciones, puedan fijar sus respectivos derechos y obligaciones.

j. Bibliografía.

- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- http://app.ute.edu.ec/content/3254-42-10-1-6-/Perfil%20de%20los%20Delitos%20Informaricos%20%20Ecuador%20-%20Fiscalia.pdf
- Delitos informáticos y delitos comunes cometidos a través de la informática margarita roig torres; enrique orts berenguer.
- Título del trabajo: "Un nuevo desafío jurídico: Los Delitos Informáticos", Autor: Dra. Esc. María José Viega Rodríguez.
- La protección penal de la intimidad, CDYT, 2016.
- Los delitos informáticos en el Código Penal**, Abeledo Perrot, 2008**
- Delitos Informáticos**, Ad Hoc, 2000.**
- https://es.scribd.com/doc/140203386/Libro-Delitos-Informaticos-INEI-pdf
- Cano, Jeimy J. Computación forense. Descubriendo los rastros informaticos.

  Primera Edición. Alfaomega Grupo Editor, S.A. de C.V., México Informática y 27-29 Derecho 28 Revista Iberoamericana de derecho informático II Universidad Nacional de Educación a Distancia Centro Regional de Extremadura- Mérida.3

k. Anexos:

UNIVERSIDAD NACIONAL DE LOJA

UNIDAD DE DUCACION A DISTANCIA

CARRERA DE DERECHO

"DESAFÍOS Y PERJUICIOS LEGALES EN LA SOCIEDAD DE LA INFORMACIÓN POR LAS INFRACCIONES INFORMÁTICAS"

PROYECTO PREVIO A OPTAR EL TITULO DE ABOGADO

AUTOR: **Héctor Roberto Gordon Quinche**

Loja – Ecuador

2016

1. Tema

“Desafíos y Perjuicios legales en la sociedad de la información por las Infracciones Informáticas”

2. Problemática;

Los efectos totalmente negativos que producen las infracciones informáticas dentro de la sociedad de la información son muchas veces desastrosas para quienes nos ha facilitado la creación, distribución y manipulación de la información, tomando en cuenta que al momento de accionar alguna infracción informática la investigación previa o posterior de la infracción requiere de conocimientos y procesos claros al establecer el peritaje informático forense muchos casos o casi todos de ellos con delitos informáticos quedan en investigación porque no se detalla las evidencias eficaces y no se juzga efectivamente a los infractores.

Nos enfrentamos a un gran problema social ya que estas conductas inapropiadas no pueden ser investigadas de forma clara, los problemas que se dan en todas sus etapas, la gran mayoría es por falta de evidencia digital probatoria en algunos casos y lo que es aún más grave en otros por falta de conocimiento, experiencia y un aparente vacío en la Ley pertinente que dificulta la aplicabilidad por parte de las autoridades encargadas de la administración de justicia para este tipo de delitos, que en nuestro país es una forma de delinquir sumamente incipiente.

Para respaldar esta investigación es importante mencionar que base legal está incluido en varios Capítulos referente a los delitos, infracciones informáticas en el Código Orgánico Integral Penal vigente actualmente en el Estado Ecuatoriano.

Debemos tomar cartas sobre el incumplimiento de las normas establecidas dentro de la sociedad ecuatoriana, están siendo porcentualmente un hecho que actúa como factor multiplicador de la impunidad en los casos sobre las infracciones informáticas, dejando un vacío por la falta de aplicabilidad de la ley en los casos judiciales, por tal particularidad las infracciones quedan como procesos investigativos extrajudiciales.

Para garantizar el pleno ejercicio de los derechos de todas las personas y la seguridad jurídica dentro de la Sociedad que debe ofrecer el Estado Ecuatoriano, es necesario el análisis profundo de las infracciones informáticas, su modus operandi y tratarlo de plasmar con el Código Orgánico Integral Penal, garantizando una administración de justicia eficiente para resolver este tipo de casos tan incipientes en nuestra Sociedad de la Información.

3. Justificación;

Cada vez existen constantes eventos totalmente atípicos que necesitan analizar la forma de investigación, sus procesos de acuerdo a cada infracción o incidente, manejando los protocolos investigativos modernos

y correctos, basados en la esencia misma de la conducta del ser humano, en el mundo digital.

