



**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
CARRERA DE DERECHO**

Tesis de Grado

Tema

**“ESTUDIO DEL TRATAMIENTO DE LOS DELITOS
INFORMÁTICOS DENTRO DE LA PENÍNSULA DE
SANTA ELENA”**

Previo a la Obtención del Título de:

**ABOGADO DE LOS TRIBUNALES Y JUZGADOS
DE LA REPÚBLICA DEL ECUADOR**

Autores:

MENDOZA ILLESCAS ALEJANDRO PAUL

MALLA REYES JORGE LUIS

TUTORA: ABG. ANA MARIA TAPIA BLACIO.

LA LIBERTAD– ECUADOR

2012

**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA
ELENA
FACULTAD DE CIENCIAS SOCIALES Y DE LA SALUD
CARRERA DE DERECHO**

Tesis de Grado

Tema

**“ESTUDIO DEL TRATAMIENTO DE LOS DELITOS
INFORMÁTICOS DENTRO DE LA PENÍNSULA DE
SANTA ELENA”**

Previo a la Obtención del Título de:

**ABOGADO DE LOS TRIBUNALES Y JUZGADOS
DE LA REPÚBLICA DEL ECUADOR.**

Presentado por:

MENDOZA ILLESCAS ALEJANDRO PAUL

MALLA REYES JORGE LUIS

TUTORA: ABG. ANA MARIA TAPIA BLACIO.

LA LIBERTAD - ECUADOR

2012

Santa Elena, 17 de Mayo del 2012

Señor Doctor.
Tito Ramos Viteri
DIRECTOR DE LA CARRERA DE DERECHO
Presente.-

Señor Director:

Dando cumplimiento a lo ordenado por el Consejo Académico de la Carrera de Derecho, celebrada el día 30 de Noviembre del 2011, fui nombrada Profesora Tutora del Trabajo de Titulación de fin de carrera de los estudiantes ALEJANDRO PAUL MENDOZA ILLESCAS Y JORGE LUIS MALLA REYES, con el tema **“ESTUDIO DEL TRATAMIENTO DE LOS DELITOS INFORMÁTICOS DENTRO DE LA PENÍNSULA DE SANTA ELENA”**, para lo cual informo:

Que una vez que he procedido a dirigir científica y jurídicamente el desarrollo del Trabajo de Titulación, en el cual está su contenido y su estructura, en consideración al artículo 27 del Reglamento del Trabajo de Titulación o Graduación, presentando el siguiente informe:

El presente Trabajo de Titulación revela rigor científico, pertinencia y calidad humana en dar solución a un problema jurídico, el cual permite transformar hacia la excelencia el desempeño de las Ciencias Jurídicas en la Provincia de Santa Elena, el mismo fue elaborado por los señores Alejandro Paul Mendoza Illescas y Jorge Luis Malla Reyes, egresados de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena, previo a la obtención del Título de Abogado de los Tribunales y Juzgados de la República del Ecuador.

Con estos antecedentes expuestos me permito aprobar el presente trabajo para los fines legales pertinentes.

Atentamente,

Ab. Ana María Tapia Blacio.
TUTORA

Santa Elena, 17de Mayo del 2012

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación, **“ESTUDIO DEL TRATAMIENTO DE LOS DELITOS INFORMÁTICOS DENTRO DE LA PENÍNSULA DE SANTA ELENA”** elaborado por la Sr. Alejandro Mendoza Illescas y Jorge Malla Reyes, egresados de la carrera de Derecho de la Universidad Península de Santa Elena, previo al título de Abogado de los Tribunales del Ecuador, me permito declarar que luego de haber orientado, estudiado y revisado la Apruebo en todas sus partes.

Atentamente

Ab. Ana María Tapia Blacio.

PROFESORA TUTORA

DEDICATORIA

El esfuerzo y sacrificio de estos cinco años de estudio y la realización de esta tesis se la dedico a dios, mis padres, mi esposa e hijos quienes tuvieron que forzosamente sacrificarse en todo este tiempo el no haber compartido con ellos momentos de calor familiar, por haber sido las personas quienes constantemente me han brindado incentivo con voz de aliento, por haberme proporcionado su apoyo para que pueda culminar con éxito mis estudios superiores que me conllevan a ser un profesional en derecho y así poder contribuir a mi comunidad peninsular.

Alejandro Mendoza.

DEDICATORIA.

Durante estos escasos cinco años de lucha constante, de gratas vivencias, de momentos de éxitos y también de angustias y desesperanza para poder cumplir mis objetivos y así poder alcanzar un peldaño más de uno de mis mas grandes anhelos, culminar mi carrera, los deseos de superarme y de lograr mi meta son tan grandes que logre vencer todos los obstáculos que hasta ahora se han presentado y es por ello que debo dedicar este triunfo a quienes en todo momento me llenaron de amor y apoyo, y por sobre todo me brindaron su amistad.

A Dios Todopoderoso por iluminarme el camino a seguir, a mis padres Matías Modesto y Rosa María; hermanos Carmen, Juan, Cesar, Martha, Diana, Patricia, Maritza, Tannya; quienes supieron darme apoyo, justo cuando mi voluntad se quebrantaba; a mi esposa Maribel Alexandra y, especialmente va dedicado a mi hija Andrea Alejandra, pues ella es mi motor, es la razón de que haya logrado llegar hasta este punto y a mi futuro hijo, pues será la razón de seguir superándome cada día más.

Jorge Luis Malla Reyes.

AGRADECIMIENTO

En primer lugar a Dios por haberme guiado por el camino de la felicidad; en segundo lugar a cada uno de los que son parte de mi familia a mi PADRE Santiago Mendoza Arroyo, mi MADRE FatimaIllescas Enriques, a mi ESPOSA Andrea Cedeño Domo, mis HIJOS Santiago y Alejandra; a mis hermanos, y un agradecimiento muy especial a la Familia Guamantica Suárez por ser amigos y Jefes en mi lugar de trabajo y por comprender y ayudarme con mi tiempo de trabajo para poder terminar mis estudios sin mayores inconvenientes y por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora. Por último a mi tutor de tesis quién nos ayudó en todo momento.

Alejandro Mendoza.

AGRADECIMIENTOS

A Dios Todopoderoso por iluminarme el camino a seguir y que siempre está con nosotros en los buenos y sobre todo en los malos momentos.

A nuestros maestros Dr. Tito Ramos Viteri, Abg. Ana Maria Tapia Blacio y Abg. Héctor Ramos Ricardo, quienes a más de maestros se convirtieron en grandes amigos.

A nuestras familias por apoyarnos económica y sentimentalmente, este proyecto es de todos ustedes.

A todos nuestros compañeros de estudio, por ser un referente y un apoyo, y a todos y cada uno de nuestros maestros por impulsarnos a seguir siempre adelante en procura de mantener un grupo unido.

A todos, de corazón,

“Gracias”

Jorge Luis Malla Reyes

TRIBUNAL DE GRADO

Ab. Carlos San Andrés Restrepo.
DECANO DE LA FACULTAD
DECIENCIAS SOCIALES Y LA
LA SALUD.

Dr. Tito Ramos Viteri
DIRECTOR DE LA CARRERA
DERECHO.

Ab. Ana Tapia Blacio.
PROFESORA-TUTORA

Ab. Héctor Ramos Ricardo.
PROFESOR DEL ÁREA

Ab. Milton Zambrano Coronado, MSc.
SECRETARIO GENERAL - PROCURADOR

ÍNDICE GENERAL

Tabla de contenido

PORTADA	I
APROBACIÓN DEL TUTOR.....	IV
DEDICATORIA	V
AGRADECIMIENTO	VII
TRIBUNAL DE GRADO	IX
ÍNDICE DE GRÁFICOS	XIII
ÍNDICE DE FIGURAS.....	XIII
ÍNDICE DE CUADROS.....	XIII
ÍNDICE DE ANEXOS	XIV
INTRODUCCIÓN	1
SITUACIÓN ACTUAL DE LA PROBLEMÁTICA.....	2
PROBLEMA DE LA INVESTIGACIÓN.....	3
JUSTIFICACIÓN.....	4
OBJETIVOS.....	7
HIPÓTESIS.....	8
VARIABLES.....	8

CAPÍTULO I

MARCO TEÓRICO

1. Antecedentes	9
1.1.Historia de las computadoras	15
1.1.1. La Electrónica	19
1.1.2. La Informática	20
1.1.3. La Cibernética.....	21
1.1.4. El Ordenador y sus componentes	22
1.1.5. La Internet.....	24

1.2.	Campos de acción de la Informática	29
1.2.1.	La Informática en las Ciencias Naturales	29
1.2.2.	La Informática en las Ciencias Sociales	31
1.3	La Informática en el Derecho	35
1.4	Delito informático	56
1.4.1	Generalidades.....	56
1.4.2	Criminalidad informática	61
1.5	Definición y concepto de delitos informáticos	62
1.5.1	Sujetos del delito informático	65
1.5.2	Sujeto activo	65
1.5.3	Sujeto pasivo.....	67
1.6	Marco jurídico sobre la informática jurídica y los delitos informáticos..	68
1.6.1	Ley orgánica de transparencia y acceso a la información pública	70
1.6.2	Ley de comercio electrónico, firmas electrónicas y mensajes de datos	71
1.6.3	Ley de propiedad intelectual	74
1.6.4	Ley especial de telecomunicaciones	76
1.6.5	Ley orgánica de control constitucional.....	76
1.6.6	Código de procedimiento penal y código de procedimiento civil	77
1.7	Propuestas internas	78
1.7.1	Departamento de criminalística de la policía judicial.....	79
1.7.2	Unidad de delitos informáticos del ministerio público.	81
1.8	Propuestas externas.....	84
1.8.1	Contemplaciones de la organización de estados americanos (OEA)	84
1.8.2	Regulaciones existentes en Latinoamérica	86

CAPÍTULO II

MÉTODOLOGÍA DE LA INVESTIGACIÓN

2.1.	Validación metodológica	88
2.2.	Métodos y técnicas aplicadas para el levantamiento de información	88
2.3.1	Tipo de investigación seleccionada	89

2.3.2	Descriptiva	89
2.3.3	Exploratoria	90
2.3.4	Bibliográfica	9
2.3.5	Campo	91
2.3.6	Documental	91
2.3.7	Fuentes secundarias	91
2.3.7.1	Encuesta	92
2.4	Selección del tamaño de la muestra.....	92
2.5	Descripción de la información obtenida	93
2.6	Análisis e interpretación de los resultados.....	94
2.7	Construcción del informe de la investigación.....	94
2.8	Conclusiones y recomendaciones.....	104

CAPÍTULO III

PROPUESTA

3.1.	Creación de un modulo practico acerca de delitos informáticos para ser implementado a la malla curricular de la Carrera de derecho de la Universidad Estatal Península de Santa Elena.....	106
3.1.2.	Alcance	106
3.2.	Responsabilidades para la aplicación del programa de capacitación	107
3.3.	Visión	107
3.4.	Misión	107
3.5.	Justificación	107
3.6.	Fundamentación	108
3.7.	Objetivos	108
3.7.1.	Objetivo general	108
3.7.2.	Objetivos específicos	108
3.8.	Importancia	109
3.9.	Ubicación sectorial y física	109
3.10.	Factibilidad	110

3.11.	Plan de trabajo.....	110
3.12.	Actividades	110
3.13.	Costo total del proyecto.....	114
3.14.	Impacto	114
3.15.	Evaluación	115
	BIBLIOGRAFÍA	117

ÍNDICE DE CUADROS

CUADRO 1.	Infracciones informáticas	77
CUADRO 2.	Departamento de criminalística	80
CUADRO 3.	Legislación de países latinoamericano.....	87
CUADRO 4.	Objetos de investigación.....	93

ÍNDICE DE FIGURAS

FIGURA 1.	Marco jurídico sobre la informática jurídica.....	68
FIGURA 2.	Unidad de Delitos Informáticos.....	83

ÍNDICE DE GRÁFICOS

	Pags.	
Gráfico 1.	Encuesta a estudiantes.....	96
Gráfico 2.	Procedimiento.....	97
Gráfico 3.	Importancia sobre el tema	98
Gráfico 4.	Delitos Informáticos	99
Gráfico 5.	Importante el tema para la preparación profesional.....	100
Gráfico 6.	implementar en la malla curricular de la Carrera.....	101
Gráfico 7.	Encuesta a funcionarios judiciales	102
Gráfico 8.	capacitados para litigar en este tipo de causas.....	103

ANEXOS

Formato de Encuesta a los estudiantes.....	120
Formato de Encuesta a los docentes.....	121
Formato de Encuesta a autoridades judiciales.....	122
Fotografías	123

INTRODUCCIÓN

UBICACIÓN Y CONTEXTUALIZACIÓN DE LA PROBLEMÁTICA

El tema a investigarse es “ESTUDIO DEL TRATAMIENTO DE LOS DELITOS INFORMÁTICOS DENTRO DE LA PENÍNSULA DE SANTA ELENA”, la misma que se encuentra al este de nuestro territorio nacional, y que cuenta con una población de Santa Elena tiene una superficie de 3,762.8 kilómetros cuadrados (1.46 % del total nacional) y con una población residente de 308.000 habitantes (2 % del total nacional) y una población flotante superior a 200,000 personas en época alta de turismo, básicamente turistas de la ciudad de Guayaquil y otros cantones de la Provincia del Guayas y del país.

Eran pocos los habitantes de la península que contaban con Internet fijo en sus casas pues no existía un proveedor de Internet fijo (ISP) en la provincia. Sin embargo, esto ha venido cambiando con el uso de modems móviles. Aún, la mayoría de usuarios lo hacen a través de cyber cafés o mediante conexión telefónica ([dial-up]) de compañías que han instalado nodos de conexión con números de acceso de Salinas.

Un importante hecho es la instalación del cable submarino de fibra óptica cuyo punto de conexión con tierra firme es la playa de Punta Carnero, situada en la parroquia José Luis Tamayo del cantón Salinas. El 15 de noviembre de 2007 se suscribe el acta de puesta en operaciones por la Superintendencia de Telecomunicaciones (Suptel) y Telefónica International Wholesale Services Ecuador (TIWS). La instalación permite intercambio de datos con una velocidad de 10 gigabits/segundo y une al país con la red del sistema Sudamérica-1 (SAM-1) cuyo punto final es Florida, Estados Unidos.

En la actualidad, la península cuenta con diversas instituciones bancarias, como por ejemplo, cuatro agencias del Banco del Pichincha, cuatro del Banco de Guayaquil, dos del Banco del Pacífico, dos del Banco Bolivariano, dos del Produbanco, una del Banco del Austro, una del Banco Rumiñahui, además de contar con varias Cooperativas de ahorro y crédito, como por ejemplo la Huancavilca, 29 de Octubre entre otras.

Al constituirse en provincia, la península ya cuenta con una Corte Provincial de Justicia, y con tres fiscalías, una en cada cantón y con respecto a la materia que nos compete en la presente investigación, contamos con dos juzgados en la materia penal.

SITUACIÓN ACTUAL DE LA PROBLEMÁTICA

En la actualidad las empresas privadas han experimentado transformación en algunos aspectos de seguridad; la situación actual nos da a conocer que los sistemas informáticos son el activo más valioso y al mismo tiempo el más vulnerable.

La seguridad informática ha adquirido gran auge, dada las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que converge en la aparición de nuevas amenazas en los sistemas informáticos.

Generalmente no se invierte ni el capital humano ni económico necesario para prevenir el daño y/o pérdida de la información confidencial en las empresas, a raíz

de ello han surgido muchos problemas relacionados con el uso de computadoras, amenazas que afectan negativamente tanto a individuos como a empresas; la proliferación de la computadora como la principal herramienta, así como la creación de la red global Internet ha provocado que cada vez más personas se las ingenien para lucrar, hacer daño o causar perjuicios.

El acceso no autorizado a un sistema informático, consiste en acceder de manera indebida, sin autorización, a un sistema de tratamiento de información, con el fin de obtener una satisfacción de carácter intelectual y/o económico por el desciframiento de los códigos de acceso o password.

La idea de la investigación es desarrollar una herramienta completa que permita llevar a cabo una auditoría para conocer el estado actual de la seguridad informática, permitiendo también proponer alternativas de mejoras a éstas

PROBLEMA DE INVESTIGACIÓN

¿Cómo brindar una optima capacitación a los estudiantes de la Carrera de Derecho de la Universidad estatal Península de santa Elena, acorde a los avances tecnológicos?

DELIMITACIÓN DEL PROBLEMA.-

La presente investigación comprenderá la realización de un modulo de aplicación que contenga aspectos relacionados con los delitos informáticos, el mismo que irá

enfocado a la aplicación en la formación de los estudiantes de la carrera de Derecho de la Universidad Estatal Península de Santa Elena.

El tiempo estimado para la elaboración del trabajo será de 3 meses a partir de la aprobación del perfil del proyecto de tesis.

El tiempo de vigencia de la propuesta estará definido por parte de la carrera de Derecho de la Universidad Estatal Península de Santa Elena, si ésta toma positivamente el proyecto de modulo de aplicación.

JUSTIFICACIÓN.-

Ya que la legislación de otros países en torno a un problema de seguridad jurídica que involucra a toda una Nación está en avance, es necesario plantearse de cómo está planteado en nuestro Código Penal el tratamiento sobre en los delitos informáticos. ¿Qué son estos mismos?, ¿Cómo están abarcados?, en nuestra opinión resulta importantísimo que se abarque un tema especial, ya que en Ecuador, existe únicamente tipificación de los delitos informáticos y electrónicos en pocas legislaciones vigentes. El delito informático en el Código Penal Ecuatoriano ha sido previsto como una modalidad de forma agravada de hurto agravado, lo cual trae inconvenientes, teniendo en cuenta la forma tradicional de comprender los elementos del delito de hurto. Así mismo, existen conductas vinculadas a los delitos informáticos que, en algunos casos, pueden configurar otro tipo de delitos, como por ejemplo, el delito de daños; consistentes en la destrucción de base de datos La sociedad y sobre todo juristas y litigantes estarían muy interesados en conocer la manera en que podrían defenderse si se convierten en sujetos pasivos de dichos delitos.

No existe argumento estricto y concienzudo alguno por el cual no se deberían tipificar en todas las legislaciones penal eso en particular los delitos electrónicos y los informáticos, ya que en la doctrina Ecuatoriana se establece que todo hecho que genere una conducta indebida debe ser tipificada en la legislación correspondiente. Cuando en un país no se tipifica en todas las legislaciones locales correspondientes algún delito que se suscite continuamente debido como es el caso que estamos investigando, a avances tecnológicos como lo son la firma electrónica para el pago de impuestos, etc., que son actos que la propia autoridad solicita, se trata de justificar lo injustificable ya que día a día se cometen fraudes electrónicos millonarios los cuales hasta nuestros días difícilmente han podido defenderse debido a la falta de legislación de estos delitos. A manera de recomendación, sería conveniente la creación de un tipo autónomo que sancione las conductas vinculadas al delito informático.

Es importante conocer sobre los procedimientos que se utilizan para cometer los delitos informáticos, así como aquellos delitos tradicionales tipificados en nuestro ordenamiento jurídico y que se valen de la tecnología para su consumación.

Las personas que hacemos uso constante de la informática, del Internet sabemos los pasos a seguir para poder obtener información, realizar pagos u otros actos sin embargo, desconocemos la forma cómo es que funcionan estos mecanismos, los cuales muchas veces son empleados para cometer delitos informáticos y otros delitos tradicionales que se apoyan en la tecnología para su comisión.

Esta investigación sólo tomará en cuenta el estudio y análisis de la información referente al problema del Delito Informático, tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juega la Informática ante éste tipo de hechos.

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

Con la aplicación del presente trabajo de investigación, lograremos que la comunidad peninsular tome conciencia de la importancia de estar informados, en lo referente a este tema, puesto que cada vez dependemos más de la tecnología.

Además, esta tesis, va dirigida a los estudiantes de la carrera de derecho de la Universidad estatal península de Santa Elena, ya que al poner a su alcance el conocimiento pormenorizado de este tipo de infracciones, estaremos preparando futuros profesionales capacitados en el tema.

CAMBIOS ESPERADOS CON LA INVESTIGACIÓN

Con la aplicación del presente trabajo de investigación, lograremos que la comunidad peninsular tome conciencia de la importancia de estar informados, en lo referente a este tema, puesto que cada vez dependemos más de la tecnología.

Además, esta tesis, va dirigida a los estudiantes de la carrera de derecho de la Universidad estatal península de Santa Elena, ya que al poner a su alcance el

conocimiento pormenorizado de este tipo de infracciones, estaremos preparando futuros profesionales capacitados en el tema.

Que la comunidad peninsular tome acciones preventivas para no ser víctimas de este tipo de delito.

OBJETIVOS.-

OBJETIVOS GENERALES

Crear un manual que pueda ser aplicado en los niveles de estudio pertinentes tanto en la carrera de Derecho como en la carrera de ingeniería en Sistemas de la Universidad Estatal Península de Santa Elena

OBJETIVOS ESPECÍFICOS.

- Dar a conocer a la comunidad el procedimiento a seguir cuando se es víctima de un delito informático.
- Análisis del funcionamiento de la unidad de delitos informáticos de la policía de la Península de Santa Elena.
- Conceptualizar la naturaleza de los Delitos Informáticos
- Estudiar las características de este tipo de Delitos
- Tipificar los Delitos de acuerdo a sus características principales
- Investigar el impacto de éstos actos en la vida social y tecnológica de la sociedad

- Analizar las consideraciones oportunas en el tratamiento de los Delitos Informáticos
- Mencionar las empresas que operan con mayor riesgo de ser víctimas de ésta clase de actos

Analizar la Legislatura que enmarca a ésta clase de Delitos, desde un contexto Nacional e Internacional.

HIPÓTESIS GENERAL.

El conocimiento del tema de Delitos Informáticos es importante para mejorar la capacitación profesional de los estudiantes de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena.

VARIABLE INDEPENDIENTE: La falta de capacitación a los estudiantes de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena, en lo referente al tema de Delitos Informáticos.

VARIABLE DEPENDIENTE: La falta de preparación pre profesional de los abogados en el libre ejercicio de la profesión, conlleva a que no se encuentren capacitados para patrocinar casos que versen acerca de delitos informáticos.

CAPÍTULO I

MARCO TEÓRICO.

1. ANTECEDENTES.

De acuerdo con la definición elaborada por un grupo de expertos en mayo de 1983, el término delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesamiento automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales. Existen delincuentes de la informática que pueden sabotear las computadoras para ganarle ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión, ya sea directamente o mediante los llamados “gusanos” o “virus”, que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro.

En 1990, se supo por primera vez en Europa de un caso en que se usó un virus para sacar dinero, cuando la comunidad de investigación médica se vio amenazada con un virus que iría destruyendo datos paulatinamente si no se pagaba un rescate por la “cura”. Pero a medida que se va ampliando la Internet, asimismo va aumentando el uso indebido de la misma. Los denominados delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o “piratería informática”, el fraude, el sabotaje informático, la trata de niños con fines pornográficos y el acecho. En los años recientes las redes de computadoras han crecido de manera asombrosa. Hoy en día, el número de usuarios que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos online.

