DERECHO Y TICS

Dr. Juan José Páez Rivadeneira

cep
CORPORACIÓN
DE ESTUDIOS Y PUBLICACIONES

ONI
20150504
$28.00
Fac# 3289
3 ej

340.
Derecho
Seguridad en computadoras

UNIVERSIDAD TECNICA PARTICULAR DE LOJA
BIBLIOTECA "BENJAMIN CARRION"

Juan José Páez Rivadeneira

DERECHO Y TICS

CORPORACIÓN DE ESTUDIOS Y PUBLICACIONES
2015

CORPORACIÓN DE ESTUDIOS Y PUBLICACIONES (CEP)

DERECHO Y TICS
Juan José Páez Rivadeneira

Revisión

Departamento Jurídico Editorial - CEP

Diagramación

Departamento de Diagramación - CEP

Impresión

Talleres de la CEP

Derecho de Autor No.:	En Trámite
Depósito Legal:	En Trámite
ISBN No.:	978-9942-10-247-8: 3-feb-2015
Tiraje:	1000
Edición:	Primera

Quito - Ecuador

Todos los derechos sobre el contenido de esta obra pertenecen a la Corporación de Estudios y Publicaciones. Prohibida su reproducción total o parcial así como su incorporación a sistemas informáticos, su traducción, comunicación pública, adaptación, arreglo u otra transformación sin autorización expresa y por escrito de la Corporación.

ÍNDICE

PRIMERA PARTE

INFORMÁTICA JURÍDICA 1

I.- CONCEPTO Y CLASIFICACIÓN DE LA INFORMÁTICA JURÍDICA 1

II.- INFORMÁTICA JURÍDICA DOCUMENTAL 3

Desarrollo de la Informática Jurídica Documental 4

Elementos Estructurales de la Documentación 6

¿Cómo está organizada la información? 8

Campos en la Jurisprudencia 9

Recursos para la recuperación de la información 9

REFLEXIONES 12

III.- INFORMÁTICA JURÍDICA DE GESTIÓN 13

CONCLUSIONES 19

IV.- INFORMÁTICA JURÍDICA DECISIONAL 20

REFLEXIONES 21

V.- LENGUAJE DOCUMENTAL 22

División del Lenguaje Natural 24

Diferencias entre Lenguaje Natural y Documental 25

VI.- LOS DOCUMENTOS 27

VII.- LA INFORMÁTICA JURÍDICA E INFORMACIÓN JURÍDICA 28

Causas del desarrollo de la Informática Jurídica 28

Naturaleza de la Informática Jurídica 29

Objeto de Estudio 29

REFLEXIONES 30
Constitución de la Información Jurídica 30
Concepto de Informática Jurídica 30
Cibernética 33
Documento Jurídico 34
Características 34
Lenguaje Jurídico 34
Clases de lenguaje 34
Lenguajes Jurídicos artificiales 35

SEGUNDA PARTE
DERECHO Y NUEVAS TECNOLOGÍAS 37

COMERCIO ELECTRÓNICO 39
DOCUMENTOS ELECTRÓNICOS 42
I.- DOCUMENTOS ELECTRÓNICOS Y MENSAJES DE DATOS 42
Definición 44
II.- VALIDEZ JURÍDICA DE LOS DOCUMENTOS ELECTRÓNICOS 46
III.- ¿QUÉ ES LA FIRMA DIGITAL Y EL DOCUMENTO ELECTRÓNICO? 48
IV.- TIPOS DE DOCUMENTO ELECTRÓNICO 49
¿Para qué sirven? 49
APLICACIONES EN PARTICULAR 50
Sobre el documento Electrónico Firmado Digitalmente 51
SEGURIDAD ELECTRÓNICA 52

I.- SEGURIDAD Y CRIPTOGRAFÍA 52
Historia de la encriptación 52
ANTECEDENTES 54
Firma Convencional ("Analógica") 54
Criptografía 56
ESTRUCTURA DE UN SISTEMA SECRETO 58
SISTEMAS DE CLAVE PÚBLICA 60
VERIFICACIÓN DE AUTENTICIDAD 60
II.- TRANSMISIÓN SEGURA DE DOCUMENTACIÓN-FIRMA DIGITAL. 61
Descripción 61
Ventajas ofrecidas por la Firma Digital 62
Aspectos técnicos 63
III.- ALGORITMOS 67
Cifrado Simétrico o de Secreto Compartido 69
Métodos Asimétricos o de Clave Pública 70
RSA 71
Digital SignatureAlgorithm (DSA) 71
IV.- SEGURIDAD EN LA RED 72
¿Qué es la Criptografía con Clave Privada? 72
¿Cómo Funciona la Criptografía con Clave Privada (Simétrica)? 72
Limitaciones de la Criptografía con Clave Privada 73
Una mejor solución: Criptografía con Clave Pública 73
¿Cómo funciona la Criptografía con Clave Pública? 73
¿Cuáles son las Ventajas de Trabajar con este Sistema? 74