La razón del porque he seleccionado este tema, es porque en el mundo de la Tecnología está en constante uso con sus beneficios en la aplicación de las herramientas para optimizar tiempos operativos en las labores diarias de trabajo o de ocio; también recalcar que a gran escala la economía a nivel del mundo se genera el mercado del consumo de Tecnologías y donde la dependencia creada por los usuarios hace que las infracciones informáticas estén estrechamente relacionadas con el uso de la parte informática y con el derecho respectivamente.

Otra motivación para esta investigación es por mi perfil profesional, donde paralelamente puedo manejar los problemas técnicos y legales en el caso de existir evidencias probatorias en algunos casos, también por la cantidad de infracciones informáticas que se dan en el país y que se han transformado en un latente problema ciber delincuencial, donde los delitos ejecutados no son bien analizados desde la perspectiva jurídica sumado a esto el mal manejo de los casos de toda índole, casos como acoso sexual, robo digital, suplantación de identidad entre otros.

Uno de los principales objetivos de este trabajo de titulación es crear un estudio minucioso de los escenarios de las infracciones informáticas así como su legislación, las seguridades y la forma correcta de buscar evidencias digitales donde se busca una justicia clara y totalmente mejorada, para frenar los embates de los ciber delitos, que se ejecutan o

cumplen su objetivo en un ámbito muy singular afectando a millones de personas a nivel del globo terráqueo.

Al ser aparentemente un tema incipiente en nuestra sociedad de la información, realmente no es así; en nuestro país aún se sigue investigando la forma más apropiada o adecuada para generar la cultura de la información en los usuarios, de la misma forma es importante que los detalles sean de conocimiento de quienes se encargan de gestionar la justicia y los derechos de todos nosotros, donde se debe involucrar sobre la gravedad de los incidentes que provocan las infracciones informáticas a todas las autoridades y la sociedad de la información.

Este trabajo investigativo va a aportar con valiosa información donde genera un campo especifico de la garantía de los derechos de las personas que han sido directamente o indirectamente afectadas por este tipo de delitos, poniendo en claro que ninguna infracción informática deberá quedar impune, la importancia de establecer un tema de análisis profundo a los estudiantes y elementos de la justicia sobre los distintos eventos que se suscitan en el mundo digital y que son perjudiciales y donde pensamos que es imposible resolver un tema Técnico – Jurídico, sin embargo una buena investigación dentro del Peritaje Informático Forense permitirá crear mejores acciones de decisión en el ámbito legal.

La Constitución de la República del Ecuador menciona en su artículo 3 numeral 8 lo siguiente:

Art. 3.- Son deberes primordiales del Estado:

8. Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción.

Ejemplo de las infracciones informáticas podemos citar el artículo inicial del Código Orgánico Integral Penal, Sección tercera donde habla de la seguridad de los sistemas de información.

SECCIÓN TERCERA Delitos contra la seguridad de los activos de los sistemas de información y comunicación

Artículo 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

4. Objetivos;

4.1 Objetivo General:

Analizar y tratar los problemas y desafíos Técnicos – Legales de los Perjuicios en la Sociedad de la Información por las Infracciones Informáticas

4.2 Objetivos Específicos:

- Analizar los contenidos doctrinarios en relación a los delitos informáticos.
- Concienciar a nivel de política nacional de los desafíos con respecto a la seguridad cibernética y sus vínculos con el desarrollo en la Sociedad de la Información.
- Identificar las mejores iniciativas legales y políticas prácticas que funcionan alrededor del mundo para crear una cultura de seguridad cibernética.
- Examinar las opciones para dar una respuesta Técnico – Legal al incremento del delito cibernético y las Infracciones Informáticas.

5. Marco teórico;

Acción Penal

El tratadista en materia penal LLORE M. Víctor, en su obra Derecho Procesal Penal Ecuatoriano, Fondo de la Cultura Ecuatoriana. Cuenca,(1990), indica que “la acción penal puede considerarse bajo dos

aspectos: uno subjetivo y otro objetivo; que subjetivamente es el poder jurídico que compete al Ministerio Público de activar las condiciones para obtener del juez la decisión sobre la realizabilidad de la pretensión punitiva del Estado, derivada de un hecho que la ley prevé como delito. Que objetivamente, la acción penal es el medio con que el órgano ejecutivo, constreñido a abstenerse de la coerción directa en las relaciones penales, determina la intervención de la garantía jurisdiccional en orden a su pretensión punitiva"