El problema radica en que, la conducta humana parece ser que está inclinada al delito, a conseguir satisfacción a sus deseos a toda costa. Con el desarrollo de la informática, aparece también lo que se denomina como: DELITO INFORMÁTICO.

De la misma manera que muchas personas se han dedicado a desarrollar sistemas de computación para solucionar problemas de la sociedad, otras tratan de utilizar la tecnología, y en el caso que nos ocupa, las computadoras y sistemas, para el cumplimiento de actividades ilícitas.

De la misma forma como se encuentran cosas positivas en el INTERNET, encontramos cosas negativas, lo cual nos lleva a pensar que el mal no está en la tecnología sino en las personas que las usan, a modo de ejemplificación diremos que la red de comunicación electrónica digital, se la ha utilizado por pederastas para estimular la prostitución infantil, del mismo modo grupos políticos racistas neo nazis lo han usado para difundir su nefasta ideología, se cree, inclusive, que el INTERNET es una vía de comunicación y negocios entre narcotraficantes y contrabandistas de armas, etc.

El Ecuador, en abril de 2002, expide la Ley de Comercio, Firmas Electrónicas y Mensajes de Datos, instrumento que da un marco jurídico a las innovaciones tecnológicas relacionadas con la transmisión de información utilizando medios electrónicos. El objeto de la Ley es la de regular los mensajes de datos, firmas electrónicas, servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico (e-business) y lógicamente la protección a los usuarios de estos sistemas de cualquier mecanismo de distorsión.

Gracias a la expedición de esta Ley, nacen como delitos con características propias el sabotaje (SPAM) y los daños informáticos (CYBER CRIME). Estas infracciones se incorporan al Código Penal ecuatoriano, logrando así una

protección concreta y específica a este tipo de actos, considerados desde abril de 2002 como delitos. Ahora bien, dentro de la regulación propia de los mensajes de datos, también se prevé mecanismos de protección propios en donde se enuncian principios y procedimientos que se deben respetar.

La Ley establece que los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Estos consisten en documentos que han sido enviados por un sistema electrónico, a los cuales se les da plena validez.

El artículo 5 de la Ley establece principios sobre confidencialidad y reserva: "se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia". Se establecen principios que armonizan con disposiciones constitucionales. La inviolabilidad y el secreto de la correspondencia es una garantía establecida en la Constitución, recogida en el numeral 13 del artículo 23, así como el numeral 14 del artículo 24.

Todos los mensajes están amparados por estas disposiciones, independientemente de la forma de envío y sin consideración de su medio o intención. La reserva protege el tratamiento de datos de carácter personal y la libre circulación de estos, en lo que se refiere a las comunicaciones comerciales y a la responsabilidad de los intermediarios. El Estado ecuatoriano garantiza la confidencialidad mediante cualquier forma de interceptar o vigilar esas comunicaciones por parte de cualquier persona que no sea su remitente o destinatario salvo que esté legalmente autorizada. En el caso de que se violen estos principios, existen mecanismos constitucionales de control legal.

Con relación a la protección de datos, para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o

transmisión de mensajes, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información que quiera compartir con terceros. Según el segundo y tercer párrafo del artículo 9 de la Ley, "la recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución de la República y esta Ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato".

La norma protege a la elaboración, transferencia o utilización de bases de datos, siempre enmarcada dentro de principios de confidencialidad y privacidad. En cualquiera de estos casos, es un requisito sine qua non el consentimiento del titular, pero no será necesario este consentimiento expreso cuando se trate de situaciones que generen correspondencia entre las partes para crear una base de datos.

Resumiendo, vemos que existen principios constitucionales y legales de protección a la información que consta en una base de datos. Los mensajes que se generen, deben estar acompañados siempre de criterios y parámetros de respeto al bien ajeno y a la propiedad privada. Por esto se requiere el consentimiento para que sea posible disponer del mensaje recibido o sujeto de envío. También es importante resaltar que se prohíben las bases de datos y la recopilación de direcciones electrónicas, salvo que exista un consentimiento por parte del dueño o sea producto de funciones propias que se desempeñen entre partes y que se vayan generando con el transcurso del tiempo. La Ley considera que si se recopila y usan datos personales sin el consentimiento previo, existe una violación flagrante

a los derechos de la privacidad, confidencialidad e intimidad que se encuentran garantizados por la Constitución.

El campo de aplicación de la Ley de Comercio y Firmas Electrónicas está dado básicamente por relaciones contractuales amparadas en el campo civil, aunque también, de menor manera, tiene injerencia dentro del ámbito penal. Este ámbito está dado concretamente dentro de lo que ésta misma considera como infracciones informáticas. La Ley agregó al Código Penal una serie de infracciones antes no contempladas para sancionar este tipo de delitos.

Hay dos artículos que revisten importancia dentro de los delitos electrónicos de SPAM y CYBER CRIME. Se agrega a continuación del artículo 553 del Código Penal el siguiente artículo:

"Falsificación electrónica: son reos de falsificación electrónica la persona o personas que con el ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, ALTEREN O MODIFIQUEN MENSAJES DE DATOS, O LA INFORMACIÓN INCLUIDA EN ÉSTOS, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial; Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad.

Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones de las que hubieren hecho".

Para tener una idea sobre la ubicación de la norma dentro del Código Penal, el legislador ha considerado que estos delitos se deben encasillar dentro de los delitos contra la propiedad y concretamente dentro del delito de robo.

Esta disposición protege al consumidor de cualquier tipo de información que sea falsa. Cuando se refiere a información comercial que induzca a error o engaño, la Ley de Defensa del Consumidor establece protecciones y sanciones para evitar que este tipo de prácticas se generalicen, lógicamente, protegiendo al consumidor para que no se le oferte un producto de una calidad y reciba otra de distinta a la ofertada. La Ley de Defensa del Consumidor no establece de manera expresa una protección al consumidor, pero si de manera general, principios de aplicación que se pueden aplicar para este caso en concreto.

A lo largo de la historia el hombre ha necesitado transmitir y tratar la información de forma continua. Aun están en el recuerdo las señales de humo y los destellos con espejos, y más recientemente los mensajes transmitidos a través de cables utilizando el código Morse, o la propia voz por medio del teléfono. La humanidad no ha cesado en la creación de métodos para procesar información. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de estas máquinas y métodos, y además con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo o de gestión.

Luego nace Internet como una tecnología que pondría la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo, delincuentes diversos encontraron el modo de contaminarla y lo que es peor impunemente.

La contaminación es de la más variada, entre los últimos ataques a la red y que podemos calificar como de los mas graves es el uso de la red por parte de la mafia internacional que maneja la prostitución infantil, por el terrorismo internacional y también por el narcotráfico. Respecto de éste último es dable destacar la

importancia de la penalización del delito del "Narcoterrorismo" según lo establecieran los fundamentos para el proyecto de ley realizado por el Dr. Ricardo Levene nieto, no solo en nuestro país sino en el mundo, ya que en todo el globo no se ha tipificado el mismo como delito autónomo.

Políticos de algunos países han pedido que se reglamente el uso de la red, de modo que quienes prestan el servicio de Internet registren a los clientes, cuándo y dónde llaman y para que, pero la iniciativa hizo que, en defensa de la libertad y de la privacidad, muchos usuarios honestos y algunas empresas que participan de los beneficios económicos de la red, protestaran enérgicamente. El desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas.

Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas para infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

El objetivo de este trabajo es analizar, Las conductas delictivas que pueden generar el gran avance tecnológico, sobre todo en el campo de la informática" desde tres de puntos de vista: normativo, delincuencia y prevención

En el presente apartado se analizarán los antecedentes y diversas definiciones en el mundo y en Ecuador de conceptos importantes tales como de la informática, la electrónica, la cibernética, la Internet. La Informática es una ciencia como el Derecho, para una mejor comprensión de los Delitos Informáticos.

1.1. HISTORIA DE LAS COMPUTADORAS.

Durante siglos el hombre ha buscado formas para facilitar y simplificar su existencia ya sea con herramientas o maquinarias, la historia de los aparatos para

calcular y computar remonta a miles de años atrás. El primer aparato de este estilo que existió fue y es el ábaco con una antigüedad de más de 5,000 años ya de origen perdido en el tiempo apareció en diversas culturas.

El código de Hammurabi da a conocer referencias del uso de este ingenioso invento tanto en contratos, bonos, recibos, inventarios y transacciones de compra – venta. La palabra "ábaco" es una palabra latina del griego "abax" o "abakon", que significa "superficie plana" o "tabla". Es posible que sea originado de la palabra semítica Abaq que significa "polvo". En China fue conocido como Suan Pan, en Japón Soroban, en Corea Tschu Pan, en Vietnam BanTuan o BanTien, en Rusia Schoty, en Turquía Coulba y en Armenia Choreb.

Leonardo da Vinci (Italia, 15 de abril de 1452 – Francia, 2 de mayo de 1519) trazó las ideas para una sumadora mecánica, había hecho anotaciones y diagramas sobre una máquina calculadora que mantenía una relación de 10:1 en cada una de sus ruedas registradoras de 13 dígitos.

A pesar de este ingenioso invento, aún persistían problemas en la realización de ciertas operaciones, por lo que Jhon Napier (Edimburgo, 1550 - 4 de abril de 1617) crea la Tabla de Logaritmos con lo que permitió realizar multiplicaciones y divisiones de manera sencilla y rápida pero aún con sus problemas por lo que fue inventada la Regla de Cálculo, aparato más sencillo y rápido de usar pero muy inexacto a través de mediciones de longitudes entre dos reglas. Durante más de 200 años, la regla de cálculo es perfeccionada, convirtiéndose en una calculadora de bolsillo, extremadamente versátil.

Blas Pascal (19 de junio de 1623 - 19 de agosto de 1662), a los 18 años de edad creó una máquina capaz de realizar operaciones mediante un mecanismo de ruedas dentadas basadas en las ideas de Leonardo da Vinci, la cual fue conocida como la primera máquina calculadora de la historia, también desarrolló la teoría de las probabilidades, piedra angular de las matemáticas modernas. Con las

limitaciones de la Pascalina a sumas y restas, Gottfried W. von Leibnitz mejoró esta máquina con la inserción de un cilindro con lo cual permitió que la Pascalina pudiera multiplicar dividir e incluso realizar raíces cuadradas.

Con la llegada de las máquinas de telar automáticas por Joseph Jackard en 1801 mediante tarjetas perforadas que guiaba a la maquinaria a realizar el mismo modelo una y otra vez sin perder detalle entre sí, siendo éste el inicio del sistema de las tarjetas perforadas y de automatización, con lo que permitió controlar por primera vez una máquina con instrucciones codificadas. Para 1823 Charles Babbage matemático inglés y científico de la computación, con apoyo del gobierno Inglés ideó una máquina denominada “Maquina Diferencial” capaz de realizar diversos tipos de operaciones, almacenar información y resolver todo tipo de problemas además de entregar el resultado impreso, pero siendo muy ambicioso para su época esta máquina jamás pudo terminarse por causas mecánicas causando cambio de diseño sin poder concordar la idea original y la terminación del apoyo del gobierno inglés.

Años después Charles Babbage ideó su Máquina Analítica, con lo que se podía idear operaciones más complejas de manera rápida además de almacenar datos en un dispositivo interno tomando la idea de las tarjetas perforadas, siendo esta la base para la creación de las computadoras, pero aún así no pudo concretarse.

Los primeros y verdaderos inicios en lo que hoy conocemos como computadoras se debe a Herman Hollerith, miembro del censo de los Estados Unidos de Norte América que basado en la idea de las tarjetas perforadas realizó una máquina la cual podía guardar de manera automática el registro de las personas censadas mediante perforaciones en los rasgos de las personas conociéndose como “Fotografías perforadas”.

El primer paso se dio entre 1939 y 1944 con la subvención de IBM (International Business Machines) la Universidad de Harvard creó la Mark I de 16 metros de

largo y 2,5 metros de alto, contenía un aproximado de 800.000 piezas y más de 800 Km. de cableado eléctrico, la cual empleaba señales electromagnéticas para mover las partes mecánicas, su programación dependía de la idea inicial de las máquinas analíticas mediante una cinta perforada, esta máquina podía realizar cualquier tipo de operaciones aunque de una manera relativamente lenta debido a la complejidad de la maquinaria interna.

Dos años después fue creada la ENIAC (Electronic Numerical Integrator And Computer) por J.P.Eckert y J.W.Mauchly en la Universidad de Pensilvania Estados Unidos, conocida como la primer computadora electrónica de la historia, pesaba 30 toneladas y ocupaba un espacio de 450 m², llenaba un cuarto de 6 metros x 12 metros y contenía 18.000 bulbos, tenía que programarse manualmente conectándola a 3 tableros que contenían más de 6000 interruptores. La ENIAC operaba con “uno decimal” y notablemente superior la MARK I, dando así el nacimiento de una nueva era abarcando periodos determinados basados en las características del sistema físico o lógico conocidas como Generaciones, dividiéndose en las siguientes:

La Primer Generación: Construidas entre 1950 y 1960 conocidas como las primeras máquinas comerciales, las cuales su estructura básica consistía con la llamada válvula al vacío, lo que permitió su fácil funcionamiento y eran capaz de realizar mil operaciones por segundo y almacenar hasta 20,000 posiciones.

La Segunda Generación: Construidas entre 1960 y 1965 su principal característica consistía en la introducción de elementos electrónicos básicos como el transistor el cual determinaba el paso de corriente entre dos puntos, este tipo de tecnología marcó una gran pauta en la creación de computadoras revolucionando la industria con el ahorro de energía y espacio además de la veracidad y velocidad de cálculo.

La Tercera Generación: Construidas entre 1965 a 1975 su funcionamiento y contracción se basaba en el uso de los circuitos integrados el cual podía abarcar

hasta 20,000 componentes en 25 m², lo que permitía que ésta pudieran abarcar menos espacio a comparación de sus predecesoras.

La Cuarta Generación: Construidas a partir de 1975 hasta nuestros días, se caracteriza esta generación por la integración de 60,000 componentes en un circuito integrado de 25 mm², la aparición del microprocesador, la contracción de computadoras personales y microcomputadoras lo que dio origen a la expansión de las computadoras por el mundo, y la especialización de las aplicaciones de la informática lo que trajo consigo la llamada “inteligencia artificial”, telecomunicaciones, tratamiento electrónico de las imágenes y base de datos.

La Quinta Generación: Fue un proyecto lanzado por Japón en los años 70s con el fin de crear computadoras con inteligencia artificial, un procesamiento paralelo y un nivel propio de lenguaje de máquina, el proyecto duró diez años sin poderse lograr.

1.1.6. La Electrónica.

Para poder entender la diferencia esencial entre un delito informático y los conocidos como los delitos electrónicos, es necesario entender lo que es la Electrónica y qué es la Informática, que consiste en: “Parte de la ciencia que estudia los fenómenos que intervienen electrones en estado libre”.² Lo cual prácticamente no dice nada, por lo que la electrónica como técnica: “es el estudio y aplicación del comportamiento de los electrones en diversos medios, como el vacío, los gases y los semiconductores, sometidos a la acción de campos eléctricos y magnéticos”.

Para poder entender de una manera sencilla en su funcionamiento dentro de un aparato electrónico se tiene que tomar en cuenta que el flujo de estos electrones genera corriente eléctrica y ésta a su vez usada en dispositivos cambian la energía

eléctrica en calor, luz o movimiento, a lo que se conoce como Eléctrica, pero usada en dispositivos provistos de inteligencia surge lo que es una radio, una televisión y una computadora y es conocida como Electrónica.

1.1.7. La Informática.

Siendo que los aparatos informáticos son electrónicos pero no necesariamente todos los aparatos electrónicos son informáticos, como el ejemplo de que una licuadora a comparación de una computadora. Ya siendo parte esencial el flujo de corriente eléctrica para transformarlo en otro tipo de energía de ambos, la palabra clave es el procesamiento de información, dando nacimiento a la informática, siendo esta: “una rama del saber humano que se ocupa de todo lo relacionado con las computadoras, su comportamiento, su diseño y desarrollo de todo tipo de programas de computadoras (desde los sistemas operativos hasta los más modesto programas de aplicación) operación y uso de las computadoras”⁴.

Es una rama de la ingeniería que estudia el tratamiento de la información mediante el uso de máquinas automáticas. Proviene del francés INFORMATIQUE que a su vez por la conjunción de las palabras información y AUTOMATIQUE, para dar idea de la automatización de la información que se logra con los sistemas computacionales.

La Informática es un amplio campo que incluye los fundamentos teóricos, el diseño, la programación y el uso de las computadoras (ordenadores) como herramienta de solución de problemas.

Esto puede ser entendido como la interpretación y procesamiento lógico de los impulsos eléctricos de manera ordenada, por ejemplo, los audio cassettes, éstos poseen las cintas magnéticas, el cual su funcionamiento básicamente consistía en que a través de esta cinta plástica quedaba un registro magnético entre una

combinación lógica y ordenada de cargas positivas y negativas por así decirlo, que en el caso de un audio cassettes estaban acomodados según las vibraciones generadas por el sonido pero en el caso de dispositivos informáticos como lo son los disquetes o discos flexibles esta relación ordenada de cargas son entendidos como “ceros y unos”, el lenguaje binario; están procesadas y entendidas lógicamente y matemáticamente mediante una computadora permitiendo reproducir o almacenar información.

1.1.8. La Cibernética.

Cibernética: “del griego κυβερνητική: Piloto o el arte de pilotear un navío”.⁵ Aunque Platón la utilizó en La República con el significado de "arte de dirigir a los hombres" o "arte de gobernar".

Las investigaciones con fines militares a partir de la segunda guerra mundial propiciaron la creación del concepto moderno de la Cibernética moderna: como una ciencia de la comunicación y el control.

Otra forma de entender a la Cibernética moderna es como: “Estudio de las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas y en particular, el de las aplicaciones de los mecanismos de regulación biológicas a las tecnológicas”.⁶

- Orígenes de la Cibernética:

En 1948 el matemático norteamericano Norbert Wiener (1894-1964) en su obra “Cibernética o el control y comunicación en animales y máquinas” (Cybernetics, or control and communication in the animal and machine) publicada en 1948, el cual empleó el término para designar a la nueva ciencia de la comunicación y control entre el hombre y la máquina.

- Diferencia entre Cibernética y la Informática.

Un punto importante es resaltar la diferencia que existe entre la Informática y la Cibernética que vistos de cierta manera parecerían que son iguales, pero aunque guardan una relación entre sí las partes que lo componen no son iguales.

La Cibernética es la ciencia que trata de explicar y dar solución a eventos de control y comunicación ya sean fenómenos acontecidos en la naturaleza, sociedad o humanos, de tal manera la Informática busca desarrollar máquinas capaces de “Inteligencia Artificial”, simular actividades y capacidades humanas como la robótica, la búsqueda de solución de problemas y la toma de decisiones por sí mismas, conocido como Heurística o Método Heurístico.

1.1.9. El Ordenador y sus componentes.

El concepto ordenador fue usado por el matemático Húngaro –Estadounidense John Von Newman (1903-1957) con el fin de simplificar su propia máquina que podía realizar cálculos.

La Computadora es: “una máquina electrónica analógica y digital, dotado de una memoria de tratamiento de la información, capaz de resolver problemas matemáticos y lógicos mediante la utilización automática de programas.”⁷

Entendido de otra manera una computadora es un “dispositivo electrónico complejo que puede ser programado para recibir, almacenar, procesar, transmitir y presentar”⁸.

Ésta se compone de dos elementos esenciales, el SOFTWARE y el HARDWARE, parte importante para una computadora y relacionadas entre sí ya que una no puede existir sin la otra.

El Hardware son los componentes físicos y materiales, en conjunto o separados, electrónicos, electromecánicos o mixtos, que compone el equipo lógico e informático en una computadora. El Software es la parte intangible de una computadora como un conjunto de instrucciones con las que el usuario y el sistema informático interactúan para realizar determinadas tareas.

Las partes que componen a una computadora se dividen en 3:

- 1) Unidades de Entrada.
- 2) Unidades de Salida.
- 3) Unidades de Procesamiento, Almacenamiento o Memoria.

La Unidad de Entrada. Está constituida de todos aquellos dispositivos con los cuales se permite ingresar datos e información además del manejo de programas informáticos, éstos se componen de: el teclado, el mouse (ratón), tablero digitalizado, lector de discos compactos (CD ROM, DVD), sistemas de lectores de tarjeta, unidades de almacenamiento (Memorias USB Flash), reconocimiento de voz y unidades de disco.

Las Unidades de Salida. Son todos los dispositivos físicos en los cuales permite representar la información susceptible a ser apreciados, éstos son pantallas, bocinas, impresoras de papel y en tres dimensiones.

Las Unidades de Procesamiento, Almacenamiento o Memoria. Es aquella en la que la información es almacenada analizada y procesada, consisten en: discos duros, (HardDisk Drive), discos Flexibles (Floppy Disk Drive de 8, 5 ¼, 3 ½ pulgadas), procesadores (micro procesadores), unidades de almacenamiento (tarjetas de memoria, memorias USB flash).

Dentro de la capacidad de almacenamiento existen dos tipos de memoria la primera llamada RAM (RandomAccessMemory) la cual consta de pequeñas

celdas en un chip que almacenan de forma temporal gran parte de la información, entre mayor memoria RAM tenga una computadora mayor velocidad operará. La otra memoria es la ROM (ReadOnlyMemory) consta en memoria semiconductora de lectura utilizada para almacenar datos que nunca necesitan modificarse.

1.1.10. La Internet.

Para poder entender los delitos informáticos es necesario poder entender lo que es la Internet, que es un conjunto de servidores conectados entre sí mediante un sistema maestro de computadoras dentro de una red alrededor de todo el mundo.

- Historia de la Internet en el mundo.

La Internet fue concebido por el Ministerio de Defensa de los Estados Unidos de América con el fin de lograr crear una red de computadoras interconectadas que no dependiera de una computadora central con el fin de que en ataques la información no comprometida se encontrara protegida en su totalidad o en parte, así como en la funcionalidad de la red que se vería comprometida al destruir el servidor central.

En 1960 empezó a desarrollarse un sistema de red en que las computadoras interconectadas no dependieran de un servidor central sino que cada computadora 13 actuase de manera independiente de las otras, con lo que nació la idea de ARPANET⁹ (AdvancedResearchProjects Agency Network), con lo cual para el funcionamiento de esta red fue necesario la creación de procesadores especiales denominados Procesadores de Mensaje de Interfaz (IMP en sus siglas en inglés), el cual el primer procesador de este tipo entró en funcionamiento el 1 de Agosto de 1969 en la Universidad de California de los Ángeles E.U.A, con una computadora Honetwell 516 con una memoria de 12 MB de memoria¹⁰, extendiéndose a otras Universidades del país dando origen a ARPANET. Para 1972 se habían instalado 37 Procesadores de Mensaje de Interfaz. ARPANET fusionaba con un programa denominado Network Control Protocol (NPC)¹¹,

facilitando su uso debido a que era compatible con diversas computadoras y programas operativos creciendo de tal forma que los propósitos militares del ministerio de defensa fueron cambiados por los fines científicos y educativos de las Universidades en los que se encontraba ya instalado.