La Clave Pública y los Certificados 74
FIRMA ELECTRÓNICA, ENTIDADES DE CERTIFICACIÓN 76
I.- INTRODUCCIÓN 76
II.- CONCEPTO DE FIRMA 78
III.- EVOLUCIÓN 78
IV.- FIRMA DIGITAL Y FIRMA ELECTRÓNICA 78
FIRMA DIGITAL 79
V.- ¿QUÉ ES UNA FIRMA ELECTRÓNICA? 79
De las Firmas Electrónicas Certificados de Firma Electrónica 84
Validez de la Firma Electrónica 85
Obligaciones del titular de la Firma Electrónica 85
Duración y Extinción 86
Los Certificados de Firma Electrónica 86
VI.- DIFERENCIA ENTRE FIRMA ELECTRÓNICA Y FIRMA DIGITAL 87
Elementos de la Firma Digital 87
VII.- EXPLICACIÓN DEL USO DE FIRMA ELECTRÓNICA 88
ENTIDADES DE CERTIFICACIÓN Y CERTIFICADOS ELECTRÓNICOS 92
Entidades de Certificación de Información 92
Organismos de Promoción de los servicios electrónicos 94
Infracciones administrativas 94
DERECHO COMPARADO 98
GUÍA ACADÉMICA DE LA FIRMA ELECTRÓNICA 103

REAFIRMANDO LOS CONCEPTOS 103
¿Qué es la firma digital? 103
¿Cómo funciona? 103
¿Claves privadas y claves públicas? 104
¿Qué son los certificados digitales? 105
¿Qué contiene un certificado digital? 105
¿Qué valor legal tiene la firma digital? 105
CONTRATOS ELECTRÓNICOS 107
1.- Acercándonos a una conceptualización 107
2.- Hacia una clasificación 108
3.- Elementos constitutivos del Contrato Informático 109
¿QUÉ SON LOS CONTRATOS INFORMÁTICOS? 109
UNA NUEVA FORMA DE CONTRATACIÓN 110
Obligación de proporcionar la información 111
Solución de controversias 111
MARCO JURÍDICO ECUADOR 112
CLASIFICACIÓN 113
CARACTERÍSTICAS PRINCIPALES 115
LOS NUEVOS CONTRATOS INFORMÁTICOS 117
1. EDI (Electronic Data Interchange) 118
2. Shrinkwrap y Webwrap 118
3. Contrato de Servicios por Internet 119
LOS CONTRATOS MÁS INDISPENSABLES 119
INFRACCIONES ELECTRÓNICAS CÓDIGO PENAL ECUADOR 120
INTRODUCCIÓN 121

CONCEPTO DE DELITO: 122
PRINCIPALES CARACTERÍSTICAS 122
RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS EN EL ECUADOR 125
INTRODUCCIÓN 125
MARCO JURÍDICO GENERAL 126
En la constitución vigente del Ecuador 126
CONSTITUCIÓN ECUATORIANA 127
LEY DE PROPIEDAD INTELECTUAL 130
Reglamento de la Ley de Defensa del Consumidor 130
HÁBEAS DATA Y MENSAJE DE DATOS 131
Naturaleza del hábeas data 132
Autoridad Competente 134
PRINCIPIOS DE LOS MENSAJE DE DATOS 135
INFRACCIONES RELACIONADAS A LOS MENSAJES DE DATOS 138
Infracciones administrativas 138
LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS 139
Finalidad de la ley 140
Acceso a los datos públicos 141
Cuestionamientos a la nueva ley 141
Derecho de privacidad de las personas 142
Protección de datos 144

TERCERA PARTE
TÉCNICA DIGITAL FORENSE 145

FORENSE 145
CONCEPTUALIZACIÓN. 145
MODELOS Y METODOLOGÍAS PARA EL ANÁLISIS DE LA TÉCNICA DIGITAL FORENSE. 153
COBIT. 167
IEEE 730. 171
ISO 9000-3. 172
ISO 17799 181
ISO/IEC 27001. 189
ISO / IEC 27037: 2012 190
NEA No. 11 194
PRUEBA PENAL. 196
ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN. 199
CADENA DE CUSTODIA. 201
FASES DE LA CADENA DE CUSTODIA 204
RFC 3227. 213
PROCEDIMIENTO DE INVESTIGACIÓN TÉCNICA DIGITAL FORENSE. 219