LEONE, Giovanni en su obra Tratado de Derecho Procesal Penal Edit. Ediciones Jurídicas Europa-América Argentina (1994); nos explica que "por su particular función y sus particulares aspectos, la acción penal se presenta a una primera visión empírica, como la actividad de un órgano del Estado encaminada a obtener una decisión del juez penal en relación a un hecho que constituye delito y que se supone cometido por alguien. Pero que cuando se parte, sin embargo de una configuración jurídica de dicha actividad, se perfilan las posiciones siguientes:".

a) La acción penal como derecho subjetivo frente al juez.

b) La acción penal como derecho potestativo.

c) La acción penal como manifestación de voluntad a la cual está condicionado el ejercicio de la jurisdicción penal.

BORJA OSORNO, Guillermo; en su obra titulada Derecho Procesal Penal (1996), nos comenta que "la acción penal surge de un delito, son sus

presupuestos precisamente delito y delincuente. De todo acto con apariencias delictivas, que ataca la existencia y la conservación de la sociedad, nace la acción penal para la sanción del culpable".

Acción Penal Pública

La acción penal pública es aquella ejercida de forma exclusiva, excluyente y de oficio por la Fiscalía, según de qué normativa procesal se trate, para la persecución de un delito.

En los procesos criminales lo común es la acción pública. En general, la mayoría de estos delitos comienzan a investigarse a partir de una denuncia, pero pueden ser investigados tan pronto tengan los poderes públicos conocimiento de los hechos por cualquier medio. Llegada la noticia de un posible crimen a los organismos del Estado, este actúa sin necesidad de intervención o pedidos de persona alguna, ni siquiera de la víctima directa del crimen, o sus herederos.

El fundamento de la acción pública es que se considera que la sociedad en su totalidad ha sido perjudicada por el delito cometido y el Estado asume entonces el papel de defensa de la sociedad. La mayoría de los países incluye todos, o casi todos, los delitos contemplados en su legislación como de acción pública.

Delitos Informáticos

El Dr. TÉLLEZ VALDÉS, Julio menciona en su obra titulada Derecho Informático, (2010) "dos clasificaciones del Delito Informático para efectos

de conceptuación, que parten de lo típico y lo atípico. El concepto típico, los Delitos Informáticos son las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin".

El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos. Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto.

Partiendo de esta compleja situación y tomando como referencia el "Convenio de Ciberdelincuencia del Consejo de Europa", podemos definir las infracciones y 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, redes y datos".

En el Ecuador así como en los demás países, todos los principios jurídicos, legales y procesales, así como doctrinarios, están presentes en el tratamiento del delito informático, su investigación y juzgamiento, sin embargo las características propias de este delito que pertenece a una nueva era, a la era de la información y el conocimiento, trasciende al ordenamiento jurídico vigente, constituyendo un elemento de inflexión o quiebre del tradicional sistema jurídico.

Tipos de Delitos Informáticos

CAMACHO LOSA, en un artículo publicado en el internet señala que el único límite 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 DON 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, se ponemos a consideración del lector en forma breve en qué consiste cada una de estas conductas delictivas:

Los Datos Falsos o Engañosos.

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”.

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 víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos c años, 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.

Bombas Lógicas

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 y Malware.

Son elementos informáticos, que como los microrganismos 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.

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.

Ataques de Denegación de Servicio.

Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios Ejemplos típicos de este ataque son: El consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventana, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

El Espionaje Informático y el Robo o Hurto de Software.

Fuga de Datos.

También 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 del 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 supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios.

Apropiación de Informaciones Residuales

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 y Suplantación de Personalidad

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.

El Acceso no Autorizado a Servicios Informáticos.

Las Puertas Falsas

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

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

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 señaló 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.

Seguridad Informática y Normativa

La Seguridad Informática.

Es el conjunto de técnicas y métodos que se utilizan para proteger tanto la información como los equipos informáticos en donde esta se encuentra almacenada ya sean estos individuales o conectados a una red frente a posibles ataques accidentales o intencionados.