Para 1980 el NPC fue sustituido por TCP/IP un programa más eficiente el cual convertía la información en pequeños paquetes los cuales pueden ser enviados a diversos puntos con base a su dirección a través de diferentes puntos de enlace de Internet y la computadora de destino, en este mismo año ARPANET se desligó por completo de sus objetivos militares a los que fue diseñado.

En 1986 se fundó la NSFNET (NationalScienceFoundation's Network) financiada por el gobierno de los Estados Unidos de América creando diferentes líneas de enlace para Internet facilitando la transferencia de datos dando lugar a la expansión de la Internet fuera del país, para 1995 NSFNET intentó crear una política de uso científico y no comercial para la Internet lo cual no fue aplicado debido a la privatización de la Internet extendiendo su uso a niveles comerciales.¹²

- Servicios en la Internet.

Al convertirse la Internet en un sistema abierto, éste realiza dos funciones importantes la primera como medio de comunicación y la segunda como medio de información.

Como medio de comunicación, la red entre computadores permite la comunicación entre sí y entre los usuarios realizada mediante cable telefónico o conexión por línea de alta velocidad o banda ancha DSL, debido a esto cualquier computadora puede conectarse a Internet sólo debe contar con el respectivo MODEM y un servidor de un proveedor de Internet el cual debe tener acceso a la espina dorsal del mismo Internet (backbone). Los medios de comunicación más populares en la Internet se encuentran en el Correo Electrónico (e-mail), la

comunicación mediante foros de discusión, servidores de lista y mensajeros instantáneos.

El Correo Electrónico. Permite el libre intercambio de información y datos a través de un servicio de red mediante sistemas de comunicación electrónicos, comparado con el correo ordinario, es más barato y rápido debido a que en cuestión de segundos pueden ser enviados datos e información, otra ventaja del correo electrónico a comparación de los medios de comunicación convencionales como el teléfono consiste en que éste necesita contacto directo entre personas, el correo electrónico puede ser enviada la información y ser revisado en otro momento, a diferencia con el Fax que éste necesita que el documento tiene que ser impreso y en caso de corrección deberá ser escaneado o en su defecto mecanografiado y corregirlo, el correo electrónico por otro lado los datos e información transmitida puede ser modificada a través de un procesador de palabras (Word, TXT).

Como comunicación mediante foros de discusión, se lleva a cabo mediante páginas especializadas en el que se mantiene un contacto directo entre las personas á través de pregunta y respuesta.

Mensajería instantánea, esta comunicación puede ser considerada como de las más eficientes y rápidas en la Internet, depende de un servidor y programa especializado que permite entablar una conversación escrita (Chat) directa con otro usuario, a comparación con el teléfono, los mensajeros instantáneos comparten las mismas cualidades entre sí como la comunicación directa entre personas que poseen el mismo servicio pero a diferencia los mensajeros instantáneos en páginas Web permiten establecer conversación con personas desconocidas.

Como medio de información, la Internet se considera como una gran biblioteca por su amplio contenido de documentos considerado como el más grande y completo del mundo en el cual cualquier persona tiene acceso desde cualquier

terminal y desde cualquier parte del mundo. A diferencia de una biblioteca las autoridades de la misma controlan el manejo de la adquisición de nuevos libros o documentos, en la Internet los usuarios pueden introducir sus documentos de manera libre, lo que propicia el crecimiento del contenido de la información disponible, pero el principal problema radica en la veracidad de alguna de esta información derivada de la libre contribución de los usuarios.

La información en la Internet pasa de una computadora a otra sin saber la ruta que ésta deberá seguir con lo cual es imposible poner cuotas a su uso por la información consultada, por tal razón el costo del uso de la Internet se dividen entre todos los usuarios, de tal forma sólo son impuestas cuotas mínimas a los usuarios a través de los servidores de acceso a Internet.

- Organización de la Internet.

Consta básicamente de una organización no jerarquizada y que todas las computadoras y sistemas de redes con capacidad de acceso a la información así como de los servicios disponibles en Internet, toda esta información y servicio no se encuentran depositados en una computadora central o red determinada sino son transmitidas entre varias computadoras.

Tampoco es posible perder la información debido a que siempre es posible encontrar otra ruta para obtener la información perdida.

Una de las características importantes de la Internet es la autorregulación, consta de un programa denominado TCP/IP con los que funciona cada computadora que a su vez enlazada entre sí, la información es dividida en pequeños bloques los cuales son enviados por canales diferentes que al final son reunidos y armados en las computadoras receptoras, con lo que no existe una comunicación directa entre las computadoras a diferencia de la línea telefónica en la que existe un servidor

central en la que dependen las comunicaciones entre teléfono, pero donde la comunicación es directa entre las partes.

- Denominación.

Cada servicio de información cuenta con sus propias direcciones con el fin de acceder de manera fácil y rápida mediante la Internet, cada dirección recibe el nombre de dominios. (www, World Wide Web) en sus siglas en inglés, creado en 1989 por las investigaciones del Sir Timothy "Tim" John Berners-Lee ante el CERN (Centro Europeo para la investigación Nuclear), es un sistema que permite extraer elementos de información llamados "documentos" o "páginas web", los cuales necesitan de un programa especial para poder ser leídas, estos programas se conocen como exploradores o navegadores ejemplo: Amya (World Wide Web Consortium), Internet Explores (Microsoft), Netscape Navigator (Netscape Communications), Opera (Opera Software).

La funcionalidad elemental de la Web se basa en tres estándares básicos:

1. (URL), Localizador Uniforme de Recursos, que especifica cómo a cada página de información se asocia a una dirección única y en dónde encontrarla.
2. (HTTP), Protocolo de Transferencia de Hipertexto que especifica cómo el navegador y el servidor intercambian información en forma de peticiones y respuestas.
3. (HTML), Lenguaje de Marcación de Hipertexto un método para codificar la información de los documentos y sus enlaces Puede referirse a una (web) como una página, sitio o conjunto de sitios que proveen información por los medios descritos, o a la (web), que es la enorme e interconectada red disponible prácticamente en todos los sitios de la Internet, ejemplo:

Servicio:// nombre del sistema . dominio . nivel más elevado . código o país / ruta /archivo; Facultad de Derecho UNAM: <http://www.Derecho.unam.mx>. Una dirección de Internet puede tener más de una sola sección, un ejemplo es la

dirección de la enciclopedia Wikipedia: WIKIPEDIA Enciclopedia libre:<http://es.wikipedia.org/wiki/Portada>

El nivel de dominio más elevado es pieza importante en una dirección debido a que indica el tipo de organización a la que pertenece el dominio, ejemplo de las más comunes:

1. .com organización comerciales.
2. .edu universidades y otras instituciones de enseñanza.
3. .gov organizaciones estatales.
4. .net sistema de la red y administración de Internet.
5. .org otras organizaciones

- Dirección de Correo Electrónico (e-mail).

Incluye el nombre del usuario seleccionado por el mismo usuario o el prestador del servicio de correo, luego se agrega el símbolo @ (arroba) que en inglés significa “en”, a continuación el nombre del servidor, el dominio y el nivel más elevado si es que éste lo tuviera, ejemplo: Usuario @ servidor. Nivel más elevado. Código del país

1.2. CAMPOS DE ACCIÓN DE LA INFORMÁTICA.

La Informática ha sido utilizada en todas las ciencias, disciplinas y artes de la humanidad sirviéndoles para alcanzar sus objetivos, a continuación haré referencia de algunas de ellas.

1.2.1. La Informática en las Ciencias Naturales.

En los últimos años con el incremento de la computación y la Internet se ha generalizado su uso en diferentes áreas del conocimiento humano y es difícil encontrar una rama de la ciencia en donde no se haga el uso de la Informática en cualquier sentido y la invasión de las computadoras en todas las actividades del

ser humano que ha traído como consecuencia beneficios que en otras épocas se consideraban sólo dentro de la imaginación humana.

- La Informática en la Medicina, en la Biología y en la Genética.

La Medicina ha sido de las más beneficiadas por la informática, facilitando los procesos de investigación y el control en cada paciente, tratamiento de datos históricos y experiencias sintomáticas y con ello la creación de máquinas capaces de analizar y realizar diagnósticos certeros, además de realizar intervenciones quirúrgicas o asistencia a distancia mediante la robótica y la Internet.

La Biología: es “la Ciencia que trata de los seres vivos”¹⁷. Actualmente tiene un enfoque sistemático y los beneficios de las nuevas tecnologías han sido enormes y difíciles de mencionar todas a la vez, tanto que han abarcado beneficios en el almacenamiento y tratamiento de información, comunicación y experimentación mediante la simulación virtual.

La Genética: iniciada en los años 70's con las primeras investigaciones sobre la información genética de los organismos, ha generado un incremento en la información cuantitativa que ha sido posible manejar y decodificar tal información, dando como resultados el desciframiento y entendimiento de las secuencias genéticas enteras o parciales de organismos, con lo que en esa misma época se decidió crear los primeros bancos de datos públicos sobre información genética. El primero en surgir fue Laboratorio Europeo de Biología a Molecular (European Molecular Biology Laboratory) ¹⁸ en julio de 1974 con un tratado intergubernamental de nueve países europeos más Israel y que para el año 2006 sumaban ya 19 países miembros, con sede en Hiedelberg Alemania, cuenta con 4 sub-sedes conectadas entre sí vía Internet las cuales son: Hinxton en Reino Unido, Grenoble en Francia bajo con el Instituto de Bioinformática Europeo, Hamburgo en Alemania y Monterotondo Italia. Sus Investigaciones abarcan el análisis experimental de la organización Biología Molecular de los organismos, Biología

Computacional y la Biología de Sistemas, todo esto apoyado por el desarrollo que permite un avance a las tecnologías disponibles para la comunidad científica y la red incorporada entre ellas. Uno de los principales logros de esta institución fue en 1995 al ser el primero en analizar y descifrar el código genético de la mosca de la fruta por Christiane Nüsslein-Vollhard y Erich Wieschaus lo cual les concedieron el premio Nóbel de Medicina em ese mismo año.

Otro segundo centro en surgir con estos mismos propósitos fue el GenBank en los E.U.A. que en 1987 se transformó en el International Nucleotide Sequence Database Collaboration¹⁹, el propósito de todas estas bases de datos es mantenerla a disposición de las instituciones educativas y el público en general de la manera más rápida en la que sea posible, ésta colección de datos se considera que ya ha superado los 100 Gigabites (cien millones de Bites) y se siguen sumando por mes más de 3 millones de secuencias genéticas nuevas.

- La Informática en la Química y Física

Estas dos ciencias han evolucionado de manera significativa con la llegada de la Informática a sus campos de estudio haciendo que éstas puedan ser presentadas de manera rápida y certera, realizando cálculos y simulaciones nunca antes imaginada que antes eran tardadas o en muchas ocasiones imposibles de hacer para una sola persona, además de que con la llegada de los medios electrónicos han surgido nuevas ramas en estas ciencias como la Física o Química Cuántica donde interviene la información para simular lo sucedido en el reino de lo inimaginable.

1.2.2. La Informática en las Ciencias Sociales.

Con la llegada de la Informática y con la Internet han revolucionado los campos de estudios y uso de a la Informática como herramienta crucial para sus

actividades que han creado nuevos conocimientos para diversas ciencias Sociales, tales como las que a continuación se mencionan:

- La Informática en la Economía y Administración.

La Informática dentro de la Administración y la Economía ha tenido una gran aceptación causado que en todas sus ramas han generado beneficios en la realización de sus actividades, por ejemplo: el uso de sistemas computacionales en la realización de cálculos administrativos, contables y financieros; control de inversiones, nóminas: automatización y evaluación de proyectos; operaciones comerciales, financieras mediante redes y la automatización de las bolsas de valores del mundo.

- La Informática en el diseño, ingenierías y manufacturas.

En cuanto a la Informática con esas áreas ha traído automatización de procesos, facilidad en las actividades lo que trae como consecuencia que la aplicación de la Informática en los diferentes fases de la producción lo que permite la producción en masa y a la vez reducir costos.

- La Informática en la educación.

La Informática puede influir en la manera en que las cosas pueden ser enseñadas y aprendidas, por lo que el uso de la tecnología puede ser destinada con fines didácticos en las instituciones educativas, esto es conocido como Informática Educativa.

Tenemos que recordar que los objetivos de un sistema educativo es el desarrollo del alumno en su expresión oral y escrita, comprensión de lectura, capacitación para argumentar y entender; en un segundo plano el alumno deberá aprender a desarrollar un razonamiento lógico-matemático para la solución de problemas y

desarrollar su potencial artístico, todo esto con el fin de que emplee sus conocimientos para entender el mundo y con ello para transformarlo preparando a los alumnos para que al salir de las instituciones educativas sean personas preparadas como ciudadanos conscientes de la realidad y preparados para enfrentarla.

Con la entrada de los medios electrónicos para la educación se da un cambio en la forma de enseñanza debido a que presenta ventajas significativas en comparación a los medios de la enseñanza tradicional. El alumno presenta mayor atención ante la forma en que se presenta la información, menos aburrida o tediosa y más dinámica, trae como consecuencia el aprendizaje y la enseñanza de manera fácil y rápida, se proporciona información detallada debido que en los recursos educativos como la Multimedia, como su nombre dice se presenta la combinación de textos, medios audiovisuales, medios interactivos, animaciones, audio, video analógico o video digital; las cuales no podrían ser presentadas en muchos casos por medios tradicionales o en aulas convencionales; ahorro de tiempo y recursos para el proceso de aprendizaje y enseñanza, los alumnos pueden aprender por su cuenta y en casa después de las horas de clases para complementar sus estudios.

Los medios actuales de la Informática Educativa que facilita el aprendizaje se presentan de muchas formas entre las cuales encuentran como las básicas:

- Simulación Informática.
- Juegos interactivos con contenido educativo.
- Recursos multimedia.
- Bibliotecas virtuales y libros electrónicos (e-books).

Aunque estos medios han sido en muchos casos analizados y en muchos de ellas presentan un verdadero método de enseñanza práctica que han mostrado resultados positivos, no muchas personas lo consideran un medio de enseñanza real, sino como un atajo tramposo a la educación o un sustituto al trabajo docente, con lo que prefieren inclinarse a los anteriores métodos de enseñanza con lo que

privan a los alumnos de estas tecnologías, creciendo la brecha de lo que se conoce como “Analfabetismo Tecnológico”.

Uno de los serios problemas que se enfrentan muchas instituciones educativas es la presión que se ejerce con la apertura de los mercados lo que trae como consecuencia que los padres de familia presionen a las instituciones educativas a adquirir equipos de cómputo evitando atrasarse en la ola tecnológica y éstas al no perder alumnos y prestigio adquieren equipos de cómputo y audio visuales a toda costa y no se enfocan en la calidad educativa sólo en la cantidad, presentando a los alumnos deficiencias en su aprendizaje al seguir esta tendencia tecnológica. Con lo que las instituciones educativas se tienen que enfocar en tres puntos importantes:

Equipos de cómputo. En ocasiones por adquirir prestigio y alumnos las instituciones educativas adquieren sistemas de cómputo sólo para satisfacer las exigencias del mercado y no se enfocan en la calidad de los sistemas, en muchos casos se adquieren sistemas de cómputo ya sean muy básicos o muy complejos, que no siempre son útiles para las necesidades educativas y resultan complejos de manejar para los alumnos y profesores, por lo que las instituciones educativas se tienen que preocupar por adquirir equipo de cómputo especializado y compatible con la mayoría de los programas especializados en la educación o equipos adicionales para la enseñanza y aprendizaje.

Sistemas operativos. En muchas ocasiones no se toma en cuenta este factor debido a que se cree que los sistemas operativos incorporados en los sistemas de cómputo son óptimos y en muchos casos éstos no son compatibles con programas o equipos educativos enfocados para la enseñanza, además de presentar complicaciones para los alumnos y profesores para realizar estos fines; por ejemplo, en los equipos de cómputo convencionales se incluyen sistemas operativos básicos enfocados a las necesidades de las personas como navegadores y uso de Internet, procesadores de textos e imagen, así como reproductores

multimedia, que en muchas ocasiones no son compatibles con fines didácticos que se les quiere dar a la informática como herramienta y en muchas ocasiones están de más en los equipos informáticos. Lo que las instituciones educativas tienen que tener cuidado y adquirir sistemas operativos especializados en satisfacer sus necesidades tanto administrativas como educativas.

Los programas (Software). Muchas instituciones educativas optan por adquirir Enciclopedias Generales en Discos Compactos (CD) y se piensa que con eso es suficiente o bien adquiere programas considerados educativos, los cuales no son enfocados en la edad correspondiente a la de los alumnos o a la calidad y cantidad de enseñanza a tratar, y toda institución educativa tiene que ser cuidadosa en adquirir programas especializados en los temas para el grado y edad de los alumnos con el fin de optimizar el aprendizaje. Otro problema es que muchas instituciones educativas sólo se enfocan a la enseñanza del uso de la computadora y del sistema básico que éstas ofrecen con lo que para ellas mantiene su prestigio pero no se optimiza a la informática como la herramienta dedicada en la que se pretende convertir.

- La Informática y la Guerra.

En los conflictos bélicos, siempre se ha buscado conseguir la superioridad de cualquier tipo en contra del enemigo y con ello han surgido los mayores avances en la tecnología e Informática ya sea en el campo de las comunicaciones o en general en cualquier área de las ciencias humanas. La industria militar utiliza la informática, como medio de almacenamiento y procesamiento de datos, inteligencia artificial de combate, estrategia y toma rápida de decisiones así como control y seguridad.

1.3. LA INFORMÁTICA EN EL DERECHO.

Como hemos visto los recientes adelantos tecnológicos en las ciencias tanto sociales como naturales han generado un gran cambio en forma y su esencia,

haciéndolas más fáciles de realizar y como consecuencia logrando grandes avances en sus respectivos campos de estudio, por lo que el Derecho no debe permanecer ajeno a estos adelantos tecnológicos y responder a los nuevos y complejos problemas que se le plantean.

La ciencia del Derecho no puede dejar pasar esta oportunidad y la relación existente entre la Informática y el Derecho no puede ser analizado sólo desde un punto de vista ya que la Informática representa un gran campo de técnicas y conocimientos en la actualidad, y que también debemos tomar en cuenta que ésta no se quedará estancada y en un futuro seguir creciendo.

También hay que tomar en cuenta que los constantes problemas que surgen con las nuevas tecnologías a estudiar no siempre son tan novedosos, sino son problemas ya existentes, sólo realizados de nuevas formas con las nuevas tecnologías, con lo que se han creado otras ramas o denominaciones para poder dar solución y entendimiento a estos problemas y sin duda a los beneficios como las siguientes:

- Derecho Informático.

Se puede hablar de los primeros señalamientos de un Derecho Informático más claro en la obra de Norbert Wiener denominada Cibernética y Sociedad (The Human Use of Human Beings: Cybernetics and Society) que, en su Capítulo IV, hace referencia a la influencia de la cibernética con los fenómenos sociales incluyendo al Derecho y ésta relación se da a través de la comunicación.

Entendemos al Derecho en su forma más pura y simple como: “el conjunto de normas jurídicas que tienen por objeto regular la conducta humana”. Y a la Informática como un: “Conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores.”²⁰.

Por lo tanto se podría entender en este caso que el Derecho Informático, está enfocado únicamente a una protección de los datos informáticos o la información concentrada en medios magnéticos o digitales, Tenemos que recordar, que anteriormente la Informática fue enfocada originalmente a los cálculos matemáticos, pero después ésta se enfocó también en el campo de la lingüística, lo que trajo consigo nuevos cambios y ventajas, sin contar los nuevos problemas que surgieron con este adelanto.

- Derecho a la Informática y a la información. Bajo esta idea ha surgido como base a lo que denominaré: “Derecho a la información”, en este campo Carlos M. Correa autor Argentino en su obra Derecho Informático la denomina como: “La Teoría Jurídica de la Información”²¹ donde en 1987 y basado en las teorías francesas de esa época en especial de Pierre Catála, donde ya tienen marcado un objeto de estudio, el cual es la Información como una mercancía, donde Pierre Catála sostiene que ésta información “tiene un valor patrimonial y es susceptible de apropiación”²² y se hace la distinción de “Derecho sobre la Información” y “Derecho a la Información”, donde el primero señala a la información referente a datos personales las cuales únicamente conciernen a ellos mismos, y que son objeto de protección y el segundo que se contrapone con el primero donde se da acceso libre a información pública desde que ésta se haga pública.

Surge el problema de ubicar al Derecho Informático, en el Derecho Público o Privado; en especial en Francia es un Derecho Público regulado por leyes especiales desde la Ley de Comunicación del 9 de Enero de 1978, aunque en esa época y basada en la protección única de datos, este Derecho estaba más orientado a un Derecho Privado.

Herminio Tomás Azpilicueta autor Argentino, en su obra Derecho Informático, señala que el Derecho Informático puede estar ubicado dentro del Derecho Civil y Comercial sin problema alguno bajo los principios tradicionales de la responsabilidad civil, contractual y delincriminal, bajo el Derecho Administrativo

debido a la materia técnica del mercado público en la Informática, dentro del Derecho Internacional debido a las determinaciones de jurisdicciones aplicables a los contratos internacionales, así como en el Derecho de Comercio Exterior bajo estas mismas causas. Otras ramas en las que señala son el Derecho de Trabajo, Derecho Fiscal y el Derecho Procesal.

La relación del Derecho y la Informática así como los avances continuos en las tecnologías ha impactado cada una de las ramas del Derecho desde extraordinarios beneficios hasta nuevos retos, por lo que se puede decir que el Derecho Informático es interdisciplinario, por lo que no puede ser ubicada en una sola rama del Derecho exclusivamente.

Este término ha venido evolucionando junto con las nuevas tecnologías hasta llegar a la definición dada por Julio Téllez Valdez sobre Derecho Informático el cual dice:

“Es una rama de las ciencias jurídicas que consideran a la informática como instrumento y objeto de estudio”²³. Que donde ya existe una interacción del Derecho y la informática desde dos puntos, un primer punto como la “Informática Jurídica” y el segundo del “Derecho de la Informática”.

- La Informática Jurídica.

Surge en el momento en que la Informática es utilizada con fines lingüísticos, el primer esfuerzo realizado fue en 1959 en la Universidad de Pennsylvania en el Healthlaw center donde fueron colocados en medios magnéticos ordenamientos legales, logrando su éxito al ser el primer sistema legal automatizado en búsqueda de información, mostrado por primera vez en 1960 ante la Barra de la Asociación Americana de Abogados y rediseñado para fines comerciales por la Corporación de Sistemas Aspen, en 1966 se inició un sistema interno de recuperación de datos legales y para 1968 se habían computarizado los ordenamientos de cincuenta estados de los Estados Unidos de América.