CUARTA PARTE

DELITO DIGITAL (INFORMÁTICO) COIP. 233

SISTEMA ADVERSARIAL 233
EXORDIO DE LOS DELITOS INFORMÁTICOS. 240
CONCEPTO DE DELITO INFORMÁTICO. 246
Clasificación 250

Sujeto activo en el delito Informático. 252
Sujeto pasivo en el delito informático. 254
INFRACCIONES INFORMÁTICAS. 258
JURISPRUDENCIA EUROPEA 283
CONVENIOS Y TRATADOS INTERNACIONALES. 287
Convenio sobre ciberdelincuencia 290
Clasificación de delitos informáticos Naciones Unidas 291
RED 24/7. 292
Commonwealth Cybercrime Initiative. 297
Iniciativa de la Mancomunidad para la Ciberdelincuencia. 297
Proyecto de Stanford 300
División de Capacidad Institucional del Estado (ICS) 300
Departamento de Instituciones para el Desarrollo (IFD) 300
Banco Interamericano de Desarrollo (BID) 300
Comité Interamericano contra el Terrorismo (CICTE) 301
Organización de los Estados Americanos (OEA) 301
Otros documentos y limitaciones. 302
I.- MEDIOS DE PRUEBA PENAL DIGITAL. 303
Casos en que se penaliza la prueba. 313
CAUSALIDAD. 314
ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN. 315
ACTUACIONES TÉCNICAS: 316
MEDIOS DE PRUEBA PENAL DIGITAL. 330
1.- EL DOCUMENTO. 331
¿QUÉ ES EL CONTENIDO DIGITAL?. 332

REGLAS PARA LA INVESTIGACIÓN DEL CONTENIDO DIGITAL. 332
Memorias volátil y no volátil. 333
2.- EL TESTIMONIO. 338
3.- LA PERICIA. 340
EL REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL. 341
DESIGNACIÓN DE PERITOS. 343
OBLIGACIONES DE LOS PERITOS. 346
INFORME PERICIAL 348
Contenido del Informe Pericial. 348
Formato del Informe Pericial. 350
Peritajes extraordinarios. 350
RÉGIMEN DISCIPLINARIO DE LOS PERITOS. 351
Práctica peritaje digital forense. 355
CASOS. 358
1.- Radiografía a los Correos Electrónicos, ¿qué esconden?. 358
La consigna es muy clara en dos vías diferentes de actuación: 358
2.- Dirección IP, la huella digital telemática del criminal. 359
3.- Facebook y las evidencias electrónicas en delitos de injurias, calumnias y otros. 361
4.- Localización y posicionamiento por medio de llamadas telefónicas. Peritaje Informático Tecnológico. 364
5.- El tratamiento de la calidad de imágenes para procesos judiciales. 366
Con la variación del brillo y el contraste 366

MEDIOS DE PRUEBA ELECTRÓNICA. 369
NUEVO PROCEDIMIENTO PENAL.- 376
PROSPECTIVA TECNOLÓGICA 381
Cloud Computing. 384
Modelos de Implementación. 384
RECOMENDACIONES PARA LA ADOPCIÓN DEL CLOUD COMPUTING. 385
Técnica digital forense cuántica. 387
GLOSARIO FORENSE 394
ANEXOS 394
BIBLIOGRAFÍA. 394

PRIMERA PARTE
INFORMÁTICA JURÍDICA

I.- CONCEPTO Y CLASIFICACIÓN DE LA INFORMÁTICA JURÍDICA

La Informática Jurídica no es otra cosa que el procesamiento de información jurídica por medios electrónicos, no sólo en lo informático, sino en las telecomunicaciones. Es decir el uso de dispositivos de las nuevas tecnologías en la actividad jurídica.

En cambio, el Derecho Informático es la regulación, la norma jurídica que regula el uso de las nuevas tecnologías, como ejemplo podemos anotar la protección de los datos. Entonces, nos referimos a la Informática Jurídica cuando el Jurista (Jueces, Secretarios, Oficiales Mayores, Abogados en ejercicio de la profesión, etc.), utilizan las nuevas tecnologías como herramienta para procesar, automatizar, organizar, y, sistematizar información de contenido jurídico, en tres niveles o fuentes.

La primera fuente está relacionada con la creación de documentos que contienen información jurídica referente a la Legislación, Jurisprudencia o Casación, y a la Doctrina del Derecho, esta primera fuente es documental.

Este nivel se fundamenta en la creación o alimentación de bases de datos que contienen Legislación, como el caso de una base de datos de legislación (ver: www.cep.org.ec), o, en el campo de la Jurisprudencia y Casación ver: **¡Error! Referencia de hipervínculo no válida.** y, en el campo de la Doctrina jurídica, como referencia podemos ver: www.derechoecuador.com www.notariadigital.ec Esta fuente documental se la denomina Informática Jurídica Documental.

Una Segunda fuente es la que se relaciona con la gestión diaria del jurista, consiste en el desarrollo de la sistematización diaria de información, y, se la denomina INFORMÁTICA JURÍDICA DE GESTIÓN.

Se puede utilizar software de gestión jurídica como el denominado Jurissoft (Ver: www.jurissoft.es).

Por último la tercera fuente es la que está relacionada con el desarrollo de la información jurídica, en la que intervienen programas o software, que se convierten en herramientas del Jurista para la toma de decisiones, se recoge toda la información jurídica, inclusive con la aplicación de inteligencia artificial y sistemas expertos, por ejemplo se puede reconstruir todos los hechos y actos jurídicos, para la toma de decisiones, esta fuente se denomina INFORMÁTICA JURÍDICA DECISIONAL.