La seguridad Informática a su vez está dividida en cinco componentes a saber:

- Seguridad Física: Es aquella que tiene relación con la protección del computador mismo, vela por que las personas que lo manipulan tengan la autorización para ello, proporciona todas las indicaciones

técnicas para evitar cualquier tipo de daños físicos a los equipos informáticos.

- Seguridad de Datos: Es la que señala los procedimientos necesarios para evitar el acceso no autorizado, permite controlar el acceso remoto de la información, en suma protege la integridad de los sistemas de datos.

- Back Up y Recuperación de Datos: Proporciona los parámetros básicos para la utilización de sistemas de recuperación de datos y Back Up de los sistemas informáticos. Permite recuperar la información necesaria en caso de que esta sufra daños o se pierda.

- Disponibilidad de los Recursos: Este cuarto componente procura que los recursos y los datos almacenados en el sistema puedan ser rápidamente accesados por la persona o personas que lo requieren. Permite evaluar constantemente los puntos críticos del sistema para así poderlos corregir de manera inmediata.

- La Política de Seguridad: Conjunto de normas y criterios básicos que determinan lo relativo al uso de los recursos de una organización cualquiera.

- Análisis Forense: El Análisis Forense surge como consecuencia de la necesidad de investigar los incidentes de Seguridad Informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera

de evitar ataques similares en el futuro y obtener pruebas periciales.

- Seguridad Normativa: Derivada de los principios de legalidad y seguridad jurídica, se refiere a las normas jurídicas necesarias para la prevención y sanción de las posibles conductas que puedan ir en contra de la integridad y seguridad de los sistemas informáticos.
- En definitiva para que exista una adecuada protección a los sistemas informáticos y telemáticos se deben conjugar tanto la seguridad informática como la seguridad legal y así poder brindar una adecuada protección y tutela tanto técnica como normativa.
- En resumen la Seguridad Informática y Normativa debe usarse para impedir los ataques ya sean fuera del sistema (virus, syware, adware, entre otros) y dentro del mismo, exigiendo políticas claras y precisas sobre el nivel de acceso a cierta información de carácter confidencial y una debida protección a esta.

Según el ilustre penalista CUELLO CALON, los elementos integrantes del DELITO son: - El delito es un acto humano, es una acción (acción u omisión). - Dicho acto humano ha de ser antijurídico, debe lesionar o poner en peligro un interés jurídicamente protegido.

Debe corresponder a un tipo legal (figura de delito), definido por La Ley, ha de ser un acto típico.

El acto ha de ser culpable, imputable a dolo (intención) o a culpa (negligencia), y una acción es imputable cuando puede ponerse a cargo de una determinada persona.

- La ejecución u omisión del acto debe estar sancionada por una pena. Por tanto, un delito es: una acción antijurídica realizada por un ser humano, tipificado, culpable y sancionado por una pena.

Infracciones Informáticas

Muchos estudiosos del Derecho Penal han intentado formular una noción de delito que sirviese para todos los tiempos y en todos los países. Esto no ha sido posible dada la íntima conexión que existe entre la vida social y la jurídica de cada pueblo y cada siglo, aquella condiciona a ésta.

A nivel internacional se considera que no existe una definición propia de la Infracción informática, aunque muchos estudiosos han intentado investigarlo desde diferentes puntos de vista puntos de vista como son el criminógeno, formal, típico y atípico.

Una primera idea al respecto la señala el profesor mexicano Julio Téllez Valdés, quien lo conceptualiza desde dos ópticas. Nos dice que desde un punto de vista atípico son “actitudes ilícitas en que se tiene al computador como instrumento o fin”, y desde uno típico son “conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como medio o fin”. Esta primera idea es común en los textos del área, así por ejemplo,

Nidia Callegari define al delito informático como “aquél que se da con la ayuda de la informática o de técnicas anexas”.

Rasgos.

- Son conductas criminógenas de cuello blanco, en tanto que solo un determinado número de personas, en este caso ingenieros de sistemas o técnicos, pueden llegar cometerlas.
- Son acciones ocupacionales, ya que generalmente se ejecutan cuando el sujeto se encuentra en pleno trabajo.
- Son acciones de oportunidad, en cuanto se aprovecha la ocasión presentada.
- Provocan serias pérdidas económicas, ya que casi siempre producen beneficios de más de cinco cifras a quienes los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundos y sin una necesaria presencia física del ejecutante pueden llegar a consumarse.
- Son muchos los casos y pocas las denuncias debido a la falta o escasa regulación por parte del Derecho.
- Debido a su carácter técnico presentan grandes dificultades para su comprobación.