La Informática Jurídica es la técnica que tiene por objeto la aplicación de la Informática para el procesamiento de información jurídica, Julio Téllez Valdez la define como: “la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicable a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación”²⁴.

- La Informática aplicada al Derecho.

Muchas ciencias han visto que las aplicaciones de los adelantos tecnológicos le traen grandes e incontables beneficios generando eficiencia y rapidez, así como ahorro de tiempo y recursos y no pasará mucho tiempo en que los juristas utilicen estas herramientas a favor del Derecho que son ramas de la Informática Jurídica.

Durante sus inicios la Informática Jurídica como ya se había mencionado enfocaba sus esfuerzos en el procesamiento de información jurídica, esto se le conoce como Informática Jurídica Documentaria con lo que se podía abarcar tanto leyes, jurisprudencia y doctrinas, hasta actos jurídicos, con lo que ha llevado a un mejoramiento del fenómeno jurídico, como una compilación.

Anteriormente la Informática Jurídica estaba separada de las aplicaciones de la Informática en Derecho como lo señaló Hermilio Tomás Azplicueta en su obra²⁵, pero con los adelantos tecnológicos ya no es posible mantenerlos separados. La Informática Jurídica de Gestión dentro de la Informática aplicada al Derecho, consistía en aplicar cada uno de los principios informáticos a toda actividad jurídica y ésta a su vez la clasificaba en tres grupos:

1. Informática Registral: Consiste en la rapidez y facilidad de accesibilidad a registros públicos en especial, dando como ventajas del recuperar dichos registros de manera instantánea y llevar a cabo labores estadísticas, así como evitar el monto de papel utilizado y facilitar los trámites.

2. **Informática Operacional:** Consiste en facilitar las actividades en las áreas públicas como lo son los juzgados y en el área privada como los bufets de abogados, permitiendo que las máquinas lleven todas las actividades, el control de asuntos y pleitos, contabilidad y registros.
3. **Informática Desicional:** Hermilio Tomás Azplicueta la considera la más difícil de comprender debido a que no se busca una “Juscibernética” y no pasar a una automatización de las decisiones, sino en que la misma Informática proporcione facilidades para evitar trabajo repetitivo al momento de redacción de escritos por medio de formatos pre impresos donde exclusivamente se cambian datos variables, permitiendo al juzgador ahorro de tiempo y continuar llevando sus labores decisorias,
4. **Informática Jurídica de ayuda a la Decisión:** en este caso los ordenadores facilitan la información adecuada para la toma de decisiones mediante el tratamiento y recuperación de información jurídica, siendo ésta la parte fundamental de la Informática Jurídica.

Otra forma en la que puede ser clasificada la Informática Jurídica es²⁶:

1. **Informática Jurídica Documentaria:** Tiene por objeto la creación de bancos de datos jurídicos referentes a todas las fuentes del Derecho excluyendo a la costumbre, para su procesamiento y con fines de consulta en el futuro.
2. **Informática Jurídica de Control-Gestión:** Enfocada en los campos jurídicos administrativos, judiciales registrales y en despachos de abogados. Dentro los que encontramos los siguientes:

En la Administración Pública: Debido al crecimiento demográfico y económico la Administración Pública ha sido orillada al uso de estas nuevas tecnologías para

mejorar la estructura jurídico administrativo y los sistemas de operación, con el fin de agilizar los trámites, disminuir la burocracia y la corrupción.

En los Órganos Jurisdiccionales: Con un enorme desarrollo en la automatización de los órganos judiciales conocido como “Informática Judicial”, por ejemplo: la formulación de agenda de jueces y magistrados, redacción automatizada de textos jurídicos a manera de sentencias, la aceptación registro e indicación del número y juzgado y verificar si hay o no conexidad de la causa, pueden seguirse las diferentes fases del proceso y el estado del juicio y en un momento en el futuro dejar de asistir a tribunales y ser consultables por vía telemática.

En los campos de Administración de Justicia se permite que ésta sea rápida, expedita, particularizada y gratuita.

En los Despachos y Notarías: Mediante el uso de sistemas computacionales se permite la automatización de oficinas, despachos y notarías en diversas labores como el control de asuntos, honorarios, redacción, verificación de escritos y funciones documentarias de consulta, con lo que permite a los abogados enfocarse a actividades jurídicas de contenido creativo, crítico e interpretativo.

3.- Sistemas Expertos Legales o meta-documentaria: Donde tras los fines documentarios de la Informática Jurídica, el sistema experto sirve con el fin de solucionar problemas con el uso de razonamientos implementados en una computadora, en lo que lo divide en 5 puntos para su fácil explicación:

a) Informática jurídica decisional: Consiste en que los mismos medios informáticos le proporcionen a los juristas ayuda en la toma de decisiones y no que un sistema tome las mismas por sí, aunque también hace referencia de la posibilidad de que en un futuro los mismos sistemas informáticos a través de sistemas expertos y la Inteligencia Artificial.

b) Educación: Los crecientes avances en la tecnología de la información y comunicación puede proporcionar mejoras en la educación tanto en aprendizaje y deconocimiento como en experiencias jurídicas facilitando las labores docentes y el aprendizaje.

c) Investigación o Informática Jurídica Analítica: Consta de los elementos matemáticos para aumentar las posibilidades de resultados, pero sin éxito por la complejidad y la ausencia de resultados exitosos. Este tipo de informática usa las computadoras para poner a prueba las hipótesis y teorías.

d) Previsión: Con gran funcionalidad en países con sistemas jurídicos romano germánico como el mexicano, donde a través de un estudio de diversos factores pueden ser tomadas diferentes decisiones aún con la más mínima variable, un ejemplo de este proceso son las jurisprudencias en materia penal de muchos Estados, donde para inferir del expediente y los antecedentes personales de los delincuentes analizando los antecedentes, medios profesionales, familiares, económicos, etc.

e) Redacción: Consiste en la ayuda y corrección en la redacción de textos en especial legislativos, durante la creación mediante un programa especializado enfocado en la lógica interna del texto facilitando la comprensión coherencia y armonización de los textos. También puede ser usado en la enseñanza jurídica por computadoras en el que se debe de reconstruir un texto jurídico mediante un sistema de interrogación con diferentes valores con el fin de asimilar la estructura de un texto.

Con lo anterior se puede resumir la Informática Jurídica se divide en tres ramas:

- La Informática Jurídica Documentaria.

Es la aplicación de métodos y técnicas de la Informática en los textos jurídicos abancos de datos, así como su procesamiento, que para poderlo lograr es necesario la recolección, organización, almacenamiento, recuperación, interpretación, identificación y el uso del documento jurídico. Para poder lograr la Informática Jurídica es necesario considerar tres aspectos:

a) La aplicación de un método de análisis, recuperación y tratamiento de la información, de los cuales existen tres sistemas comunes para el análisis de la información jurídica: 1. Indexación, en el cual crea una lista y calificando e individualizando la información designado por una o varias palabras o claves numéricas lo que permite su fácil ubicación y consulta; 2.- Full-Text: que consiste en el almacenamiento del texto en su totalidad en las máquinas; 3.- Abstract: consiste en almacenar los textos completos de forma lógica a través de restrictores de distancia en el cual puede ser organizarlo y consultarlo con mayor facilidad.

b) La formación de banco de datos mensuales, sistematizados, sectorizados o integrales.

c) La utilización de los lenguajes o mecanismos de recuperación de información.

- Informática Jurídica de Gestión:

Consistente en todas las facilidades que proporcionan los sistemas informáticos en la organización, administración y control de la información, documentos, expedientes y libros jurídicos mediante programas o sistemas de clasificación, utilizado en el área pública y privada, utilizada en el seguimiento de trámites y procesos, el uso rápido de registros contenidos en base de datos, facilitar actuaciones y actividades administrativas.

- Informática jurídica de apoyo en la decisión:

Consiste en la interacción hombre-máquina para la toma de decisiones jurídicas y el aprendizaje del Derecho, por medio de proporcionar banco de datos con

hechos experiencias e información jurídica. Además de facilitar el trabajo mediante el proporcionamiento de elementos considerados repetitivos y tediosos con lo que permite enfocar a los juristas realizar trabajo creativo en el campo el Derecho

- La Internet y el Derecho.

Con la llegada de la Internet diferentes ramas de la ciencias naturales y sociales han visto una oportunidad de mejoramiento en sus campos ya sea como consulta, investigación y comunicación, acortando tiempos y facilitando trabajos. La ciencia del Derecho debe aprovechar este medio para obtener grandes beneficios los cuales pueden enfocarse a los siguientes 3 campos: la comunicación, la Información y el aspecto laboral.

- En el campo de la comunicación, con otros seres humanos resulta importante basado en toda tecnología que permita mejorarla y simplificarla. La Internet proporciona en materia de comunicaciones al Derecho una amplia gama de posibilidades que es difícil no aprovechar.

- Correo Electrónico (e-mail)

Es un servicio de mensajería electrónica que permite un libre intercambio de información y datos entre las computadoras conectadas, en el caso de redes privadas este servicio puede ser usado exclusivamente a los equipos conectados a esta misma red con lo que no permitirá la entrada de cualquier otro correo electrónico de otro tipo de red. El servicio de correo electrónico consta de servidores que ofrecen este servicio utilizando la Internet como medio de envío con lo que permite que cualquier correo puede ser recibido por cualquier servidor por cualquier computadora siempre que sean compatibles; la gran ventaja que presenta el correo electrónico es la posibilidad que ofrece para poder enviar

Documentos Adjuntos al correo (Attached) y éste ser enviado de manera instantánea a cualquier parte del mundo de manera más segura hasta cierto punto, la disminución de costos, debido que es más económico enviar un correo electrónico que hacer una llamada telefónica, enviar un fax o el costo del correo común, en especial si ésta es realizada en diferentes partes del mundo.

Otra ventaja es el ahorro de tiempo y trabajo debido a que el correo electrónico es un envío instantáneo, que a diferencia de un correo tradicional es necesario que la carta sea redactada, impresa, firmarse, colocarse en sobre y ser depositada en el buzón o en su caso ser enviada por fax, con lo que lleva gasto de tiempo y trabajo; otra ventaja del correo electrónico, es que el correo es depositado en un buzón virtual ya sea del servidor o de programas especializados con lo que permite que no se necesita estar disponible para recibirlo y ser revisado en cualquier momento, o en su caso para viajes puede ser revisado en cualquier computadora con acceso a Internet o a dispositivos móviles inalámbricos.

Este medio presenta riesgos en la seguridad que aún hace que muchas personas no puedan confiar en este sistema al 100% debido a que el correo al ser enviado tiene que ser fragmentado y enviado por diferentes rutas que al final serán rearmados, pero esta unión se lleva a cabo por diferentes puntos que supone que puede ser visto o modificado en cualquiera de estos puntos, lo que reitera un serio problema en especial en el caso del secreto profesional. Otro riesgo que presenta el correo electrónico es que como en los medios tradicionales como lo son: el fax, las cartas, las llamadas telefónicas las cuales pueden ser conocidas por personas ajenas y sin autorización con la intervención de llamadas telefónicas, robo de correo y documentos; el correo electrónico también se encuentra sujeto a este tipo de riesgos las cuales se pueden reducir al máximo tomando medidas de seguridad adecuadas.

Estas medidas de seguridad pueden ser técnicas o no, con diferentes grados de dificultad ya que, en primer lugar se tiene que el correo electrónico para poder

ser enviado tiene que ser fragmentado y ser unido en diferentes puntos hasta llegar al destinatario con lo que se está en riesgo de que los correos sean vistos, lo que puede ser considerado como medida de seguridad al respecto es contratar a un proveedor del servicio seguro y conocido, tomando en cuenta que proporciona este tipo de seguridad contra filtraciones de información y ataques externos; otra medida de seguridad es la codificación de mensajes mediante programas especiales, el problema que conlleva este tipo de medidas de seguridad consiste en que los programas no son fáciles de conseguir, el costo, necesidad de conocimientos básicos sobre codificación y la compatibilidad de programas con el destinatario. En el caso de redes privadas no existen mayores riesgos debido a una comunicación directa entre equipos.

Otro de los problemas que trae consigo el correo electrónico es el acceso no autorizado, con lo que pueden ser prevenidos relativamente de manera fácil, ya que primero es mantener una contraseña a salvo, nunca ser revelada a personas extrañas, no dejar guardada en las cuentas de correos electrónicos en equipos propios o extraños, en caso de anotarla mantenerla en un lugar seguro y desconocido para las demás personas. Para el caso de contar con acceso a correos electrónicos en equipos personales y evitar filtraciones de información, las medidas de seguridad a seguir son básicamente en mantener apagados los dispositivos de comunicación inalámbricos cuando éstos no son utilizados y contar con programas denominados Anti-Virus siempre activos y actualizados.

Tomando en cuenta estas medidas de seguridad los juristas pueden tomar esta herramienta de comunicación como parte de su vida profesional, con lo que les permitirá un ahorro significativo de tiempo, dinero y trabajo, además, de mejorar su calidad de trabajo jurídico. Los principales servidores de correo electrónico en Ecuador y en el mundo de manera gratuita y segura a considerar son:

- Gmail.google.com
- www.hotmail.com
- www.terra.com.

•www.yhadoo.com

- Foros de Discusión o grupos LISTSERV.

Este tipo de medio de comunicación por Internet resulta de mayor facilidad y nace de la necesidad de intercambiar información y mensajes entre las personas pertenecientes a la comunidad; los grupos LISTSERV consisten en una lista de correos electrónicos trabajando con una computadora central el cual envía la información o preguntas a cada uno de los correos electrónicos en la lista de miembros; los foros de discusión dependen de una computadora central en el cual queda a disposición de todos los usuarios en el cual se puede dejar información, opiniones etc. las cuales pueden ser vistas por otras personas o los miembros los cuales pueden dejar contestación, o a su vez dejar información comentarios u opiniones, ambos sistemas pueden ser públicos pero la mayoría necesita de un registro para pertenecer al grupo de discusión.

- Mensajería Instantánea o Chat.

Como otro de los servicios que ofrece la Internet, éste permite una comunicación directa a través de programas especializados que se conectan entre los usuarios compatibles, que posean el mismo servicio o mediante ciberespacios especializados ofrecidos por compañías en la Internet en cualquier parte del mundo; este medio permite establecer conversaciones en tiempo real entre dos o más personas a la vez mediante comunicación escrita (Chat), hablada o mediante video conferencia, con lo que representa ahorro de dinero a comparación con el teléfono en especial en llamadas de larga distancia, además, de interactuar a la vez con un mayor número de personas que en una conversación telefónica normal y ahorro de tiempo debido a que no es necesario desplazarse a otros lugares con el fin de comunicarse con otra persona.

- En el Campo de la información:

La Internet en muchas ocasiones se le ha considerado como la biblioteca más grande y accesible del mundo, debido a que desde cualquier parte del mundo puede consultarse cualquier tipo de información en Bibliotecas Virtuales o libros electrónicos (e-Books), de manera gratuita o no; la manera en la que se puede acceder a esta información es mediante sistemas de búsqueda de información encontrado en la página de inicio (home page). Las ventajas de la intervención de la Internet como medio de información es básicamente la facilidad que proporciona para acceder a información en cualquier momento y desde cualquier lugar de manera gratuita si así se dispone; la desventaja consiste en que no todo lo publicado en Internet es cierto o actualizado en sitios gratuitos, siempre que se tenga que consultar información en la red es necesario realizarlo en lugares conocidos.

En el campo laboral la Internet ha beneficiado al Derecho ya sea en el sector público o privado a distancia, con lo que permite realizar trabajos desde diferentes partes del mundo para un mismo fin, en el sector público y privado se han visto recientes oportunidades de crecimiento en este campo debido a grandes beneficios que trae consigo, entre estos se encuentran: el acceso remoto a sistemas y bases de datos, incremento en la productividad, ahorro en el personal, costos y espacio de oficina; mejor calidad del trabajo, reducción de costos en la gestión de clientes, mejoras en las condiciones de trabajo, permanencia del servicio, velocidad de actuar y calidad de vida.

No sólo en la área privada se ha visto beneficiado el Derecho con el trabajo a distancia que trae consigo la Internet, ya que se ha visto la posibilidad de emplear políticas públicas creando un gobierno digital; Julio Tellez Valdes define un Gobierno Digital como el “proyecto de políticas públicas en el que se programan acciones relativas a la eficiencia en la administración pública y sus vínculos con los ciudadanos y empresas”²⁸ con lo que para la defensa de los ciudadanos y empresas se pretenden establecer diferentes medios para la solución de

controversias y su defensa derivado de su relación mediante el uso de la Internet lo que se le denominó “Ciberjusticia”.

Los primeros en aparecer en el campo de la “Ciberjusticia” fueron los “Cibertribunales” que funcionan igual que los arbitrajes y surgen de los conflictos surgidos del uso común en Internet ya sea entre público en general o conflictos entre empresa, con lo que les permite a las partes igual que en un arbitraje de elegir entre diversos expertos para proponer soluciones, los primeros “Cibertribunales” en surgir fueron en el año de 1996 en los Estados Unidos de América con la aparición de VirtualMagistrate²⁹ con colaboración del CyberspaceLawInstitute (CLI) y el Nacional Center ofAutomatedInformationResearch (NCAIR), que ahora se encuentra en la Universidad de Chicago-Kent y sus principales objetivos son: establecer el uso de resoluciones establecidas para conflictos que provienen en Internet, proveer de operadores de sistemas informados y neutros para los juicios, proporcionar un medio de solución de controversias, con autonomía para las partes, rápido, económico y accesible; proporcionar asesoría para definir deberes y obligaciones de las partes, estudiar la posibilidad de usar el mismo sistema u otros disponibles en la red.

Un segundo “Cybertribunal” es el The Online Ombuds Office³⁰ fue establecido en Junio de 1996 bajo la iniciativa del Center of InformationTecnology and Sioute Resolution de la Universidad de Massachussets, que consiste en un servicio de mediación para la resolución de decisiones para personas e instituciones surgidas de una actividad en línea, en especial entre los miembros de un grupo de debate, competidores proveedores de acceso a Internet y sus abonados, y los que se relacionen con la propiedad intelectual.

Otro de los denominados Cibertribunales fue el Cyber-Court un proyecto de cortavida creado en septiembre de 1996 y terminado en diciembre de 1999 creado por CenterRecherche en Detroit Publique de la Universidad de Montreal, el cual su función era el de Moderador en las mediaciones y prestar asistencia técnica o

administrativa. Al término de este fue creado el “Resolution”³¹ que continuó con este mismo trabajo.

Por ahora todos los intentos de un Cybertribunal están esencialmente enfocados aun arbitraje entre las partes por conflictos derivados del uso de servicios en Internet, creados por particulares; pero cabe la posibilidad que en un futuro existan Cybertribunales creados por el Estado, no únicamente enfocados a litigios creados por la Internet, sino también enfocados a todo tipo de litigio que normalmente un tribunal conocería, aunque en la actualidad y en nuestra realidad es posible revisar las actuaciones, acuerdos, sentencias y estado procesal mediante Internet, en un futuro no sólo se pueda revisar el estado procesal de los asuntos sino realizar actuaciones de manera telemática sin la necesidad de presentarse físicamente a los tribunales.

A pesar de que la existencia de un Cybertribunal en México parezca una idea alejada de la realidad debido a que se tendría que adaptarse nuestro sistema legal, la solución de problemas de índole técnico-jurídico, el fortalecimiento de la confianza de las personas en los medios electrónicos como la Internet y en la justicia mexicana y el afinamiento de ligeros detalles en los asuntos que siendo similares no son únicos entre sí; los Cybertribunales tendrían como ventajas entre otras: el ahorro de tiempo y recursos tanto para el litigante como para el tribunal, en cuanto a evitar el traslado desde un despacho aun juzgado en una ciudad caótica como la nuestra, en especial cuando el asunto no se ha movido o en el caso de realizar actuaciones urgentes e inesperadas, disminuir el tiempo de reacción para emitir una respuesta rápida ante contratiempos desde cualquier parte del mundo, evitar la corrupción, ahorro de recursos que trae la disminución en los costos tanto para los litigantes como para el Estado; pero a su vez esto presenta desventajas para las partes, debido a que la seguridad y honestidad del sistema de un Cybertribunal depende de los conocimientos y honestidad de quien está encargada de la vigilancia y creación de un Cybertribunal o quien hace uso de él, la interacción entre las partes se vería disminuida o eliminada casi en su

totalidad. Aunque con la idea de los Cybertribunales no puede ser tomada a la ligera y ser tema de estudio en trabajos posteriores.

- La Cibernética Jurídica.

Los avances en la ciencia nos han llevado a un mundo de maravillas tecnológicas que antes nunca pudieron ser imaginadas, con lo que ha llevado a mejorar la calidad de vida de los hombres en todos sus aspectos y aunque parece difícil de creer y de ciencia ficción, la posibilidad de que en una mañana las computadoras puedan tomar decisiones por sí mismas sin simular los pensamientos humanos ni ser manipulada o la necesidad de intervención humana para lograr complejas decisiones, conocido como “Inteligencia Artificial”.

Se entiende como “Inteligencia Artificial” el: “Desarrollo y utilización de ordenadores con los que se intenta reproducir los procesos de la inteligencia humana”³².

Aunque en los campos de la Inteligencia Artificial apenas está dando sus primeros pasos la idea de que una computadora pueda tomar decisiones jurídicas por sí mismo sin la necesidad de intervención humana, e incluso el grado de suplantar jueces y magistrados pueda causar controversia y considerar un tanto impráctico e innecesario.

Para la toma de decisiones jurídicas dependen de muchos elementos y vertientes para buscar una verdad jurídica sólida aún la más mínima decisión requiere de un número de elementos que no pueden ser analizados fácilmente, explicados y ser plasmados de manera práctica, aunque se puede hablar de “Sistemas Inteligentes Legales” los cuales no es necesario que la misma computadora tome las decisiones por sí, sino que ésta pueda proporcionar auxilio en las tomas de decisiones jurídicas como una herramienta y éstas para un funcionamiento óptimo deben contener como requerimientos básicos: una base de conocimientos como banco de datos, un sistema cognoscitivo o mecanismos de

inferencias para la estructura de esquemas de razonamiento, elementos que permitan el establecimiento de comunicación entre el sistema y el usuario, que al igual que en otras ciencias estos sistemas expertos funcionan a través de complejas ecuaciones y modelos lógico-matemáticos, para resolver problemas y simulaciones complejas lo que ha llevado a diversos estudiosos en diversas áreas de las ciencias a realizar complejas emulaciones a procesos que llevarían semanas en resolver por la mente humana, aunque el proceso mental que lleve al planteamiento, razonamiento y solución de problemas es difícil de explicar y describir, además de que necesita determinados factores como el conocimiento, la experiencia y determinadas circunstancias, así como otros factores que pueden ser considerados como subjetivos, para la existencia de un sistema capaz de tomar decisiones sin la necesidad de la intervención o manipulación humana, en especial para el ámbito del Derecho se necesita la existencia de una computadora capaz de resolver y plantear decisiones jurídicas se necesitaría que ésta pudiera obtener conocimientos por sí misma, aprender de errores del pasado en forma de experiencia, así como, de analizar factores que pueden ser considerados como subjetivos para poder llegar a una verdad jurídica, pero no ser descartada ya que los avances en la tecnología siempre trae sorpresas en el futuro.