Académicamente también se habla de una fuente registral, que consiste en el registro de datos jurídicos, denominándose esta actividad como Informática Jurídica Registral.

La Informática Jurídica, consiste en la automatización de la información jurídica, generada por el propio Jurista, en base de tres aspectos importantes:

La Informática Jurídica Documental, que se encarga de procesar o crear documentos jurídicos o bases de datos que contengan compilación de las Leyes, Casación, Jurisprudencia, y la Doctrina del derecho.

La Informática Jurídica de Gestión, que se encarga de sistematizar la información jurídica que desarrolla el Jurista en forma diaria, es decir, se gestiona la información jurídica, como ejemplo podemos indicar que se organiza la información indizando y automatizando los procesos en carpetas, pudiendo inclusive controlar la actividad laboral de funcionarios y empleados.

La Informática Jurídica Decisional, es aquella que con la aplicación de sistemas lógicos o programas, a través del uso de la inteligencia artificial, o sistemas jurídicos expertos, sirven para la toma de decisiones del Jurista.

Previamente, antes de profundizar el estudio del procesamiento de información, es importante conocer algunos aspectos generales de la Informática.

El Hardware que en español se traduce Herramienta, está constituido por las partes físicas del Computador. El régimen jurídico de protección está relacionado con la propiedad industrial.

El software, que es el elemento lógico, es decir las aplicaciones para procesar datos, está relacionado con el régimen jurídico de los derechos de Autor, incluyéndose las bases de datos.

II.- INFORMÁTICA JURÍDICA DOCUMENTAL

El Jurista, no tiene conocimiento de programación y de sistemas de computación. Sin embargo la necesidad de procesar información jurídica le obliga a relacionarse con este tipo de conocimiento. Lo ideal es que el Jurista debe tener conocimientos básicos de informática, por ejemplo debe saber utilizar paquetes ofimáticos como procesadores de texto, hojas de cálculo, presentaciones, etc.

La aplicación de la Informática en el campo del Derecho, resulta particularmente complicada, precisamente, porque el Computador está preparado para procesar operaciones numéricas, conforme a una lógica formal, binaria, matemática.

Cuando el procesamiento de los datos Jurídicos deben ser en un principio según la lógica del lenguaje y en un segundo momento, la lógica modal o la lógica deóntica, propia del lenguaje jurídico (Sentencias, Divorcios, Expropiaciones, etc.).

La Informática Jurídica surge por el desarrollo de las bases de datos jurídicas y fue allí que se observó que la computadora no era capaz de realizar ni siquiera la más simple operación de recuperación de la información guardada, pues la imprecisión en el lenguaje jurídico daba lugar a los fenómenos que se conocen como ruido y silencio, en la recuperación de los datos.

La respuesta de los jurídicos y los informáticos, fue la de utilizar un lenguaje documental, a través de la indización de descriptores, para alimentar un tesauro, como lo vamos a ver en el tema del lenguaje documental.

Los Juristas construyen y procesan el lenguaje jurídico, basado en el léxico jurídico.

La Informática Jurídica es un campo de aplicación que surge de la lingüística de la lógica del derecho, superando su nivel experimental y afirmándose como una herramienta para el jurista.

El problema que enfrenta la Informática Jurídica, es que en la representación y procesamiento de los significativos presentes en los textos hace que se priorice el manejo de la semántica y sintaxis del lenguaje jurídico.

Ejemplo, el término Matrimonio, si no procesamos la información en base al concepto jurídico del mismo, tendremos muchas distorsiones. Sin embargo a estas dificultades la aplicación de la Informática al Derecho ha dado como posibilidad que se eliminen las contradicciones existentes en un cuerpo de ley y se dé agilidad a la administración de la justicia.

Para que el Abogado pueda hacer uso de las aplicaciones informáticas, como nuevo instrumento de trabajo, es necesario que conozca la problemática que comporta su desarrollo, sólo allí tendremos calidad y rapidez en las actividades del jurista, como resultado, la Computadora se convertirá en aliada del Jurista.

Desarrollo de la Informática Jurídica Documental

En el caso de las bases de datos con información Jurídica, para encontrar las ventajas después de conocer qué tipo de información tiene almacenada, se debe aprender las diferentes formas de consultar, recuperar y aprovechar la información, esto es: primero, debe conocer cómo está estructurada la información, segundo debe aprender a buscar

y ordenar la búsqueda de los datos y, tercero, debe saber personalizar la información recuperada.

Estos tres aspectos constituyen el objeto principal para identificar las limitaciones y las facilidades de la información existente.

TRABAJO ESTUDIANTIL: Realizar comentarios respecto a la experiencia de haber ingresado al Internet, analizar la situación informática en el lugar de trabajo, señalando lo que se tiene y las expectativas hacia el futuro.