- 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.

Sujeto Activo

Las personas que cometen los “Delitos Informáticos” son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, 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, aun cuando, en

muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Sujeto pasivo

En primer término tenemos que distinguir que sujeto pasivo o 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 personas naturales o jurídicas, instituciones crediticias, gobiernos, etc. que usan sistemas automatizados de información, generalmente conectados a otros.

6. Metodología;

Se utilizara los métodos inductivo, deductivo, descriptivo y analítico, los mismos que nos ayudaran en el análisis demostrativo del problema planteado permitiéndonos observar en forma clara y concisa la propuesta de esta investigación.

Método inductivo y deductivo

Estos métodos nos permitirán primero conocer la realidad del problema a investigar partiendo desde loa particular hasta llegar a lo general en algunos casos, y segundo partiendo de la general para arribara lo particular de la problemática en otros casos.

Descriptivo

Este método nos compromete a realizar una descripción objetiva de la realidad actual en al que se desarrolla el problema y así demostrar la actual aplicación.

Analítico

Nos permitirá estudiar el problema enfocándolo desde el punto de vista social, jurídico y político; y analizar así sus defectos en su aplicación.

Método de Investigación Científica

El mismo que me lleva hacia la formulación de diversos caminos interesantes y creativos de investigación. Esta investigación nos conlleva a consultar libros, códigos, artículos, información de Internet para conocer, enfocar causas, criterios, conceptos de varios especialistas expertos en el área del código penal ecuatoriano, en lo que se refiere a las conductas inapropiadas por medio de las infracciones informáticas.

7. Cronograma;

2016																								
MESES	**ABRIL**				**MAYO**				**JUNIO**				**JULIO**				**AGOSTO**				**SEPTIEMBRE**			
SEMANAS	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**
ACTIVIDADES																								
Inicio de proyectos																								
Recolección Bibliográfica																								
Organización de la información obtenida																								
Presentación de la Información																								
Análisis y presentación de los datos																								
Verifricación de los Objetivos																								
Redacción del trabajo final																								
Presentación del trabajo investigativo																								
Socialización del trabajo investigativo																								

8. Presupuesto y financiamiento; e,

Recursos Humanos

Equipo de Investigación: Estudiante del Módulo X de Derecho MED UNL.

Héctor Roberto Gordon Quinche

Recursos Materiales y costos

- Computadora
- Diccionarios
- Internet
- Celular

- Recurso económico, para trasladar a la ciudad de Loja y para la aplicación de instrumentos de recolección de información.
- Hojas de Papel bond.

Presupuesto

DESCRIPCIÓN	COSTO
Material Bibliográfico	$ 40
Material de Escritorio	$ 100
Impresión de Documentos	$ 100
Gastos de Intervención	
Movilización y estadía	$100
Reproducción material de recolección de información	$40
Imprevistos	$25
	Total: $ 405

Financiamiento.

Los gastos serán financiados única y exclusivamente con los recursos del investigador.

9. Bibliografía.

- http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- http://app.ute.edu.ec/content/3254-42-10-1-6-/Perfil%20de%20los%20Delitos%20Informaricos%20%20Ecuador%20-%20Fiscalia.pdf
- Delitos informáticos y delitos comunes cometidos a través de la informática margarita roig torres; enrique orts berenguer.
- Título del trabajo: "Un nuevo desafío jurídico: Los Delitos Informáticos", Autor: Dra. Esc. María José Viega Rodríguez.
- La protección penal de la intimidad, CDYT, 2016.
- Los delitos informáticos en el Código Penal**, Abeledo Perrot, 2008**
- Delitos Informáticos**, Ad Hoc, 2000.**
- https://es.scribd.com/doc/140203386/Libro-Delitos-Informaticos-INEI-pdf
- Cano, Jeimy J. Computación forense. Descubriendo los rastros informaticos.

  Primera Edición. Alfaomega Grupo Editor, S.A. de C.V., México Informática y 27-29 Derecho 28 Revista Iberoamericana de derecho informático II Universidad Nacional de Educación a Distancia Centro Regional de Extremadura- Mérida.

INDICE