- Derecho de la informática.

Como ya hemos visto las nuevas tecnologías han traído mejoras en todos los campos del Derecho e incluso nuevas formas en las que esta ciencia puede ser vista a partir de ahora, así como ha pasado en otras ciencias del conocimiento humano, pero los nuevos adelantos no podían quedarse al uso exclusivo de los científicos, investigadores y estudiosos de las ciencias, sino también han pasado a ser uso del público en general y en mayor medida del uso comercial, aprovechando sus enormes beneficios tanto como herramienta para adquirir conocimientos, analizar comunicaciones y simplificar la vida humana.

A partir de los años 60's con el uso de los medios informáticos surgieron mayores relaciones sociales y comerciales entre los pueblos y a partir de ellos

surgieron problemas derivados de la expansión de relaciones, con lo que se da nacimiento al Derecho de la Informática, pero en esos momentos no era tan estudiada ya que se le daba más importancia a la Informática Jurídica o en muchas ocasiones junto a ella era estudiado, debido a que todos estaban enfocados y maravillados en los beneficios que traían las Computadoras al mundo del Derecho.

Con lo que atendiendo a esta problemática ha surgido el Derecho de la Informática para poder dar solución a estos conflictos, entendiendo como tal al: “Conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática”³³, con lo cual los problemas a enfrentarse en el mundo de la informática e Internet son entre otros:

- La regulación jurídica de los derechos y obligaciones derivados de las relaciones existentes al adquirir, distribuir, explotar y utilización del Software y Hardware, protección jurídica de Software considerado como un bien inmaterial.
- Derechos y obligaciones para los creadores, distribuidores y usuarios de base de datos.
- Regulación jurídica derivada de la contratación de bienes y servicios informáticos ya sea dentro de un Estado y fuera de ellos ya sea de manera directa o indirecta.
- Protección de datos personales, surgida de la potencial agresión informática con respecto al procesamiento de estos mismos datos.
- Responsabilidad, derechos y obligaciones surgidos de la transferencia electrónica de fondos o datos, dentro de un país o incluso entre usuarios localizados en diferentes países con diferentes regulaciones jurídicas.
- Validez probatoria de los documentos generados por medios informáticos o incluso de los documentos encontrados en soportes informáticos.
- Regulación jurídica derivada de la relación laboral a través de los medios informáticos a distancia.

- Transacciones comerciales llevadas a través de medios informáticos realizados dentro de un país o fuera de él.
- Los denominados Delitos Informáticos.

Debido a estos problemas que se suscitan en estos campos el primer paso para dar una solución y en especial una regulación y protección es la planificación mediante normas que conforman una política la cual se tiene que acoplar a un fomento del desarrollo industrial en el campo de la informática, contratación gubernamental de servicios y equipos informáticos confiables y seguros, plantación, control, aplicación, difusión y del fenómeno informático.

- La protección de base de datos.

Actualmente la información ha dejado sus connotaciones pasadas, convirtiéndose en un bien fundamental en un mundo cada vez más apegado a la tecnología la cual se ha convertido como una herramienta de fácil acceso con ella, pero a la vez que éste sea considerado con un bien con valor económico, debido a que en las diferentes fases en el procesamiento de la información implica un costo que es reflejado en precio ante los usuarios, pero en muchos casos la información no tiene una cuantía imaginable debido que contar con ella permite tomar decisiones de manera más rápida, certera e informada, generar riquezas superiores al valor mismo de la información, e incluso manipular a las personas y sociedades enteras, bien incluso se menciona que quien tenga el conocimiento tiene el poder.

Las bases de datos han proliferado con la llegada de las nuevas tecnologías en diferentes áreas de la sociedad que en muchos casos son usados con fines tanto administrativos, de control, académicos e incluso económicos.

Para la creación de base de datos eficientes interfiere diversos procesos que involucra a una gran cantidad de personas especializadas, con lo que éstos se convierten en un producto con costo determinado que muchas veces se ve

reflejado en la calidad de la base de datos y según para el fin que esté creada la base de datos esta presentara variados problemas a tratar.

Las base de datos en general tiene 3 problemas fundamentales básicos por resolver, el primero el derecho de autor del material almacenado en los bancos de datos, la autorización sobre el uso de sus obras y otorgar la facultad de administrar la base de datos; el segundo es el derecho originado a los productores de la base de datos por la sistematización y elaboración; el tercero son los derechos y obligaciones derivados entre la relación del creador, distribuidor y usuario, este último al ser consultado y ser adquirido.

El caso de las base de datos con fines académicos han revolucionado a las ciencias debido a la facilidad que conlleva manejar grandes volúmenes de información en corto tiempo, con lo que ha llevado a las computadoras sean consideradas como una herramienta académica por el manejo de la base de datos en soportes electrónicos que únicamente pueden ser leídos por los mismos, pero en otros casos las bases de datos sólo pueden ser consultadas de manera “on-line” mediante la Internet o el uso de redes privadas.

Con fines económicos y administrativos las bases de datos han creado una relación de dependencia con las empresas, lo que los hace completamente vulnerables a posibles atentados, que generan daños y pérdidas económicas y que en muchas ocasiones termina en el cierre de la empresa por lo que las bases de datos de este tipo necesitan de 3 tipos de seguridad: la física que concierne a la estructura física que sustenta la base de datos, como lo son soportes magnéticos (diskettes), ópticos (CD ROM) y las mismas computadoras; la lógica que es toda la base de programación necesaria para el correcto funcionamiento de la base de datos; y en especial protección jurídica en cuanto los ataques físico como lógicos de la base de datos.

- Protección de datos personales.

La información no es exclusiva de los medios tecnológicos, aunque con ésta tuvo su auge en los años 70's con el gran almacenamiento de documentos en medios electrónicos, con lo que permitió el rápido manejo y el control de grandes volúmenes de información en menor espacio y debido con el creciente uso comercial de los medios informáticos, permitió que la mayor parte del público, empresas, instituciones públicas crearan su propia información, e incluso de información de tipo personal, los cuales contenían datos personales desde los más básicos como nombre, edad, fecha de nacimiento, domicilio, estado civil, hasta los archivos con datos más complejos como el tipo sanguíneo, nivel y logros académicos, enfermedades o padecimientos pasados o actuales, religión, cuantas bancarias, los cuales pueden ser almacenados en diferentes centros de acopio o banco de datos públicos o privados, incluso en los mismos hogares, que sin la ayuda de la informática el tratamiento de todos estos datos para diferentes personas sería una labor compleja, pero se tiene que recordar que la seguridad de cualquier medio de cómputo así como la buena voluntad humana no son perfectas al 100% y la información personal comprometida depositada en los bancos de datos es susceptible de caer en manos de terceros y ser susceptible de ser revelada lo que puede generar un sin fin de problemas.

1.4. DELITO INFORMATICO

1.4.1. Generalidades

El Ecuador, en abril de 2002, expide la Ley de Comercio, Firmas Electrónicas y Mensajes de Datos, instrumento que da un marco jurídico a las innovaciones tecnológicas relacionadas con la transmisión de información utilizando medios electrónicos. El objeto de la Ley es la de regular los mensajes de datos, firmas electrónicas, servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el

comercio electrónico (e-business) y lógicamente la protección a los usuarios de estos sistemas de cualquier mecanismo de distorsión.

Gracias a la expedición de esta Ley, nacen como delitos con características propias el sabotaje (SPAM) y los daños informáticos (CYBER CRIME). Sobre este punto trataremos más adelante, hasta mientras diremos que estas infracciones se incorporan al Código Penal ecuatoriano, logrando así una protección concreta y específica a este tipo de actos, considerados desde abril de 2002 como delitos. Ahora bien, dentro de la regulación propia de los mensajes de datos, también se prevé mecanismos de protección propios en donde se enuncian principios y procedimientos que se deben respetar.

La Ley establece que los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Estos consisten en documentos que han sido enviados por un sistema electrónico, a los cuales se les da plena validez.

El artículo 5 de la Ley establece principios sobre confidencialidad y reserva: "se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia". Se establecen principios que armonizan con disposiciones constitucionales. La inviolabilidad y el secreto de la correspondencia es una garantía establecida en la Constitución, recogida en el numeral 13 del artículo 23, así como el numeral 14 del artículo 24.

Todos los mensajes están amparados por estas disposiciones, independientemente de la forma de envío y sin consideración de su medio o intención. La reserva protege el tratamiento de datos de carácter personal y la libre circulación de estos, en lo que se refiere a las comunicaciones comerciales y a la responsabilidad de los intermediarios. El Estado ecuatoriano garantiza la confidencialidad mediante cualquier forma de interceptar o vigilar esas comunicaciones por parte de cualquier persona que no sea su remitente o destinatario salvo que esté legalmente autorizada. En el caso de que se violen estos principios, existen mecanismos constitucionales de control legal.

Con relación a la protección de datos, para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información que quiera compartir con terceros.

Según el segundo y tercer párrafo del artículo 9 de la Ley, "la recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución de la República y esta Ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente. No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato".

La norma protege a la elaboración, transferencia o utilización de bases de datos, siempre enmarcada dentro de principios de confidencialidad y privacidad. En cualquiera de estos casos, es un requisito sine qua non el consentimiento del titular, pero no será necesario este consentimiento expreso cuando se trate de

situaciones que generen correspondencia entre las partes para crear una base de datos.

Resumiendo, vemos que existen principios constitucionales y legales de protección a la información que consta en una base de datos. Los mensajes que se generen, deben estar acompañados siempre de criterios y parámetros de respeto al bien ajeno y a la propiedad privada. Por esto se requiere el consentimiento para que sea posible disponer del mensaje recibido o sujeto de envío. También es importante resaltar que se prohíben las bases de datos y la recopilación de direcciones electrónicas, salvo que exista un consentimiento por parte del dueño o sea producto de funciones propias que se desempeñen entre partes y que se vayan generando con el transcurso del tiempo. La Ley considera que si se recopila y usan datos personales sin el consentimiento previo, existe una violación flagrante a los derechos de la privacidad, confidencialidad e intimidad que se encuentran garantizados por la Constitución.

El campo de aplicación de la Ley de Comercio y Firmas Electrónicas está dado básicamente por relaciones contractuales amparadas en el campo civil, aunque también, de menor manera, tiene injerencia dentro del ámbito penal. Este ámbito está dado concretamente dentro de lo que ésta misma considera como infracciones informáticas. La Ley agregó al Código Penal una serie de infracciones antes no contempladas para sancionar este tipo de delitos.

Hay dos artículos que revisten importancia dentro de los delitos electrónicos de SPAM y CYBER CRIME. Se agrega a continuación del artículo 553 del Código Penal el siguiente artículo:

"Falsificación electrónica: son reos de falsificación electrónica la persona o personas que con el ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, ALTEREN O MODIFIQUEN MENSAJES DE DATOS, O LA INFORMACIÓN INCLUIDA EN ÉSTOS, que se encuentre

contenida en cualquier soporte material, sistema de información o telemático, ya sea:

Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial; Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad

Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones de las que hubieren hecho".

Para tener una idea sobre la ubicación de la norma dentro del Código Penal, el legislador ha considerado que estos delitos se deben encasillar dentro de los delitos contra la propiedad y concretamente dentro del delito de robo.

Esta disposición protege al consumidor de cualquier tipo de información que sea falsa. Cuando se refiere a información comercial que induzca a error o engaño, la Ley de Defensa del Consumidor establece protecciones y sanciones para evitar que este tipo de prácticas se generalicen, lógicamente, protegiendo al consumidor para que no se le oferte un producto de una calidad y reciba otra de distinta a la ofertada. La Ley de Defensa del Consumidor no establece de manera expresa una protección al consumidor, pero sí de manera general, principios de aplicación que se pueden aplicar para este caso en concreto.

1.4.2. Criminalidad informática

De todos modos, quiero repasar puntualmente ciertas preguntas que son usualmente formuladas, con el fin de que estos temas sean resueltos de la manera más clara posible:

"Si podemos usar otras normas para atacar el envío de spam, como por ejemplo, leyes de protección de consumidores o sobre privacidad"

Si bien la Ley de Defensa del Consumidor establece normas generales sobre inducir a error o engaño relacionado con propagando o difusión de información, la ley compete en estos casos, por ser una ley específica sobre la materia, va a ser la Ley de Comercio Electrónico. Como vimos anteriormente, el SPAM está regulado por la Ley de la materia.

"Hay leyes sobre spam o emails que traten con temas particulares como pornografía, distribución de un virus u otro código malicioso, u oferta de bienes ilegales"

Dentro de la Ley de Comercio Electrónico, sobre distribución de virus u otro código malicioso, se regulan dentro de las disposiciones ya analizadas. En el caso de pornografía u oferta de bienes ilegales, no existe ninguna prohibición ni norma al respecto relacionada directamente con la difusión a través de medios electrónicos de manera específica, pero en el Código Penal de manera más amplia, dentro de los delitos sexuales, considera como un atentado contra el pudor a este tipo de manifestaciones, sin importar el medio que se utilice. La ley se expidió recientemente, por lo que no hay ningún fallo jurisprudencial o doctrina que avalen este criterio. Sin embargo, hay normas constitucionales que protegen la honra, la moral, las buenas costumbres, la libertad, la falta al decoro y la dignidad personal, que se ven alterados con el envío de este tipo de información.

"Hay leyes en contra del hacking"

Salvo las normas que se establecen en la Ley de Comercio Electrónico, no hay normas adicionales al respecto.

"Hay proyectos de ley en el Congreso sobre estos temas"

La Ley fue aprobada el 11 de abril de 2002 por el Congreso Nacional y se publicó en el Registro Oficial Suplemento No. 557 de 17 de abril del mismo año. Por el momento, no hay ningún proyecto de ley sobre la materia.

1.5. DEFINICIÓN Y EL CONCEPTO DE DELITOS INFORMÁTICOS

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 entorno a la necesidad de distinguir o no los delitos informáticos del resto. Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios. De hecho, el Código Penal español, no contempla los delitos informáticos como tal.

Partiendo de esta compleja situación y tomando como referencia el “Convenio de Ciberdelincuencia del Consejo de Europa”, podemos definir los delitos informáticos como: “los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos”.

Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas. Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos o hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etcétera. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado a su vez la necesidad de regulación por parte del derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.

Por lo que se refiere a las definiciones que se han intentado dar en México, cabe destacar que Julio Téllez Valdés señala que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los códigos penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún".

Para Carlos Sarzana, en su obra *Criminalista e tecnología*, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo". Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Rafael Fernández Calvo define al delito informático como "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático o telemático contra los derechos y libertades de los ciudadanos definidos en el título 1 de la constitución española".

María de la Luz Lima 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 ya sea como método, medio o fin".

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como "delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora", "delincuencia relacionada con el ordenador".

En este orden de ideas, en el presente trabajo se entenderán como "delitos informáticos" todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Lógicamente este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes en México debido a que la legislación se refiere a derecho de autor y propiedad intelectual sin

embargo, deberá tenerse presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

1.5.1. Sujetos del delito informático

Muchas de las personas que cometen los delitos informáticos poseen ciertas características específicas tales como la habilidad para el manejo de los sistemas informáticos o la realización de tareas laborales que le facilitan el acceso a información de carácter sensible. En algunos casos la motivación del delito informático no es económica sino que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Muchos de los "delitos informáticos" encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland en 1943. Esta categoría requiere que: (1) el sujeto activo del delito sea una persona de cierto estatus socioeconómico; (2) su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional.

1.5.2. Sujeto activo

Al respecto los Doctores Julio Valdés y María Luz Lima entre otros sostienen que las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son

hábiles en el uso de los sistemas informatizados, aún cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los delitos cometidos. De esta forma, la persona que "entra" en un sistema Informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

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

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

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como "delitos de cuello blanco", aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros".

Asimismo, este criminólogo estadounidense dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no son de acuerdo

al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Es difícil elaborar estadísticas sobre ambos tipos de delitos. La "cifra negra" es muy alta; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes lo cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; ésta no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos "respetables". Otra coincidencia que tienen estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativo de la libertad. Por nuestra parte, consideramos que a pesar de que los "delitos informáticos" no poseen todas las características de los "delitos de cuello blanco", si coinciden en un número importante de ellas, aunque es necesario señalar que estas aseveraciones pueden y deben ser objeto de un estudio más profundo.

1.5.3. Sujeto pasivo

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

En primer término tenemos que distinguir que el 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", mediante él podemos conocer

los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.

Ha sido imposible conocer la verdadera magnitud de los "delitos informáticos" ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables; que sumado al temor de las empresas de denunciar este tipo de ilícitos por el desprestigio y su consecuente pérdida económica que esto pudiera ocasionar, hace que éste tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra"

1.6. MARCO JURÍDICO SOBRE LA INFORMÁTICA JURÍDICA Y LOS DELITOS INFORMÁTICOS.

Antes de conocer las regulaciones que se han establecido en el Ecuador y que están relacionadas con las tecnologías de la información, se mostrará cual es la estructura general de dichas regulaciones, para ello, se toma como referencia la Pirámide Kelseniana (16). El cual es un recurso que permite ilustrar, la jerarquía de las normas jurídicas:



Figura 1. Marco jurídico sobre la informática jurídica

Desde los años ochenta, las Naciones Unidas han venido promoviendo por medio de la Uncitral (CNUDMI – Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) una adecuación de las diferentes legislaciones mundiales

a sus leyes modelos, entre los documentos aprobados por dicha comisión están, por ejemplo: la Ley Modelo sobre Comercio Electrónico (17) y la Ley Modelo sobre Firmas Electrónicas (18).

En Sudamérica, el primer país que se preocupó por estos temas fue Colombia, ya que en 1999 publica su ley 527, la misma que regula el comercio electrónico, firmas digitales y las entidades de certificación, luego en el mes de mayo del año 2000 Perú publica la ley 27269, sobre Ley de Firmas y Certificados Digitales. Luego, le siguen en el 2001 Argentina y Venezuela en el año 2001, luego Chile y Ecuador en el año 2002.

GerberthAdín Ramírez Rivera (19), expresa “para que todo lo realizado en la informática forense sea exitoso, es necesario que se tengan regulaciones jurídicas que penalicen a los atacantes y que pueda sentenciárseles por los crímenes cometidos. Cada país necesita reconocer el valor de la información de sus habitantes y poder protegerlos mediante leyes. De manera que los crímenes informáticos no queden impunes”.

En la legislación del Ecuador bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de las tecnologías, tales como:

- 1) Ley Orgánica de Transparencia y Acceso a la Información Pública.
- 2) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- 3) Ley de Propiedad Intelectual.
- 4) Ley Especial de Telecomunicaciones.
- 5) Ley de Control Constitucional (Reglamento Habeas Data).

1.6.1. Ley orgánica de transparencia y acceso a la información pública.

La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTaip), publicada en el Registro Oficial Suplemento # 337 del 18 de mayo del 2004, fue expedida con la finalidad de llevar a la práctica la disposición contenida en el Art. # 81 de la Constitución Política de 1998, en la que se señala que “la información es un derecho de las personas que garantiza el Estado”.

La ley establece que todas las instituciones del sector público pongan a disposición de la ciudadanía, el libre acceso a la información institucional (estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc.), a través de sus sitios web, bajo este mismo contexto las disposiciones contenidas en la Constitución del Ecuador vigente, en su capítulo tercero de las Garantías Jurisdiccionales de sus secciones cuarta y quinta de los Art. 91 y 92 sobre la acción de acceso a la información pública y acción de Habeas Data, también se establece dichas garantías. De acuerdo a un estudio realizado por el Grupo Faro (20), en marzo del 2007. Los Ministerios Ecuatorianos cumplen, en un promedio del 49% de lo dispuesto en la Ley Orgánica de Transparencia y Acceso a la Información.

Otro organismo que vigila, analiza, realiza controles permanentes y se encarga del cumplimiento de la Ley Orgánica de Transparencia y Acceso a la Información Pública, es la Defensoría del Pueblo, quienes a través de un informe, publicado en el Diario El Telégrafo (21), del 27 de octubre del 2008, revelaron los siguientes datos con respecto del monitoreo de la ley:

1. De 380 instituciones públicas, 291 cumplen publicando su información de acuerdo a lo dispuesto en la Ley.
2. A 89 instituciones se les notificó para que cumplan con la Ley.
3. 72 instituciones solicitaron una prórroga para completar y cumplir con las disposiciones de la Ley.
4. 70 instituciones cumplieron luego de haber recibido la notificación.
5. 17 instituciones no remitieron ninguna respuesta acerca de la notificación.

6. 12 instituciones respondieron la notificación indicando que las páginas se encuentran en fase de construcción.

7. Por último 7 instituciones no cumplen con las disposiciones de la Ley.

El mismo informe revela que en el caso de la Provincia del Guayas la Defensoría del Pueblo suscribió un convenio con Participación Ciudadana que promueve el cumplimiento de la Ley, el cual inicio el mes de junio del 2008.

1.6.2. Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos (LCElec.) fue publicada en el Registro Oficial N° 557 del 17 de Abril del 2002 en el que se dispone que los mensajes de datos tendrán, igual valor jurídico que los documentos escritos.

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos está conformada por cinco títulos conteniendo cada uno varios capítulos y artículos

1) Título Preliminar.

2) De las Firmas electrónicas, certificados de firmas electrónicas, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.

3) De los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios, e instrumentos públicos.

4) De la prueba y notificaciones electrónicas.

5) De las infracciones informáticas.

La Ley contiene los principios jurídicos que regirán las transmisiones de los mensajes de datos. Se le concede pleno valor y eficacia jurídica a los mensajes de datos, tanto a su información como a su contenido general; la interpretación de la Ley y el ejercicio de la Propiedad Intelectual se rigen por la legislación ecuatoriana y por los tratados internacionales incorporados al cuerpo legal ecuatoriano. Se protege la confidencialidad de los mensajes de datos en sus diversas formas, señalando lo que se entenderá por tal concepto y su violación. Se equipara el documento escrito con el documento electrónico para el caso en que se requiera la presentación de un documento escrito, procediendo de igual manera con el documento original y la información contenida en él, siempre y cuando exista garantía de su conservación inalterable.