Abrir un Correo Electrónico, crear un blog: www.blogspot.com www.wordpress.com, y estos resultados comunicar al Profesor.

La Informática Jurídica, es un campo de aplicación que surge de una gran variedad de disciplinas: La Computación, la Informática, la Lingüística, la Lógica, el Derecho, la Programación y, el Cálculo y otras que han superado el nivel de la experimentación.

Ya no es una mera experiencia, se ha convertido en una herramienta imprescindible del Jurista, pero enfrenta un principal problema que es el de la representación y el procesamiento de los significados presentes en los textos, por eso se da a la SEMÁNTICA y a la SINTAXIS del Lenguaje Jurídico, independiente de la dificultad que plantea la sistematización de los procesos jurídicos.

El lenguaje jurídico, se debe construir, los informáticos no pueden satisfacer las necesidades del Jurista, lo óptimo sería que el Jurista sea el propio Programador.

Con la aparición de la Informática se ha presentado una verdadera revolución, en la que aparece un nuevo orden y se convierte en necesidad el uso de estas Tecnologías.

El conocer y aplicar el uso de las nuevas tecnologías nos relaciona con la informática jurídica, que está en el campo de las ciencias de la

información y comunicación, relacionándose con el derecho sólo por el contenido de información jurídica.

La regulación, normativa, legislación del uso de la Informática, es un campo de estudio del Derecho Informático.

La Propiedad Intelectual, está relacionada con la informática jurídica por el régimen de protección, que puede ser en el de derechos de autor cuando implica regulación de bases de datos y software; y en el campo del régimen de propiedad industrial cuando los componentes y partes de las nuevas tecnologías de la información y comunicación están reguladas, como el caso de marcas, signos distintivos, patente, etc.

En el desarrollo de la INFORMÁTICA JURÍDICA DOCUMENTAL, el Jurista ya no sólo se conforma con tener accesorios de computación, Fax, Módem, CD ROM, sino que se aprovecha de las ventajas que ofrecen estas herramientas en su actividad laboral.

Se convierten en herramientas esenciales para almacenar grandes cantidades de información.

En el caso de las bases de datos o bancos de datos con información jurídica, para encontrar las ventajas y aprovechar el tipo de información, que tiene almacenada, el Jurista debe aprender diferentes formas de consultar, recuperar y, aprovechar los datos jurídicos. Este aprendizaje se reduce a tres aspectos:

Debe conocer como está estructurada la información.
Debe saber buscar u ordenar la búsqueda del dato y,
Debe saber personalizar la información de contenido jurídico.

Elementos Estructurales de la Documentación

Como hemos analizado la informática jurídica, tiene tres niveles o fuentes: DOCUMENTAL, DE GESTIÓN, DE DECISIÓN.

En la Informática Jurídica documental, tenemos bases de datos, que provienen de la Legislación, de la Casación y Jurisprudencia y de la Doctrina.

En el caso de bases de datos de Legislación y de Jurisprudencia tenemos la siguiente estructura: Palabras, Temas, Índice de Contenidos, Conceptos o Descriptores.

El Elemento Estructural para organizar, procesar, automatizar y guardar la información se denomina INDIZACIÓN, por medio de la cual se ordenan los componentes descriptores de la "A" a la "Z", a través de este sistema organizamos un listado de palabra o caracteres que se registran en la base de datos.

Cuando lo hacemos con PALABRAS, registramos todas las palabras o caracteres en la base de datos. Por ejemplo, si el tema es Legislación tendremos todas las Leyes en palabras, así, si ponemos la palabra Ley de Aguas, dependerá del tipo de indización utilizado, que nos puede llevar al contenido de toda la ley, o la información de normativa histórica del descriptor.

Cuando estamos indizando por TEMAS, nos referiremos al listado de los conceptos mencionados independientemente de la secuencia de las palabras o caracteres con lo que hayan sido registrados en la base de datos. Ejemplo: Matrimonio, al respecto de este tema nos hará referencia al Art. Respectivo del Código Civil, pero independientemente de las palabras o de los caracteres.

En los temas, los CONCEPTOS son el contenido de la Información.

Por último los CONTENIDOS, se consideran listados de tópicos en los que se encuentran clasificados la información en base de datos, en el campo de Legislación, por Ejemplo: Derecho Civil, Derecho Penal, Derecho Tributario, etc.

Cuando nos referimos al listado de tópicos, nos referimos al concepto del tópico y los descriptores.

¿Cómo está organizada la información?

En las bases de datos en lo relativo al NOMBRE, tenemos SUB DIVISIONES, cuando se identifican las palabras en las que se encuentra clasificada la información almacenada.

Puede utilizarse la NUMERACIÓN de los artículos, en el que se encuentra la Ley o el Número que identifica por ejemplo a los Registros Oficiales.

Otra técnica es la de utilizar el TEXTO de los artículos en cuanto a unidad documental, en la que se registra la información, por ejemplo: En el texto relacionado a Estafa, se recuperará el contenido de los artículos correspondientes al código penal que contiene esta información.

Se puede con el recurso del texto "Estafa", acceder a la información deseada.

También se estructura por COMENTARIOS, a través de notas u observaciones al margen del texto de la Ley que el Usuario quiere revisar, por ejemplo: Por materias.

Por el HISTORIAL, debido a que se actualiza las reformas a las Leyes, cada artículo sufre cambios, hay que considerar por ejemplo, las Resoluciones de Corte Constitucional, que pueden suspender la vigencia de algún artículo de Ley.

Por la época fuente y el año de emisión de las leyes, en este caso están los Registros Oficiales.

En el Campo de la Legislación también podemos registrar efectos de la Ley por Concordancias, inclusive nos puede llevar a información de Derecho Comparado.

Campos en la Jurisprudencia

POR SALAS, ordenamiento de la Corte para circunscribir la búsqueda en la función de la materia.

NOMBRES POR TRIBUNALES, para ubicar al Tribunal que ha emitido la información, cuando la tesis no se ha pronunciado por alguna de las Salas de la Corte.

TÍTULO, dentro del Ordenamiento de la Tesis cuando el órgano emisor describe el concepto Jurídico, que siempre habrá de consultar el Derecho de la Casación.

POR EL CUERPO DE LA TESIS, por el cual se examina el problema jurídico y se observan o se dan los argumentos.

POR LOS PRECEDENTES, razones Jurídicas por el cual el órgano emisor expone sus argumentos.

POR CONTRADICCIÓN, tesis en el que el órgano emisor emitió sus argumentos en sentido contrario.

Una vez que se conoce como está organizada la información, se puede saber dónde la podemos buscar, es importante que el Jurista sepa manejar los recursos de la recuperación necesarios para que el sistema localice la información.

Recursos para la recuperación de la información

Los Recursos de Recuperación, son la parte modular del Software o Programa de las bases de datos, ya que sólo es posible localizar los datos Jurídicos con cierto grado de precisión, cuando se emplean dichos recursos. Su valor no es preciso, porque se trata de datos lingüísticos, no matemáticos.

El lenguaje Jurídico, es difícil de hacerlo preciso ante la tecnología, pero son recursos necesarios para recuperar la información.

El Jurista debe aprender a ordenar a la base de datos para la búsqueda de la información mediante los siguientes Recursos de Recuperación:

Por palabras simples.- Para localizar las secuencias ininterrumpidas de caracteres o palabras previamente seleccionadas para identificar con signos de puntuación y comandos.

Descriptores.- Para localizar los documentos previamente señalados como recuperables.

Por frases.- Para localizar las secuencias de palabras señaladas como pertenecientes a una frase, Ejemplo: Despido Intempestivo, refleja toda la información que contenga la frase.

La parte más difícil de los recursos de la recuperación, para el Jurista es:

Enmascaramiento.- Cuando se desconocen los caracteres.

Del prefijo.- De la raíz del Prefijo, por existir la posibilidad de diferentes raíces y la misma terminación Ejemplo: Legal e Ilegal, ambos tienen diferentes raíces pero la misma terminación.

Enmascaramiento.- Cuando se desconocen o existe la DEL INFIJO posibilidad de que hayan sido alterados los caracteres intermedios infijos de la palabra Ejemplo: Médico o Medico con o sin tilde.

Enmascaramiento.- Cuando se inicia con la misma raíz DEL SUBFIJO independientemente de la terminación que haya sido registrada en torno a los verbos Ejemplo: la sustantivación, adjetivación y configuración de los verbos: juega, jugamos.

Existe también el Recurso de Recuperación por EL TIPO DE CARACTERES.

Para buscar aquellas palabras que adquieren un significado diferente a la causa de estar escritos los caracteres Minúsculas y Mayúsculas.

Otro Recurso de Recuperación es el de POR EL CAMPO DE BÚSQUEDA.

Para buscar aquellas palabras que adquieren un significado diferente a causa de estar escritos, en determinado campo de la información.

Otro Recurso de Recuperación es POR EL REGISTRO DE BÚSQUEDA.

Para buscar aquellas palabras que adquieren un significado diferente a causa de estar escritos en un grupo o nivel de información, los recursos utilizados son:

AND
OR
XOR
AND-NOT
NOT
ADJ.- Para recuperar sólo los adjetivos
NEAR.- Cuando las palabras para su recuperación se les anteponen con este recurso y no importa cuál esté primero o después, siempre se va a recuperar.
WITH.- Cuando la búsqueda no de palabras, sino de oraciones o textos, se antepone este vocablo.
SAME.- Para restringir la búsqueda, se recupera la información más restringida.

Otros recursos de recuperación son:

LOS SINÓNIMOS.- Búsqueda de palabras con diferentes formas y significados.

LOS HOMÓNIMOS.- Cuando las palabras tienen la misma forma pero diferentes significados.