Como punto esencial, se establece que la firma electrónica tendrá validez cuando conste como un requisito de legalidad documental. Además se protege las bases de datos creadas u obtenidas por transmisión electrónica de un mensaje de datos, concediendo al titular de dichos datos el poder para autorizar la disposición de su información, sea que dichos datos fueron obtenidos como usuario de un servicio o sea que fueron obtenidos en el intercambio de mensajes de datos. Se ratifica la defensa legal mediante el Derecho Constitucional de Habeas Data.

Se busca que especialmente en los negocios relacionados con el comercio electrónico las notificaciones sean por medio de correo electrónico, estableciéndose obligatoriedad de notificar por éste medio y por el tradicional para el caso de resoluciones sometidas a Tribunales de Arbitraje. El documento electrónico será considerado como medio de prueba con todos sus efectos legales. Para que existan presunciones legales sobre la veracidad de un documento, éste deberá cumplir los principios de integridad e identidad, para justificar la voluntad contractual de obligarse por dicho documento. Aquella parte que niegue la validez de un documento electrónico deberá probar que este no cumple con los requisitos

técnicos mencionados anteriormente. Se establecen varios requisitos para la correcta aplicación de la prueba en estos casos, entre ellos señalamos:

- 1) La presentación de los soportes necesarios en papel del documento electrónico y los mecanismos para la lectura y verificación de la firma.
- 2) La presentación del certificado validado por un proveedor de servicios de certificación.
- 3) Los demás mensajes de datos deberán guardar especial atención con la integridad de su contenido. Las pruebas serán juzgadas y valoradas de acuerdo con “la seguridad y fiabilidad con la cual se la verificó, envió, archivó y recibió”. Para una mejor apreciación de la prueba el juzgador contará con el asesoramiento de un perito en la materia, es decir un perito informático.

El organismo facultado para autorizar a las entidades de certificación de información es el Consejo Nacional de Telecomunicaciones, según lo dispuesto en la Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos y el Reglamento expedido por el Presidente de la República, mediante Decretos Ejecutivos 3496 (31 de julio del 2002) y 1356 (29 de Septiembre del 2008) en los que se establecen el modelo de Resolución para la Acreditación como Entidad de Certificación y Información y Servicios Relacionados, tal como lo establece el Art. 29 del Capítulo II de la ley.

Las funciones y responsabilidades otorgadas por el Consejo Nacional de Telecomunicaciones, a las entidades de certificación de información y servicios relacionados, es que dichas entidades se encargan de la generación, gestión, administración, custodia y protección de las claves y los certificados de firma electrónica, así como la validación de la identidad e información de los usuarios o solicitantes de firmas electrónicas, mediante el uso de infraestructura y recurso

humano capacitado para operar dicha infraestructura con absoluta pericia y confidencialidad.

Uno de los organismos que obtuvo la autorización del Consejo Nacional de Telecomunicaciones como Entidad de Certificación es el Banco Central del Ecuador para emitir certificados a personas naturales, jurídicas y funcionarios públicos.

1.6.3. Ley de propiedad intelectual.

La Ley de Propiedad Intelectual (LPInt.), publicada en el Registro Oficial N° 320 del 19 de Mayo de 1998, nace con el objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos, como un elemento imprescindible para el desarrollo tecnológico y económico del país.

El organismo nacional responsable por la difusión, y aplicación de las leyes de la Propiedad Intelectual en el Ecuador es el INSTITUTO ECUATORIANO DE PROPIEDAD INTELECTUAL (IEPI), el mismo que cuenta con oficinas en Quito, Guayaquil y Cuenca. Es una persona jurídica de derecho público, con patrimonio propio, autonomía administrativa, económica, financiera, y operativa, con sede en la ciudad de Quito.

Dar a conocer la importancia que tiene la Propiedad Intelectual en el Ecuador y su debida aplicación en los sectores económico, industrial, intelectual y de investigación, debe ser tarea no sólo del profesional del derecho, sino de los industriales y empresarios, de las instituciones públicas y privadas, de los centros superiores de estudios e inclusive del propio estado ecuatoriano.

Conocer la propiedad intelectual es también conocer, que uno de los principales problemas que enfrenta esta rama del derecho moderno, es la piratería y falsificación de las obras del intelecto humano, las cuales traen graves consecuencias económicas y sociales; a más de los perjuicios de los titulares de derechos de propiedad intelectual, pues esta pérdida no solo afecta a los fabricantes de los productos falsificados, sino a la reducción de ingresos tributarios e inclusive la pérdida de empleos, debido a los efectos negativos resultantes de la mano de obra clandestina, de las labores creativas y de investigación, perjudicando la vitalidad cultural y económica de un país.

Es importante resaltar que la ley incluye en su codificación la protección de bases de datos que se encuentren en forma impresa u otra forma, así como también los programas de ordenador (software) los cuales son considerados como obras literarias.

El estudio de piratería mundial de software (22), que corresponde al año 2007, realizado por la International Data Corporation (IDC), publicado por la Business Software Alliance, establece que Ecuador mantiene una tasa de piratería de un 66%, que constituyen pérdidas por aproximadamente 33 millones de dólares y representan un incremento del 10% con respecto a la última medición (30 millones de dólares). Las iniciativas dadas para la protección y respeto de las especificaciones de la Ley de Propiedad Intelectual, así como los Derechos de Autor se han desarrollado por campañas de la Business Software Alliance (BSA) tales como “Marca el Límite”, “Anímate 2007”, “Buenos Negocios”, “Evite riesgos, use software legal” como acciones puntuales que impulsan el uso de software legal. Otro proyecto impulsado por la BSA es la habilitación del portal “Reporte confidencial sobre piratería de software”, que permite denunciar de manera confidencial la piratería del software en América Latina.

1.6.4. Ley especial de telecomunicaciones.

La Ley Especial de Telecomunicaciones fue publicada en el Registro Oficial N° 996 del 10 de Agosto de 1992, en el que se declara que es indispensable proveer a los servicios de telecomunicaciones de un marco legal acorde con la importancia, complejidad, magnitud tecnología y especialidad de dichos servicios, así como también asegurar una adecuada regulación y expansión de los sistemas radioeléctricos, y servicios de telecomunicaciones a la comunidad que mejore de forma permanente la prestación de los servicios existentes.

La Ley Especial de Telecomunicaciones tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo radioelectricidad, medios ópticos y otros sistemas electromagnéticos.

1.6.5. Ley orgánica de control constitucional.

La Ley Orgánica de Control Constitucional (LOCCConst.), fue publicada en el Registro Oficial N° 99 del 2 de Julio de 1997 y fue calificada con Jerarquía y carácter de Ley Orgánica, por resolución Legislativa, publicado en Registro Oficial 280 del 8 de Marzo del 2001.

La Ley Orgánica de Control Constitucional, en su Capítulo II del Habeas Data establece que “las personas naturales o jurídicas, nacionales o extranjeras, que desean tener acceso a documentos, bancos de datos e informes que sobre si misma o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les este por dar, podrán imponer el recurso de Habeas Data para requerir las

respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta ley, por parte de las personas que posean tales datos o informaciones”.

En la Constitución del Ecuador vigente (2008), en su capítulo tercero de las Garantías Jurisdiccionales de su sección quinta Art. 92 sobre la acción de Habeas Data, también se establece recurso jurídico de Habeas Data.

1.6.6. Código de procedimiento penal y código de procedimiento civil.

De acuerdo a la especificación contemplada en la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, en su título quinto de las infracciones informáticas, los delitos informáticos que se tipifican, mediante reformas al Código de Procedimiento Penal, se muestran a continuación en la siguiente tabla:

Cuadro 1. Infracciones informáticas

INFRACCIONES INFORMATICAS	REPRESION	MULTAS
Delitos contra la información protegida (CPP Art. 202)		
1. Violentando claves o sistemas accede u obtiene información	6 meses a 1 año	\$500 a \$1000
2. Seguridad nacional o secretos comerciales o industriales	1 a 3 años	\$1.000 - \$1500
3. Divulgación o utilización fraudulenta	3 a 6 años	\$2.000 - \$10.000
4. Divulgación o utilización fraudulenta por custodios	6 a 9 años	\$2.000 - \$10.000
5. Obtención y uso no autorizados	2 meses a 2 años	\$1.000 - \$2.000
Destrucción maliciosa de documentos (CCP Art. 262)	3 a 6 años	---
Falsificación electrónica (CPP Art. 353)	3 a 6 años	---
Daños informáticos (CPP Art. 415)		
1. Daño dolosamente	6 meses a 3 años	\$60 - \$150
2. Servicio público o vinculado con la defensa nacional	3 a 5 años	\$200 - \$600
3. No delito mayor	8 meses a 4 años	\$200 - \$600
Apropiación ilícita (CPP Art. 553)		
1. Uso fraudulento	6 meses a 5 años	\$500 - \$1000
2. Uso de medios (claves, tarjetas magnéticas, otros instrumentos)	1 a 5 años	\$1.000 - \$2.000
Estafa (CPP Art. 563)	5 años	\$500 - 1.000
Contravenciones de tercera clase (CPP Art. 606)	2 a 4 días	\$7 - \$14

Fuente: Código de Procedimiento Penal.

Hemos visto la definición de los delitos informáticos, su principal insumo que es la evidencia digital y las técnicas o mecanismos con los procedimientos existentes para su investigación, vale destacar, entonces que los profesionales dedicados a la persecución de actos ilícitos en los que se utilizan medios tecnológicos, se mantengan a la vanguardia de conocer los avances que se den de ésta índole, y de esta manera mantenerse preparados y reaccionar de manera adecuada ante los actos cometidos por la delincuencia informática.

Ecuador ha dado sus primeros pasos con respecto a las leyes existentes, en las que se contemplan especificaciones de la información y la informática, lo que se considera un avance importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, pero es evidente que aún falta mucho por legislar, para asegurar que no queden en la impunidad los actos que se comentan relacionados con las tecnologías.

1.7. PROPUESTAS INTERNAS.

Conforme a las disposiciones establecidas en la Constitución del Ecuador vigente, en su Capítulo IV, Sección Décima sobre la Fiscalía General del Estado, en el Art. 195 señala: “La Fiscalía dirigirá de oficio o a petición de parte, la investigación pre procesal y procesal penal”, esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que “el ejercicio de la acción pública corresponde exclusivamente al fiscal”. Además contará como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial que realizarán la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control del Ministerio Público.

Phil Williams (27) manifiesta que “es necesario contar no solo con las leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la delincuencia informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle

frente a ese nuevo tipo de delitos”. Estas aseveraciones promueven que a más de las regulaciones, los especialistas necesitan contar con la infraestructura necesaria para la investigación de hechos que involucran el uso de las tecnologías.

1.7.1. Departamento de criminalística de la policía judicial.

La Ley Orgánica del Ministerio Público, según el Art. 2 inciso tercero, dispone que la Policía Judicial estará a órdenes del Ministerio Público para el cumplimiento de sus funciones, siendo entonces, este organismos quién colabore con las investigaciones de orden técnico científico del delito. El Reglamento de la Policía Judicial, fue publicado en el Registro Oficial # 368 de 13 de Julio de 2001, en donde se establecen sus atribuciones, departamentos, atribuciones, y sus campos de acción. El Reglamento de la Policía Judicial, Art. 4 de la Naturaleza y Atribuciones especifica que: “La Policía Judicial es un cuerpo auxiliar del Ministerio Público, integrado por personal especializado de la Policía Nacional. Su funcionamiento se sujetará a las disposiciones contempladas en la Constitución de la República; en la Ley Orgánica del Ministerio Público; en la Ley Orgánica de la Policía Nacional; en el Código de Procedimiento Penal; y en el Reglamento de la Policía Judicial”.

La enumeración que se constituyen en el Reglamento para el Departamento de Criminalística, establece que: “Bajo la dirección de los fiscales, corresponde a los departamentos de criminalística, acudir al lugar de los hechos para proteger la escena del delito; buscar, fijar, levantar, etiquetas las muestras dando inicio a la cadena de custodia, y analizar todos los indicios, señales o evidencias sobre un presunto hecho delictivo, de conformidad con lo establecido en Código de Procedimiento Penal”.

La Policía Judicial, mantiene Departamentos de Criminalística en las provincias de: Pichincha, Guayas, Manabí, Chimborazo, Azuay, Tungurahua, Imbabura, Loja,

Cotopaxi y Los Ríos. Los departamentos de criminalística cuentan con las siguientes secciones:

Cuadro 2. Departamento de criminalística

Secciones del Departamento de Criminalística			
Inspección ocular técnica	Audio, video y afines	Fotografía pericial	Dibujo y planimetría
Identidad física humana	Registro de Detenidos	Balística	Biología
Identificación de grabados y marcas seriales	Incendios y explosivos	Análisis Informático y Telecomunicaciones	Centro de Acopio y conservación de evidencias
Química analítica	Toxicología Analítica	Física	Documentología

Como podemos ver en el cuadro 2, el Departamento de Criminalística, de la Policía Judicial, cuenta con una sección especializada en Análisis Informático y Telecomunicaciones. Según el Reglamento de la Policía Judicial en el Art. 81, se especifica que, a la Sección de Análisis Informático y Telecomunicaciones le corresponde:

- 1) Identificar los procesos y autores de fraude, falsificación, invasión y atentado de los sistemas informáticos y de telecomunicaciones.
- 2) Recopilar y mantener actualizada la información referente a medidas de seguridad informática y en Telecomunicaciones.
- 3) Mantener la cadena de custodia; y
- 4) Demás funciones que se le asignen, creen y/o dispusiere la autoridad legal tendiente al esclarecimiento de un hecho punible.

El Gobierno Nacional del Ecuador, de acuerdo con el proyecto del Plan de Seguridad Ciudadana y Modernización de la Policía (2008-2009) (28), ha presupuestado invertir progresivamente 320 millones de dólares en equipamiento, capacitación, servicios, y remodelación de la Policía.

El proyecto también contempla adquirir herramientas como ADN Forense, microscopio electrónico que permite confirmar residuos de pólvora, elementos que actualmente no existen en el país, así como también dotar de nuevos terminales y servidores para el Sistema IBIS (Sistema Integrado de Identificación Balística), IAFIS (Sistema Integrado Automático de Identificación de Huellas Dactilares) que se conservan en el Departamento de Criminalística.

El proyecto además contempla, iniciativas que involucran convenios con los siguientes organismos:

- 1) Policía Nacional del Perú.
- 2) Secretaria Nacional Anticorrupción.
- 3) Cámara de Comercio de Quito.
- 4) Universidad Central del Ecuador y la Universidad Católica.
- 5) Organismo nacional de trasplante de órganos y tejidos.

1.7.2.Unidad de delitos informáticos del ministerio público.

En correlación con el avance de las tecnologías y ante el incremento de los delitos de esta índole, el Dr. Santiago Acurio del Pino, Director Nacional de Informática del Ministerio Público del Ecuador, propone, el Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público (UDIMP) (29).

La Unidad de Delitos Informáticos del Ministerio Público, tendrá la misión de investigar, perseguir y prevenir todo lo relacionado con la criminalidad informática en todos sus aspectos y ámbitos tales como: amenazas, injurias, pornografía infantil, fraudes, terrorismo informático y hacking.

Entre los objetivos establecidos para dicha unidad se establecen los siguientes:

- 1) Investigar y perseguir a nivel pre-procesal y procesal penal toda infracción que utilice a la informática como medio o fin para la comisión de un delito.
- 2) Capacitar a los miembros de la unidad a nivel técnico para combatir esta clase de infracciones.
- 3) Contribuir y colaborar con la formación continua de los investigadores.
- 4) Formar y mantener alianzas con unidades Especiales de investigación a nivel internacional.
- 5) Desarrollar una política de Seguridad Informática General.
- 6) Implementar a nivel nacional el Sistema de Información de Delitos Informáticos.
- 7) Promover canales de comunicación y trabajo con las distintas estructuras y organizaciones gubernamentales implicadas con la lucha contra el fenómeno de la delincuencia informática.

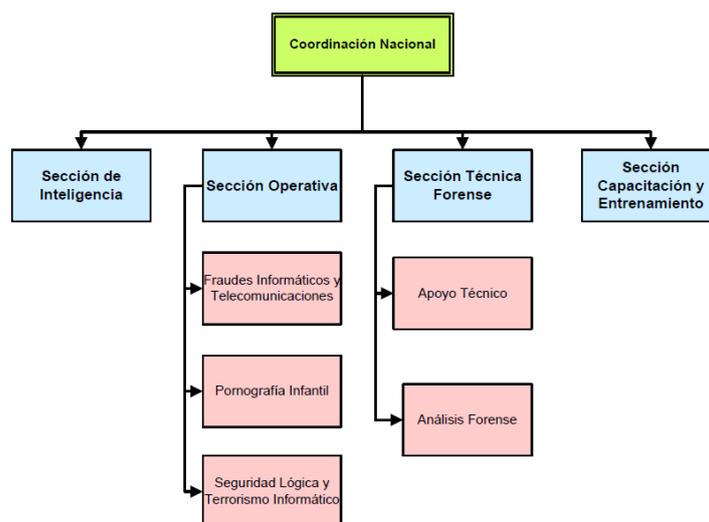
La unidad se conformaría por una coordinación nacional y otra coordinación internacional.

En lo que corresponde a la coordinación nacional la estructura estaría compuesta de la siguiente manera:

- 1) Coordinación Nacional:- Establecerá las políticas y directrices generales de la investigación de los Delitos Informáticos.
- 2) Sección de Inteligencia:- Se encargará de la recolección de las evidencias e indicios relacionados con el cometimiento de los delitos informáticos.
- 3) Sección Operativa:- Realizará las investigaciones de lo relacionado con la criminalidad informática.
- 4) Sección Técnica y Forense:- Brindará apoyo técnico y realizara el análisis forense de las evidencias.

5) Sección de Capacitación y Entrenamiento:- Formación del personal de la Unidad, de la acreditación de los Peritos Informáticos a nivel nacional.

Figura 2. Unidad de Delitos Informáticos



En lo que corresponde a la coordinación internacional del Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público, establece que es primordial instaurar mecanismos de cooperación con organizaciones internacionales, tales como: la INTERPOL, Unión Internacional de Telecomunicaciones(UIT), etc. , en el tema de la cyber delincuencia, para ello se contará con los servicios de la Unidad de Asuntos Internacionales del Ministerio Público del Ecuador, quienes trabajarán estrechamente y en combinación con el Coordinador Nacional, y el Ministro Fiscal General de la Nación, a su vez ellos tendrán la responsabilidad de establecer las políticas de cooperación internacional en materia de delitos informáticos. La UDIM, requiere además contar con la logística (Física y Lógica) necesaria para el funcionamiento de la unidad.

Como podemos advertir, la iniciativa del Dr. Acurio, fomenta la creación de un organismo institucional dentro del Ministerio Público, sin embargo, se deben considerar otros factores externos como la sociedad, las funciones del

Departamento de Criminalística de la Policía Judicial, y como actuaría dicha unidad ante los casos que son manejados de oficio por el Ministerio Público.

1.8.PROPUUESTAS EXTERNAS.

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

1.8.1.Contemplaciones de la organización de estados americanos (OEA)

La Organización de Estados Americanos (OEA), está conformada por 35 países independientes de las Américas, de Norte, Sur y Centroamérica y el Caribe que han ratificado la carta de la OEA y pertenecen a la Organización.

En el mes de marzo del año 1999, los Ministros de Justicia de las Américas que pertenecen a la OEA, encomendaron establecer un Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos (30), que les permita:

- 1) Realizar un diagnostico de la actividad delictiva vinculada a las computadoras y la información de los Estados miembros.
- 2) Realizar un Diagnostico de la legislación, las políticas y las practicas nacionales con respecto a dicha actividad.
- 3) Identificar las entidades nacionales e internacionales que tienen experiencia en la materia; y

4) Identificar mecanismos de cooperación dentro del sistema interamericano para combatir el delito cibernético.

El Grupo de Expertos Intergubernamentales en Materia de Delitos Cibernéticos conformado y creado por recomendación de los Ministros de Justicia, ha mantenido reuniones y talleres importantes a lo largo de los últimos nueve años, en las que se ha permitido conocer las realidades de los países miembros con respecto a los delitos informáticos. Durante la cuarta reunión del Grupo de Expertos Gubernamentales en Materia de Delitos cibernéticos efectuada el 27 y 28 de Febrero del 2006 en Washington DC, de los Estados Unidos, se efectuó un cuestionario a los países miembros de la OEA, sobre delito cibernético en donde se obtuvieron los siguientes resultados.

- 1) 50% de los países posee legislación en delito informático.
- 2) 40% de los países posee legislación procesal que permite la persecución del delito cibernético.
- 3) 53 % de los países posee investigadores especializados.
- 4) 40% de los países posee fiscales especializados.

Entre tanto las recomendaciones de la quinta reunión del Grupo de Expertos, efectuada el 19 y 20 de Noviembre del 2007, en Washington DC, de los Estados Unidos, fueron las siguientes:

- 1) Establecer unidades para que efectúen la investigación y persecución del delito cibernético.
- 2) Mantener información del punto nacional de contacto para la cooperación internacional en materia de delito cibernético.
- 3) Adoptar legislación en materia de delito cibernético.
- 4) Adoptar legislación y procedimientos para la utilización de la prueba electrónica en los procesos penales.
- 5) Vincularse a la “Red de Emergencia de Contactos sobre Delitos de Alta Tecnología las 24 horas los siete días de la semana” del G-8.

- 6) Consolidar el Portal Interamericano de Cooperación contra el Delito Cibernético.
- 7) Compilar las legislaciones en materia de delito cibernético y sobre la prueba electrónica.
- 8) Considerar la aplicación de los principios de la Convención del Consejo de Europa sobre la Delincuencia Cibernética a la adhesión a la misma.
- 9) Fortalecer la cooperación con otras organizaciones internacionales.
- 10) Desarrollar las relaciones con el sector privado para prevenir y combatir el delito cibernético.
- 11) Expresar su satisfacción con los resultados de los talleres auspiciados por Estados Unidos en el 2006 con la cooperación de Brasil, Costa Rica y Barbados.
- 12) Aceptar el ofrecimiento de los Estados Unidos sobre la realización de talleres adicionales.
- 13) Que el grupo de Expertos se reúna por lo menos una vez entre una y otra REMJA (Reunión de Ministros de Justicia de las Américas).

Con estas iniciativas proporcionadas y puestas a consideración de los países miembros de la OEA, se impulsa la cooperación internacional para el seguimiento e investigación de los delitos que afectan las modernas tecnologías así como la habilitación de leyes y organismos que cuenten con tecnología para la persecución de la delincuencia informática.

1.8.2. Regulaciones existentes en Latinoamérica.

A nivel de Latinoamérica algunos países como Chile, Argentina, Venezuela, Perú, cuentan con regulación, a nivel legislativo que tipifica los delitos informáticos, mientras que en otros países se ha procedido a la reforma de los Códigos de Procedimiento Penal para la aplicación de las sanciones, ante las infracciones informáticas cometidas. Además de las reformas concernientes al Código de Procedimiento Penal se mantienen leyes como: Ley de Propiedad Intelectual, Ley de Comercio Electrónico, Ley de Habeas Data, Ley de Firmas Digitales, entre

otras, que establecen especificaciones que conciernen a lo información e informática.