LOS IMPLÍCITOS Conceptos implícitos en el Texto.

Las estructuras de organizar la documentación doctrinal, son mixtas.

REFLEXIONES

Las bases de datos son solamente textos. Siempre la base de datos requerirá del lenguaje documental jurídico, no del sistema binario matemático de cálculo.

La Informática Jurídica Documental está en pleno desarrollo, por lo que se construye base de datos de Legislación, Jurisprudencia o Mixtas.

Las bases de datos pueden ocupar mucho espacio y ser lentas en su recuperación.

No existen todavía reguladores informáticos para depurar la información, es difícil depurar la información de texto.

El desarrollo de las bases de datos de Legislación y Jurisprudencia, lo han elaborado los Informáticos y no los juristas, hay diferencia.

El Jurista debe permanentemente procesar información que contribuya a la creación del lenguaje jurídico para aplicarlo en la base de datos.

La Informática Jurídica Documental, alimenta y crea bases de datos con contenidos jurídicos.

La Informática Jurídica Documental es una herramienta de uso del jurista para procesar, sistematizar información, por lo que se desarrolla con la Ciencia de la información, no con el Derecho, pues contribuye solamente como una herramienta para el Jurista.

La Informática Jurídica Documental debe ser elaborada por el Jurista en lo que respecta al desarrollo de los datos y por los informáticos en lo que respecta al procedimiento lógico de los datos.

Cada persona en forma individual aporta al desarrollo de la base de datos desde su lugar de trabajo.

Es importante adaptarse a la computación, ya que en ella está la riqueza del Conocimiento. La tecnología nos permite acumular conocimientos, tener, bases de datos a servicio de la comunidad.

Hay que aprovechar los recursos para tener nuestra propia base de datos. Tenemos los ciudadanos que tener derecho al acceso a la tecnología, creemos que sí, la transferencia de la tecnología debe darse.

Las Herramientas no podemos construirlas, pero es factible y hay potencial para desarrollar los Programas.

III.- INFORMÁTICA JURÍDICA DE GESTIÓN

TRABAJO ESTUDIANTIL.-En el Restaurante "mamá Miche", existen tres meseros, dos cocineros, una cajera y una persona que administra el local. Tiene al día un flujo de 60 a 70 clientes, al igual que tiene horas en el que el trabajo se intensifica. El Restaurante necesita procesar información, ¿cómo la utilizaría? ¿El Restaurante tiene una computadora donde la ubicaría? ¿Cómo sugiere usted se sistematice la información? ¿Cómo se controlarían lo sueldos y más aportaciones de Ley? Hacer una reflexión de cómo es importante que se automatice el local, para controlar la información.

La Informática Jurídica de Gestión, se refiere a la actividad que el Jurista desarrolla en el día a día, a través de escritos, providencias, sentencias, control de procesos, rol de pagos de la oficina, cálculos de intereses, aspectos tributarios, cobro de honorarios, en fin, toda la gestión diaria.

Esta Informática Jurídica de Gestión, se la denomina también como OFIMÁTICA o también se la conoce como BUROCRÁTICA.

En el ejemplo realizado acerca del Restaurante "Mama Miche", podemos señalar que los meseros toman el pedido del cliente y se lo trasladan a los cocineros, los mismos que cumplen con las órdenes de los meseros, el Restaurante a su vez tiene facturas para el control de las ventas.

La información que se maneja en el Restaurante está relacionada con el Sistema de Gestión.

En una Oficina Jurídica o en una Judicatura, se aplica el Sistema de Gestión para:

Establecer la función que tiene el Sistema dentro de la Estructura (Establecimiento, Oficina, Ministerio, etc.).

Qué tipo de información manejan individualmente las personas. En el caso de una Judicatura, de acuerdo a los artículos 273 al 276, del Código de Procedimiento Civil, al Juez le corresponde dictar Sentencias, Autos y Decretos o Providencias, en base a ello, el Juez determinará funciones para el Oficial Mayor, los Ayudantes Judiciales, el Secretario y el Mensajero.

Qué Sistema de información específico se proponen desarrollar en una Judicatura.

En la actualidad en la Función Judicial, podemos decir que no existe un sistema informático racional, para establecer el rol que ocupan los funcionarios y empleados, en cada una de las Judicaturas.

En el caso de una Notaria, por Ley le corresponde Protocolizar, Autentificar y Certificar, en base a estas responsabilidades, el Notario deberá determinar tareas para que cumplan el Secretario, los Ayudantes o Amanuenses, desarrollar o pasar las correspondientes Matrices, por lo tanto se deberá establecer un Sistema de Información, en base a las funciones que desarrollan cada uno de los empleados, para efectuar una debida supervisión y control en cada uno de ellos que se responsabilicen de las tareas establecidas.

La riqueza de la información nace del aporte diario de cada una de las personas, desde su lugar o sitio de trabajo.