Cuadro 3.Legislación de países latinoamericano.

Legislación de Países Latinoamericanos	Ley de Propiedad Intelectual	Ley de Habeas Data	Ley de Comercio Electrónico, Mensajes de Datos y	Ley de Delitos Informáticos	Ley de Transparencia y Acceso a la Información	Ley de Pornografía Infantil	Ley Uso de correo electrónico (SPAM)
Argentina	▼	◆	●	▲			
Bolivia					D		
Brasil		◆	●				
Chile	▼		●	▲		◆	
Colombia			●	▲	■		
Costa Rica				▲			
Ecuador	▼	◆	●		■		
Guatemala			●				
México				Proy.	■		
Panamá			●				
Paraguay					■		
Perú			●	▲	■		▼
República Dominicana			●				
Uruguay							Proy.
Venezuela			●	▲			

El cuadro 3 resume de manera general las leyes con las que cuentan países latinoamericanos, en donde se establecen mecanismos que permiten la persecución de delitos en los que se utilizan las tecnologías.

CAPÍTULO II

METODOLOGÍA

2.1. VALIDACIÓN METODOLÓGICA

Para la realización de este trabajo, se utilizaron varios métodos, técnicas, procedimientos, como actividades, encuestas a docentes y estudiantes de la carrera de Derecho, también se realizó las entrevistas a los funcionarios judiciales de la provincia de Santa Elena, con la finalidad de alcanzar los objetivos planteados. Entre ellos el método descriptivo, deductivo, analítico, explicativo, evaluativo y como base del trabajo el método científico.

2.2. MÉTODOS Y TÉCNICAS APLICADAS PARA EL LEVANTAMIENTO DE INFORMACIÓN:

En la investigación que se está realizando el paradigma cualitativo, se refiere a solucionar el problema que se presenta a la hora de ofrecer servicios de que implique delitos informáticos, tomando en cuenta que los involucrados en la actividad hacen caso omiso de sanciones apropiadas para aquellos que cometen este tipo de delitos, por lo que esta investigación se la caracteriza mediante:

- Utilización de técnicas cualitativas
- Interpretación del problema o fenómeno de estudio
- Se refiere a aspectos particulares
- Es más subjetiva, porque el investigador puede filtrar datos según su criterio.
- Conocimiento orientado a los procesos.

En este estudio no sólo se investigó especialistas, sino que plantea una propuesta viable que conlleve a la solución de los perfiles de desempeño en cada una de las personas que laboran en el área de derecho, considerando el apoyo de investigaciones de tipo documental y de campo, que conlleven a establecer las pautas y características esenciales inherentes a la fundamentación teórica de la investigación.

2.3. TIPO DE INVESTIGACIÓN SELECCIONADA

El éxito de la investigación depende de la calidad de la información que se adquiera, tanto de las fuentes primarias como de las secundarias así como del procesamiento y presentación de la información

Por ello se presenta a continuación los tipos de investigación utilizadas en el trabajo de investigación:

- Descriptiva
- Exploratoria
- Bibliográfica
- De Campo
- Documental

2.3.1. Descriptiva

El estudio descriptivo identifica características del universo de investigación, señala formas de conductas, establece comportamientos concretos y describe y comprueba la asociación entre las variables de la investigación.

Se aplicó este tipo de investigación tomando como base el fenómeno informático de las actividades que se realizan en la Santa Elena, tal como se mencionó en el capítulo I.

Utilizando el método descriptivo, resultó evidente la recopilación de datos obtenidos mediante entrevistas a los involucrados en el área de Derecho de la Provincia, así como también las encuestas realizadas a los estudiantes de la comunidad.

2.3.2. Exploratoria

Su objetivo fue la formulación de un problema y posibilitó una investigación precisa el desarrollo de una hipótesis. Pero tuvo otras funciones, como la de aumentar la familiaridad del investigador con el fenómeno que va a investigar, aclarar conceptos, establecer preferencias para posteriores investigaciones.

2.3.3. Bibliográfica

Por otro lado la recopilación de datos secundarios se obtuvo de fuentes como: Bibliotecas, textos, revistas especializadas, internet, departamentos jurídicos, filmaciones, fotografías, guías de observación, trabajos de investigación. Así como de la participación de la comunidad, sin olvidar que el trabajo será coordinado en tiempo y espacio.

Mediante este tipo de investigación se ayudó a respaldar el tema de investigación tomando datos de conocidos autores considerando principalmente su fuente bibliográfica en el marco teórico, los mismos que ayudaron a la realización de la propuesta mediante su aporte con los conocimientos que ellos relatan en cada una de sus autorías.

2.3.4. Campo

Mediante esta investigación se pudo recopilar una información relevante para respaldar o fundamentar el tema de investigación, mediante los datos que se obtuvieron en la comunidad misma.

2.3.5. Documental

Se utilizó la investigación documental al momento que se tomó referencias bibliográficas aplicadas a aspectos generales que son de base para fundamentar la naturaleza y el propósito del trabajo de tesis.

Mediante la recopilación de datos provenientes de documentos, trabajos y libros directamente relacionados al sector Legislativo, específicamente al manejo de delitos informáticos, considerando que son de gran importancia al brindar orientación para la elaboración de la propuesta la misma que debe estar en función de los resultados de campo que se llevó a cabo, contribuyendo significativamente al desarrollo y seguridad de la localidad.

2.3.6. Fuentes secundarias

Para el presente estudio, se utilizaron técnicas de investigación que permitieron la obtención de información mediante su procesamiento, considerando la problemática existente.

Se realizó el respectivo análisis de resultados para determinar la confiabilidad y validez del trabajo de investigación tomando en cuenta la información que se obtuvo de los diferentes instrumentos utilizados. Entre las técnicas de investigación más utilizadas se detallan:

2.3.6.1. Encuestas

Consistió en una investigación realizada sobre una muestra de sujetos, representativa de un colectivo más amplio que se lleva a cabo en el contexto de la vida cotidiana, utilizando procedimientos estandarizados de interrogación con el fin de conseguir mediciones cuantitativas sobre una gran cantidad de características objetivas y subjetivas de la población.

Para un mejor estudio se llevó a cabo la técnica de recolección de datos llamada encuesta personal. Las encuestas fueron realizadas en los diferentes sitios, considerando a estudiantes, funcionarios y docentes y sin hacer distinción de clase social.

El objetivo de las encuestas fue determinar cuál fue la percepción de los habitantes en cuanto al conocimiento sobre el delito informático.

2.4 . SELECCIÓN DEL TAMAÑO DE LA MUESTRA

La población y muestra tiene un universo de estudio que es el siguiente:

3 Funcionarios Judiciales de la provincia de Santa Elena

5 Docentes de la carrera de Derecho de la Universidad Estatal Península de Santa Elena.

10 Estudiantes del último semestre de la carrera de Derecho de la Universidad Estatal Península de Santa Elena.

CANTIDADES QUE SE SINTETIZAN EN LA TABLA N° 1

Cuadro N° 4: OBJETOS DE INVESTIGACIÓN

OBJETO DE LA INVESTIGACIÓN	POBLACIÓN	MUESTRA	PORCENTAJE
Funcionarios	3	3	100
Estudiantes	184	18	10
Docentes	15	5	30

2.5. DESCRIPCIÓN DE LA INFORMACIÓN OBTENIDA

La técnica que permitió obtener la información y determinar la necesidad de diseñar un plan de propuesta fue la encuesta, a partir de la cual se realizó el análisis, traficación e interpretación de los resultados. La muestra de 18 estudiantes se estructuró tomando 6 estudiantes de cada uno de los últimos semestres de la carrera de Derecho de la Universidad Estatal Península de Santa Elena.

Las encuestas aplicadas a los docentes y estudiantes de la carrera de Derecho, y los funcionarios judiciales de la provincia de Santa Elena, se orientan con cada hipótesis planteada en el problema de investigación.

Las informaciones y opiniones recolectadas son coincidentes con relación a la necesidad de dar más énfasis en la instrucción en lo referente a las infracciones o delitos informáticos dentro de nuestro medio.

2.6. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

El análisis e interpretación de los resultados se efectuaron considerando datos cuantitativos y cualitativos que proyectaron las técnicas de investigación como en este caso, la encuesta.

La preparación de datos consistió: en un proceso de organización de la información con el objeto que sea lo más preciso y permita realizar un análisis fidedigno de las opiniones, criterios proporcionados por los docentes y estudiantes de la carrera de Derecho, y los funcionarios judiciales de la provincia de Santa Elena.

Con la ayuda de la tecnología se ingresaron los datos obtenidos al programa de EXCEL, utilizando formulas y cálculos estadísticos, creando así una base de datos sobre la cual se realizó distintas lecturas y análisis que nos sirvieron para acceder a las conclusiones y recomendaciones, a su vez la elaboración de una propuesta que será de gran aporte para la institución educativa.

2.7. CONSTRUCCIÓN DEL INFORME DE LA INVESTIGACIÓN

La estructuración del Informe de investigación direccionó a la presentación escrita de los resultados alcanzados a través de la investigación realizada.

Este proceso parte de la contextualización del problema planteado y estudiado como los objetivos e hipótesis formuladas, los resultados obtenidos que nos permitieron confrontar las hipótesis y la interpretación de resultados, para la elaboración de conclusiones y recomendaciones parciales, y en base al análisis de las mismas, llegar a la fase de elaboración de las conclusiones y recomendaciones finales.

Y finalmente acceder al diseño y descripción de los lineamientos de la propuesta alternativa como una posibilidad de mejoramiento y de solución a un problema, visualizado en el proceso de investigación.

ANÁLISIS

HIPÓTESIS GENERAL.

El conocimiento del tema de Delitos Informáticos es importante para mejorar la capacitación profesional de los estudiantes de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena.

VARIABLE INDEPENDIENTE: La falta de una profunda capacitación a los estudiantes de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena, en lo referente al tema de Delitos Informáticos.

VARIABLE DEPENDIENTE: La falta de preparación pre profesional de los abogados en el libre ejercicio de la profesión, conlleva a que no se encuentren capacitados para patrocinar casos que versen acerca de delitos informáticos.

Encuesta a estudiantes

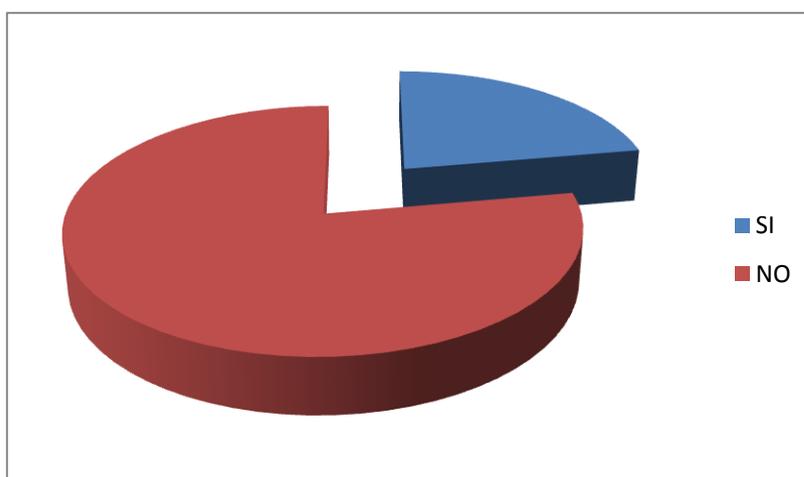
Pregunta:

1) **¿Ha estudiado usted la reforma al Código Penal por parte de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas publicada en Ley No. 67? Registro Oficial. Suplemento 557 de 17 de Abril del 2002?**

Tabla 1: ENCUESTA A ESTUDIANTES

Alternativas	ESTUDIANTES	
	N°	%
SI	4	22.3
NO	14	77.7
Total	18	100

GRAFICO 1: ENCUESTA A ESTUDIANTES



Fuente: Estudiantes de la Carrera de Derecho UPSE.

Responsables: Alejandro Mendoza y Jorge Malla.

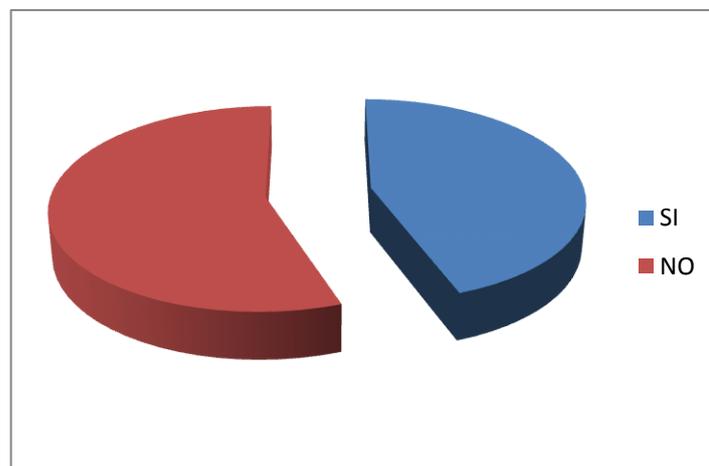
Consultado sobre el conocimiento de los estudiantes a las reformas aplicadas al código penal, se obtiene que el 15% manifiesta que SÍ, y el 85% que NO. En función de las respuestas obtenidas, se establece que QUINCE POR CIENTO de los estudiantes dicen que Sí conocen información referente a las reformas que se han aplicado al código penal, mientras que la gran mayoría desconoce del tema.

Pregunta:2) ¿Conoce que procedimiento debe seguir para la persecución de un delito informático?

Tabla 2: Procedimiento

Alternativas	ESTUDIANTES	
	N°	%
SI	8	44.5
NO	10	55.5
Total	18	100

GRAFICO 2: Procedimiento



Fuente: Estudiantes de la Carrera de Derecho UPSE.

Responsables: Alejandro Mendoza y Jorge Malla.

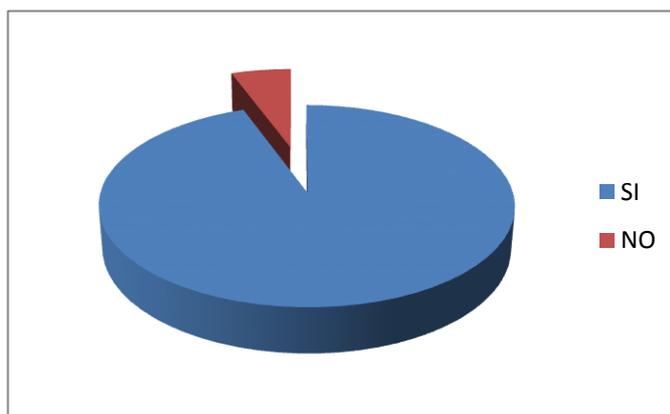
Consultado sobre el conocimiento de los estudiantes a las reformas aplicadas al código penal, se obtiene que el 15% manifiesta que SÍ, y el 85% que NO. En función de las respuestas obtenidas, se establece que QUINCE POR CIENTO de los estudiantes dicen que Sí conocen información referente a las reformas que se han aplicado al código penal, mientras que la gran mayoría desconoce del tema.

Pregunta:3) ¿Considera usted que es importante aprender sobre este tema?

Tabla 3: Importancia sobre el tema

Alternativas	ESTUDIANTES	
	N°	%
SI	17	94.4
NO	1	5.6
Total	18	100

GRAFICO 3: Importancia sobre el tema



Fuente: Estudiantes de la Carrera de Derecho UPSE.

Responsables: Alejandro Mendoza y Jorge Malla.

Consultado a los estudiantes sobre la necesidad e importancia de aprender el tema de delitos informáticos, se obtiene que el 94.4% manifiesta que SI, y el 5.6% que NO. En función de las respuestas obtenidas por los estudiantes, se establece que el noventa y cuatro por ciento manifiesta la necesidad e importancia de tener más información referente al tema de delitos informáticos, mientras que el cinco por ciento se muestra renuente a profundizar en el tema.

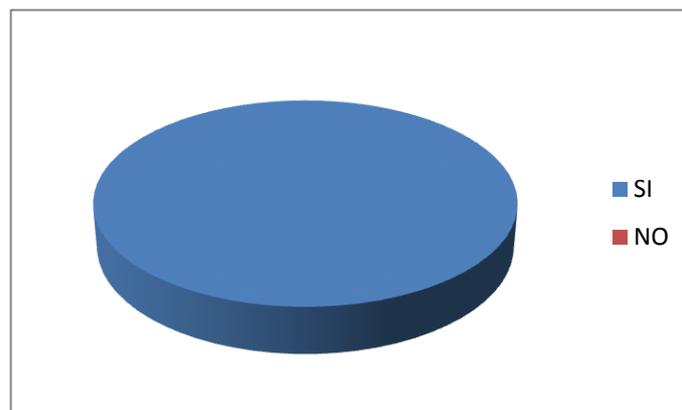
Pregunta:

4) ¿Cree usted que es importante enfatizar en la enseñanza en lo referente a Delitos Informáticos a los estudiantes de la Carrera de Derecho?

Tabla 4: **Delitos Informáticos**

Alternativas	DOCENTES	
	N°	%
SI	5	100
NO	0	0
Total	5	100

GRAFICO 4: **Delitos Informáticos**



Fuente: Estudiantes de la Carrera de Derecho UPSE.

Responsables: Alejandro Mendoza y Jorge Malla.

Consultado sobre la importancia de enfatizar la enseñanza en lo referente a Delitos Informáticos a los estudiantes de la Carrera de Derecho, se obtiene que el 100% manifiesta que SÍ, y el 0% que NO. En función de las respuestas obtenidas por los docentes, se establece que el cien por ciento está de acuerdo con que se debe enfatizar la enseñanza en lo que respecta a delitos informáticos, puesto que cada vez son más comunes las infracciones de este tipo dentro de nuestro medio.

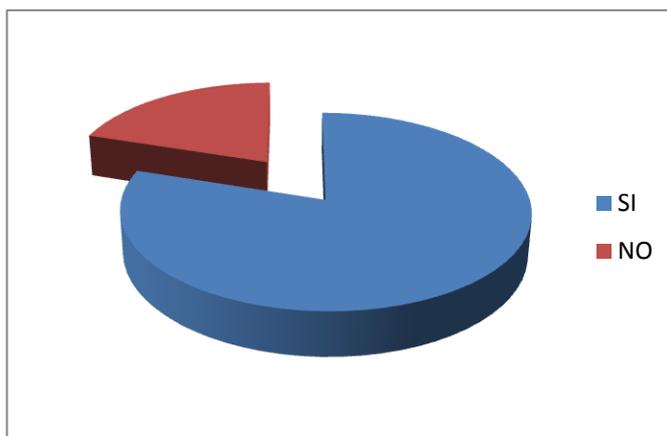
Pregunta:

5) ¿Cree que es importante el tema para la preparación profesional de los estudiantes de la Carrera de Derecho?

Tabla 5: importante el tema para la preparación profesional

Alternativas	DOCENTES	
	N°	%
SI	4	80
NO	1	20
Total	5	100

GRAFICO 5: importante el tema para la preparación profesional



Fuente: Estudiantes de la Carrera de Derecho UPSE.

Responsables: Alejandro Mendoza y Jorge Malla.

Consultado sobre la importancia del tema para la preparación profesional de los estudiantes de la carrera, se obtiene que el 80% manifiesta que SÍ, y el 20% que NO. En función de las respuestas obtenidas de los docentes, se establece que el ochenta por ciento está de acuerdo con que el tema es importante para la preparación profesional de los futuros abogados, mientras que el veinte por ciento manifiesta que depende de cada estudiante cultivarse en el tema.

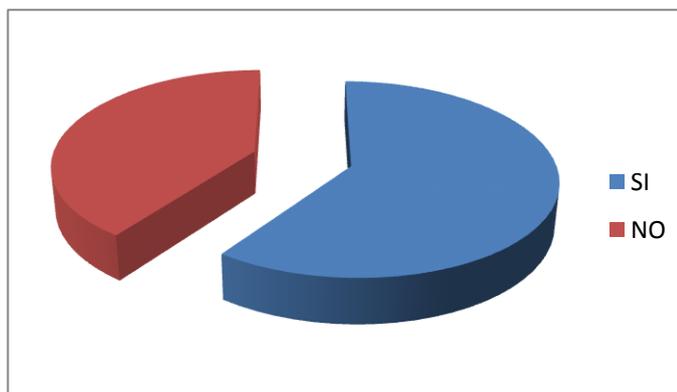
Pregunta:

6) ¿Cree necesario implementar en la malla curricular de la Carrera de Derecho de la UPSE, un modulo que capacite en Delitos Informáticos?

Tabla 6: implementar en la malla curricular de la Carrera

Alternativas	DOCENTES	
	N°	%
SI	3	60
NO	2	40
Total	5	100

GRAFICO 6: implementar en la malla curricular de la Carrera



Fuente: Estudiantes de la Carrera de Derecho UPSE.

Responsables: Alejandro Mendoza y Jorge Malla.

Consultado a los docentes acerca de la necesidad de implementar en la malla curricular de la carrera de derecho de la Universidad Estatal Península de Santa Elena un modulo para la capacitación de sus estudiantes, se obtiene que el 60% manifiesta que SÍ, y el 40% que NO. En función de las respuestas obtenidas, se establece que en un sesenta por ciento los docentes están de acuerdo con que se implemente un modulo especializado en delitos informáticos dentro de la malla curricular de la carrera, mientras que un cuarenta por ciento considera que con las materias que ya existen dentro de la antes mencionada malla curricular es suficiente para la capacitación del estudiantado de la carrera de derecho.

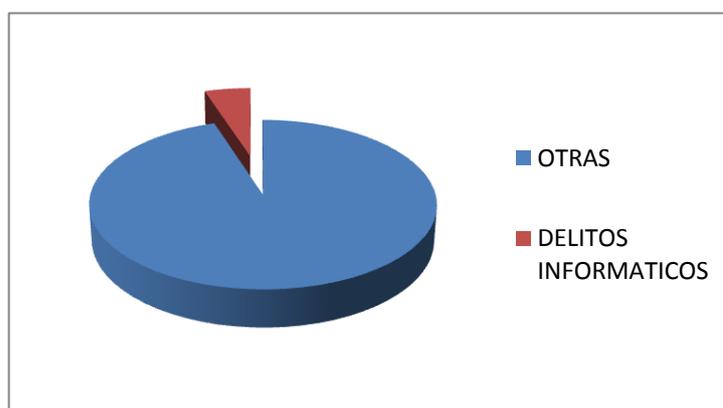
Pregunta:

7) ¿De las causas tramitadas en su despacho, cuantas se refieren a delitos informáticos?

Tabla 7: ENCUESTA A FUNCIONARIOS JUDICIALES

Alternativas	FUNCIONARIOS JUDICIALES
	%
OTRAS	98
DELITOS INFORMÁTICOS	2
Total	100

GRAFICO 7: ENCUESTA A FUNCIONARIOS JUDICIALES



Fuente: Estudiantes de la Carrera de Derecho UPSE.

Responsables: Alejandro Mendoza y Jorge Malla.

Consultado a los funcionarios judiciales sobre la cantidad de causas tramitadas en sus despachos y el porcentaje correspondientes a Delitos Informáticos, se obtiene que el 98% pertenezcan a otras causas, y el 2% que corresponden a delitos informáticos. En función de las respuestas obtenidas por los funcionarios judiciales, se establece que el noventa y ocho por ciento de las causas que se tramitan en sus despachos corresponden a otro tipo de infracciones, mientras que solo el dos por ciento se generan por delitos informáticos lo que deja en evidencia que la ciudadanía no opta por perseguir justicia en estos casos debido a la falta de patrocinio especializado.

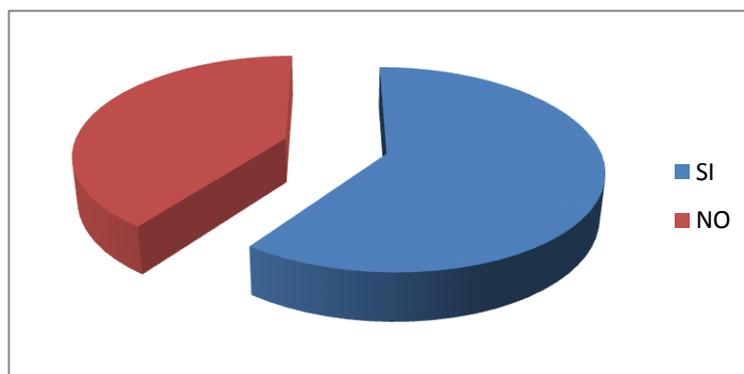
Pregunta:

8) ¿Considera usted que los profesionales del derecho se encuentran lo suficientemente capacitados para litigar en este tipo de causas?

Tabla 8: capacitados para litigar en este tipo de causas

Alternativas	FUNCIONARIOS JUDICIALES	
	Nº	%
SI	1	33.3
NO	2	66.6
Total	3	100

GRAFICO 8: capacitados para litigar en este tipo de causas



Fuente: Estudiantes de la Carrera de Derecho UPSE.

Responsables: Alejandro Mendoza y Jorge Malla.

Consultado a los Funcionarios Judiciales sobre la preparación de los profesionales del derecho en cuanto a lo referente a Delitos informáticos, se obtiene que el 33.3% manifiesta que SÍ, y el 66.6% que NO. En función de las respuestas obtenidas por los funcionarios judiciales, se establece que el treinta y tres por ciento de los profesionales del derecho en el libre ejercicio de la profesión se encuentran preparados para litigar en los casos que versen acerca de delitos informáticos, mientras que la gran mayoría no se encuentran preparados para patrocinar este tipo de causas.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones.

Una vez realizado el trabajo de investigación **“ESTUDIO DEL TRATAMIENTO DE LOS DELITOS INFORMÁTICOS DENTRO DE LA PENÍNSULA DE SANTA ELENA”** se llega a las siguientes conclusiones:

- En la carrera de Derecho de la Universidad Estatal Península de Santa Elena, todos sus actores coinciden que si se profundizara en la enseñanza en lo que respecta al tema de delitos informáticos, el rendimiento no solo de los estudiantes si no de los profesionales del derecho en general, sería más especializado sobre todo en la parte práctica.
- Pese a existir esta realidad, en la institución, desde sus autoridades hasta sus docentes, no toman medidas para que cada uno de sus integrantes, tengan una capacitación adecuada en lo referente a el tema de Delitos Informáticos.
- Existe la necesidad de implementar procesos de capacitación, con talleres, charlas, concientizando la importancia de mostrar para crear mecanismos de mejoramiento personal que mejoren el proceso de aprendizaje en lo referente al tema de Delitos Informáticos.

Recomendaciones

- Socializar los resultados, de la investigación en espacios democráticos y participativos en los que intervengan docentes y estudiantes.

- Como gestores impulsar la importancia que tiene el tema de Delitos Informáticos, en el ámbito legal. como un proceso de diálogo, comprensión y mejoramiento.
- Aplicar nuevas estrategias para que la Universidad Estatal Península de Santa Elena, innove su malla curricular incorporando contenidos enfocados a la capacitación especializada en Delitos Informáticos.
- Programar para cada año lectivo actividades de capacitación a docentes y estudiantes; enfocando nuevos temas en materias de derecho, que se hacen necesarios por los constantes cambios sociales y tecnológicos que se viven en el medio. Desembocando todo, en un acto de principios que regulen la vida de nuestra sociedad.

CAPITULO III

PROPUESTA ALTERNATIVA

3.1 TITULO

“Creación de un modulo practico acerca de delitos informáticos para ser implementado a la malla curricular de la Carrera de derecho de la Universidad Estatal Península de Santa Elena”

3.1.2. Alcance

El conocimiento sobre el delito informático en el ecuador al igual que la orientación a los estudiantes de la carrera de Derecho para que desarrollen otras actividades complementarias que impulsen a la seguridad interactiva de localidad, las que son presentadas en el presente módulo de Capacitación

En el alcance se describe lo siguiente:

- A quien va dirigido el servicio (Estudiantes y docentes de la carrera de Derecho)
- Necesidades de la población
- Región geográfica a cubrir
- Áreas relacionadas

3.2. RESPONSABILIDADES PARA LA APLICACIÓN DEL MÓDULO DE CAPACITACIÓN.

La aplicación indicadas en el presente Módulo de Capacitación, deben ser asumidas de manera responsable por los involucrados en el área de Derecho, quien es responsable de verificar el conocimiento asimilación y cumplimiento de las leyes que rigen la sociedad en el caso de la presencia de algún delito informático en cualquiera de los sectores productivos de la comunidad peninsular.

3.3 VISION

La provincia de Santa Elena genera e impulsa el desarrollo tecnológico mediante los servicios que ofrece la internet y demás técnicas relacionadas la optimización y mejora de los servicios que las diferentes empresas ofrecen mediante la misma, el cual esta propenso a sufrir de algún tipo de sabotaje informático el mismo que debe ser protegido y penalizado de acuerdo a las leyes del Ecuador.

3.4. MISIÓN

Establecer a la provincia de Santa Elena como un sitio con seguridad y servicio capacitado y oportuno de las personas que ejercen en el área de Derecho, plenamente capacitado y listo para actuar cuando se presente algún delito informático.

3.5. JUSTIFICACIÓN

Los resultados de la investigación demuestran la necesidad de implementar un modulo practico sobre delitos informáticos con el cual queremos lograr que los futuros profesionales de la Carrera de Derecho de la Universidad Estatal

Península de Santa Elena estén actualizados en sus conocimientos acorde con los adelantos tecnológicos.

Con esta propuesta se aspira a realizar actividades educativas fundamentales que los docentes indicados de la carrera de derecho de la universidad deberán de tratar, socializar y evaluar lo que este modulo acerca de delitos informáticos les pueda ayudar a los nuevos profesionales de la carrera de derecho.

3.6 FUNDAMENTACIÓN

Esta propuesta se fundamenta en los resultados de esta investigación los mismos que indican el poco conocimiento por parte de un importante grupo de nuevos profesionales de derecho ya que debido al avance tecnológico y jurídico se hace necesario profundizar en este tema y se tenga el conocimiento necesario para poder litigar en lo referente a esta nueva forma de delitos.

3.7 OBJETIVOS

3.7.1 General

El objetivo general de esta problemática es que los nuevos profesionales de la Universidad Estatal Península de Santa Elena tengan el conocimiento necesario y suficiente en materia de delitos informáticos y puedan hacer frente en los campos de la justicia ordinaria.

3.7.2 Específicos

- Revisar todos los antecedentes posibles como Derecho Civil, Derecho Penal, Derecho Administrativo, y demás ramas jurídicas relacionados al tema de delitos informáticos.

- Entender los conceptos básicos y la importancia de los delitos Informáticos en los procesos Judiciales.
- Conocer los principales tipos de delitos informáticos y la legislación vigente en el Ecuador para sancionarlos.
- Revisar el Código penal y de procedimiento penal para establecer cuáles son considerados como delitos informáticos.
- Entender todos los convenios internacionales acerca de los delitos informáticos.

3.8. IMPORTANCIA

La importancia de la propuesta radica en la necesidad de adquirir nuevos conocimientos jurídicos en materia de delitos informáticos a los estudiantes de derecho de la universidad estatal península de Santa Elena, ya que debido a los adelantos tecnológicos que ha experimentado la sociedad y a los nuevos métodos de delinquir se hace necesario un estudio minucioso referente a la temática antes expuesta.

3.9. UBICACIÓN SECTORIAL Y FÍSICA.

En la Universidad Estatal Península de Santa Elena la misma que está ubicada en la Provincia de Santa Elena en la vía principal Santa Elena La Libertad.

En la actualidad esta Universidad cuenta con 184 estudiantes y 15 profesores

3.10. FACTIBILIDAD

Debido a que en la Carrera de Derecho de la Universidad Estatal Península de Santa Elena no cuenta con un estudio focalizado referente a los delitos informáticos, este modulo será de gran utilidad para la carrera, docentes y alumnos para que de esta forma conjunta se pueda dar una mejor preparación académica y por ende unos mejores profesionales.

3.11. PLAN DE TRABAJO

A fin de motivar y socializar a las autoridades, la propuesta de trabajo, y poder plantear un esquema educativo en este tipo de delito, es indispensable elaborar y presentar un plan de trabajo hacia los objetivos propuestos.

3.12. ACTIVIDADES

Para el logro de los procesos planteados y con el fin de que la propuesta, sea aceptada en el desarrollo metodológico de las actividades, los diseños que se utilizarán estarán basados en los modelos y técnicas contenidas en la educación.

TABLA N° 9: ACTIVIDADES

Etapa	ACTIVIDADES	DURACION	INICIO	FINALIZACION
INICIAL	Reunión con docentes sobre la realización de el modulo acerca de delitos informáticos	4horas	16-12-2011	16-12-2011
INTERMEDIA	Etapa de Inicio del desarrollo del Modulo Educativo acerca de delitos informáticos para los estudiantes de la Carrera de Derecho	10 días	22-12-2011	5-01-2012
INTERMEDIA	Etapa media del desarrollo del Modulo Educativo acerca de delitos informáticos para los estudiantes de la Carrera de Derecho	10 días	7-01-2012	17-01-2012
INTERMEDIA	Etapa final del desarrollo del Modulo Educativo acerca de delitos informáticos para los estudiantes de la Carrera de Derecho	10 días	20-01-2012	30-01-2012
FINAL	Revisión de los docentes especializados en desarrollo de materiales educativos.	Al finalizar el modulo 4 horas	01-02-2012	01-02-2012

Programación: Duración del Modulo 8 horas en el cual se desarrollaran las clases antes programadas para la capacitación de los estudiantes. Los temas se detallan a continuación.

TABLA N° 10: CONTENIDOS

DIAS	Contenidos
1	Introducción a los delitos Informáticos 1.- Delimitación del Fenómeno de la Delincuencia Informática
2	1.1.- Generalidades 1.2.- Delimitación del Fenómeno a) Delincuencia informática y Abuso Informático b) Criminalidad informática 1.3.- Definición y el concepto de Delitos Informáticos
3	2. – Sujetos del Delito Informático 2.1.- Sujeto Activo 2.2 - Sujeto Pasivo
4	3. - Bien Jurídico Protegido 3.1.- Los Bienes Jurídicos Protegidos 4. – Tipos de Delitos informáticos
5	Tipificación de los delitos informáticos 4.1. - Los fraudes
6	4.2. - El sabotaje informático 4.3. - El espionaje informático y el robo o hurto de software 4.4. - El robo de servicios 4.5. - El acceso no autorizado a servicios informáticos
7	5.- El Delito Informático y su realidad procesal en el Ecuador

8	6.- Problemas de Persecución 6.1.- Problemática con la concepción tradicional de tiempo y espacio 6.2. Anonimato del Sujeto Activo
Responsables	Rector Decano de la Carrera de Derecho Director de la Carrera de Derecho

RECURSOS (ADMINISTRATIVOS, FINANCIEROS, TECNOLÓGICOS).

TABLA N° 11: RECURSOS

A.- TALENTOS HUMANOS		
TIPO DE PERSONAL	DURACION DEL CONTRATO	COSTO
Docentes externos	8 horas	\$ 80,00
B.- RECURSOS MATERIALES		
TIPO	CANTIDAD	COSTO
Hojas papel A4	1 resma	\$ 3,00
Módulo	3	\$ 9,00
Material y Suministro varios	10	\$ 50,00
C.- VARIOS		
TIPO	CANTIDAD	COSTO
REFRIGERIOS	10	\$ 10,00
IMPREVISTOS		\$ 10,00
TOTAL		\$162,00

3.13. COSTO TOTAL DEL PROYECTO.

El costo total del proyecto asciende a la cantidad de \$ 162 (Ciento sesenta y dos, 00/100 DÓLARES AMERICANOS).

3.14 IMPACTO.

El impacto de la presente propuesta redundará positivamente en las estructuras educativas de la Escuela de Derecho de la Universidad Estatal Península de Santa Elena, ya que la capacitación y la formación del talento humano siempre tiende a la actualización, más aun cuando se trata de profesionales en materia de Derecho, que están constantemente orientando y facilitando procesos jurídicos a ciudadanos de nuestra Península.

Por lo tanto creemos que impactarán en los siguientes aspectos:

En materia de derecho, la comunidad Peninsular contará con personas valiosas en pensamientos e ideas actualizadas, con profesionales altamente preparados, con actitud de crecimiento profesional, la inclusión de este modulo en delitos informáticos a la comunidad universitaria será una experiencia nueva y positiva que podrá servir a todos los estudiantes que cursen en la escuela de derecho hacia la consecución de tener profesionales capacitados en este tema.

En el aspecto social se logrará que los nuevos profesionales sean multiplicadores de este nuevo conocimiento y aporten en todo lo relacionado al tema para fortalecer a todo el sistema judicial peninsular, ya que esta actualización de conocimiento se constituye en una herramienta muy importante para combatir a este nuevo tipo de delincuencia.

3.15. EVALUACIÓN.

Todo proceso educativo tiene que ser evaluado, de allí que se realizará una evaluación diagnóstica, la misma que será monitoreada al final de la capacitación, para tener un referente cercano de los conocimientos, que tienen los estudiantes con relación al tema que se expone.

En la fase final, se confrontará la evaluación diagnóstica con el nivel de desarrollo alcanzado, luego también se visualizará falencias y errores, para la reprogramación del proyecto de ser necesario.

Y finalmente se analizarán y sistematizarán los resultados.

GUÍA DE EVALUACIÓN DE PROCESO-RESULTADOS

Participante:

Fecha:

Responsable:

Dimensión de la Evaluación

1.- Efectividad de la Propuesta

2.- Relevancia de la Propuesta.

Escala Valorativa

A= Óptima = Superior al 80% de calidad y/o rendimiento

B= Aceptable = Entre el 60% y el 79% de calidad y/o rendimiento

C= Mínima = Entre el 40% y el 59% de calidad y/o rendimiento

D= Deficitaria = Menos del 40% de calidad y/o rendimiento

TABLA N° 12: Criterios

1	EFFECTIVIDAD DE LA PROPUESTA	A	B	C	D
1.1	Grado de cumplimiento de la programación				
1.2	Grado de cumplimiento de los objetivos de la propuesta				

Fuente: Universidad Estatal Península de Santa Elena

Elaboración: Jorge Malla Reyes y Alejandro Mendoza Illescas

TABLA N° 13: Criterios

2	RELEVANCIA DE LA PROPUESTA	A	B	C	D
2.1	Grado de Correspondencia entre los contenidos de la propuesta y los requerimientos del desarrollo social.				
2.2	Grado de impacto de la propuesta en la sociedad.				

Fuente: Universidad Estatal Península de Santa Elena

Elaboración: Jorge Malla Reyes y Alejandro Mendoza Illescas

TABLA N° 14: Valoración

VALORACIÓN GENERAL DE LA PROPUESTA	CRITERIO %
1 Grado de cumplimiento de la programación	
2 Grado de cumplimiento de los objetivos	
3 Grado de correspondencia contenidos-social	
4 Grado de impacto de la propuesta en la sociedad	

Fuente: Universidad Estatal Península de Santa Elena

Elaboración: Jorge Malla Reyes y Alejandro Mendoza Illescas

BIBLIOGRAFÍA

- ALESTUEY D, Ma.(2004). “Apuntes sobre la perspectivacriminológica de los delitos informáticos”, Aranzadi Ed. Mérida,
- ÁLVAREZ, José L. (2007). “Delitos Informáticos”. Ponencia en las Jornadas sobre Marco Legal y Deontológico de la Informática, Mérida.
- ANDRADE S, Diana (2004). El Derecho a la Intimidad, Centro Editorial Andino, Quito – Ecuador.
- BAÓN R, Rogelio. (2006) “Visión general de la informática en el nuevo Código Penal”, en *Ámbito jurídico de las tecnologías de la información*, Madrid.
- BARATTA Alessandro (2005) Derecho Penal Mínimo, Editorial Temis S.A. Santa Fe de Bogotá, Colombia.
- BARBIERI Pablo (2003), Contratos de Empresa, Editorial Universidad, Buenos Aires, Argentina.
- BARRIUSO RUIZ, Carlos (2002). “Interacción del Derecho y la informática”, Dykinson, pág. 245 a 252, Madrid.
- BECCARIA Alessandro, (2001). De los Delitos y las Penas, Editorial Temis S.A. Santa Fe de Bogotá, Colombia.
- BETTIOL Giuseppe (2005), Derecho Penal, Editorial Temis, Bogotá, Colombia.

- BUENO ARÚS, Francisco. (2008) “El delito informático”, Actualidad Informática Aranzadi N° 11.
- CABANELLAS, Guillermo (2005) Diccionario de Derecho Usual, Tomo 1, Editorial Heliasta.
- CORREA Carlos María, (2003) El Derecho Informático en América Latina, Publicado en Derecho y Tecnología Informática, Edit. Temis, Bogotá,
- CREUS Carlos, (2006) Derecho Penal Parte Especial, Edit. Astrea, Buenos Aires, Tomo 2.
- CUERVO José, (2010) Delitos Informáticos y Protección Penal a la Intimidad, Publicación hecha en Internet URL: www.derecho.org
- DALLAGLIO Edgardo (2002), “La Responsabilidad Derivada de la Introducción y Propagación del Virus de las Computadoras”.
- DAVARA R, M (2001) “De las Autopistas de la Información a la Sociedad Virtual”, Editorial Aranzadi.
- JIJENA LEIVA, Renato (2006) Chile: Protección Penal a la Intimidad y los Delitos Informáticos, Edit. Jurídica de Chile.
- PÉREZ LUÑO, Antonio (2008). “Manual de informática y derecho”, Editorial Ariel S.A., Barcelona.
- SALT G. Marcos, Informática y Delito, Publicación en Internet, URL:<http://www.derecho.org.ar>

- TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Editorial Temi.
- ZABALA BAQUERIZO Jorge (2004), Delitos contra la Propiedad, Tomo 2, Editorial Edino, Guayaquil, Ecuador.
- ZANONI Leandro. Los Hackers, (2004) la nueva cara de los piratas de Fin de siglo, Revista de Informática y Derecho. De Palma, Argentina.

ANEXO A-2
**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA.
ESTUDIO DE LOS DELITOS INFORMÁTICOS EN LA PENÍNSULA DE
SANTA ELENA.**

ENCUESTA A ESTUDIANTES

OBJETIVO: Recabar información de estudiantes de los últimos semestres de la carrera de Derecho de la Universidad Estatal Península de Santa Elena, referentes a sus conocimientos en lo que respecta a delitos informáticos para implementarla en el proyecto: "ESTUDIO DEL TRATAMIENTO DE LOS DELITOS INFORMÁTICOS DENTRO DE LA PENÍNSULA DE SANTA ELENA"

Instructivo: Marque con una x (equis) la respuesta que usted crea conveniente.

1.- ¿Ha estudiado usted la reforma al Código Penal por parte de la Ley de Comercio Electrónicos, Mensajes de Datos y Firmas Electrónicas publicada en Ley No. 67? Registro Oficial. Suplemento 557 de 17 de Abril del 2002?

a) SI_____

b) NO_____

2.- ¿Conoce que procedimiento debe seguir para la persecución de un delito informático?

a) SI_____

b) NO_____

3.- ¿Considera usted que es importante aprender sobre este tema?

a) SI_____

b) NO_____

GRACIAS POR SU COLABORACIÓN

ANEXO A-3

**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA.
ESTUDIO DE LOS DELITOS INFORMÁTICOS EN LA PENÍNSULA DE
SANTA ELENA.**

ENCUESTA A DOCENTES

OBJETIVO: Recabar información de profesores de la carrera de derecho de la Universidad estatal Península de Santa Elena referentes a los conocimientos impartidos a sus estudiantes, para implementarla en el proyecto: "ESTUDIO DEL TRATAMIENTO DE LOS DELITOS INFORMÁTICOS DENTRO DE LA PENÍNSULA DE SANTA ELENA "

Instructivo: Marque con una x (equis) la respuesta que usted crea conveniente

1.- ¿Cree usted que es importante enfatizar en la enseñanza en lo referente a Delitos Informáticos a los estudiantes de la Carrera de Derecho?

a) SI_____

b) NO_____

2.- ¿Cree que es importante el tema para la preparación profesional de los estudiantes de la Carrera de Derecho?

a) SI_____

b) NO_____

3. ¿Cree necesario implementar en la malla curricular de la Carrera de Derecho de la Universidad Estatal Península de Santa Elena, un modulo que capacite a los estudiantes en Delitos Informáticos?

a) SI_____

b) NO_____

GRACIAS POR SU COLABORACIÓN

ANEXO A-4

**UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA.
ESTUDIO DE LOS DELITOS INFORMÁTICOS EN LA PENÍNSULA DE
SANTA ELENA.**

ENCUESTA A AUTORIDADES JUDICIALES.

OBJETIVO: Recabar información de autoridades judiciales referentes a los delitos informáticos para implementarla en el proyecto: "ESTUDIO DEL TRATAMIENTO DE LOS DELITOS INFORMÁTICOS DENTRO DE LA PENÍNSULA DE SANTA ELENA "

Instructivo: Marque con una x (equis) la respuesta que usted crea conveniente.

1.- ¿De las causas tramitadas en su despacho, cuantas se refieren a delitos informáticos?

a) _____%

2. ¿Considera usted que los profesionales del derecho se encuentran lo suficientemente capacitados para litigar en este tipo de causas?

a) SI_____

b) NO_____

GRACIAS POR SU COLABORACIÓN

ANEXO FOTOGRÁFICO



Fotografía 1. Socialización del Proyecto



Fotografía 2. Recolección de Información



Fotografía 3. Recolección de Información estudiantes



Fotografía 4. Recolección de estudiantes