En una Oficina Jurídica que está integrada por el Abogado, empleados, Contador Financiero, Recepcionista, Mensajero, etc., se debe

determinar qué tipo de información realizan cada uno de ellos, así podemos señalar que los empleados llevan el control de procesos, tramitan la documentación, el Abogado supervisa y legaliza todos los escritos y el seguimiento de las causas, el Contador lleva la contabilidad para determinar los ingresos y gastos de la oficina, liquidar honorarios y sueldos y salarios, transferir lo que le corresponde al Fisco etc., la Recepcionista se encarga del archivo y el Mensajero en la entrega de la documentación en las distintas judicaturas y trae correspondencia de los Casilleros Judiciales.

El Sistema de Información se desarrolla en base a las tareas que les corresponde realizar a cada persona, por lo tanto es necesario:

Contar con un ORGANIGRAMA FUNCIONAL, en el que se determine claramente las funciones de todo el personal, las responsabilidades de cada una de las personas que forman parte de la Estructura de la dependencia.

Es necesario establecer NIVELES DE ORGANIZACIÓN, para procesar información.

La Actividad de Sistematizar la Información, corresponde a los Juristas, mientras que el desarrollo de los Programas, es un tema de los Informáticos.

A los Programas se los llama Software, para alimentar los mismos, el Jurista tendrá que ayudar a construir el lenguaje jurídico u organizar la información para establecer un sistema de información.

En una Oficina Jurídica la Sistematización sirve para saber cómo encauzar mejor los procesos judiciales, determinar fechas, presentar alegatos, controlar el juicio, etc.

La Tecnología está al alcance de todos, se convierte en una necesidad para procesar la información.

Los Niveles de Organización, dependen de lo que cada uno quiera.

El Volumen de Información, puede dificultar el trabajo, tiene que tomar y seleccionar la información necesaria, lo lógico es tener información actualizada vigente.

La Informática Jurídica de Gestión tiene la característica de organizarla hoy para el futuro, el material valioso es el que tiene que ser procesado diariamente y ser actualizado, el documento "viejo" pero necesario deber ser guardado, para que esté al alcance, cuando sea necesaria su recuperación.

Luego de establecer el ORGANIGRAMA FUNCIONAL, así como determinar los NIVELES DE INFORMACIÓN, es necesario:

IDENTIFICAR el Sistema de Información. Si estamos en una Judicatura, se identifica la función de cada uno y así el Juez por Red, puede ordenar el trabajo y a su vez controlar el mismo a los empleados dependientes de la Judicatura.

El proceso de sistematizar la información debe ser controlado a través de la tecnología, el actual sistema judicial no funciona correctamente.

Sin embargo cabe rescatar que se está implementando procesos electrónicos en la administración de justicia, como casilleros virtuales, firma electrónica, notificación electrónica, por el impulso de la ley de comercio electrónico aprobada en el 2002, de la que haremos un profundo análisis en capítulos siguientes.

Un proceso o juicio, puede demorar porque no se ejerce ninguna presión para que sea despachado, por no tener algún Abogado que se interese por su solución. Cabe indicar que, no existe un control válido de las diferentes causas. Pero con el sistema adversarial vigente, la oralidad permitirá el uso de nuevas tecnologías en la función judicial.

Podemos estar seguros que la Justicia mejorará, al implantar un sistema de información técnico, estructurado de acuerdo a sus reales necesidades.

La Información Jurídica, necesita por una parte de un Hardware o computador y de los Programas o Software Jurídicos. El Derecho Informático, no hace otra cosa que regular el uso correcto de los Programas, que se encuentran Registrados como Propiedad Intelectual.

El Software es el sistema lógico que posibilita el funcionamiento de la computadora. El Software se regula bajo el Régimen de la Propiedad Intelectual, pero hay una gran corriente que no participa totalmente de esta relación, ya que argumentan que el Software sin la computadora, no podrían utilizarse, por lo tanto deben estar establecidos por un Régimen especial, ya que el Software es desarrollo de la tecnología pero necesita de intelecto.

El Software pirateado se sanciona con el decomiso y además multa y hasta tres años de prisión.

Para el desarrollo de los sistemas informáticos de gestión, constan de cinco etapas principales:

a) Diseño del sistema.
b) Programación
c) Cargado y Pruebas
d) Implantación
e) Actualización y mantenimiento.

En la primera etapa interviene el jurista, para identificar dos elementos importantes, en el primero, qué se hace, durante el procedimiento que se quiere automatizar, cuando se hace, poruqe se hace, donde se hace, como se hace y quien lo hace. En el segundo, qué debe hacerse, cuando, porque, donde, como y por quien, al final se elabora el plan de ruta a seguir o el denominado diagrama de flujo.

Las siguientes etapas son netamente técnicas y corresponde a los programadores.

En el país se desarrollan verdaderos programas o software de exportación. Existen varias empresas que han elaborado programas

específicos como el administrado por el Servicio de Rentas Internas (SRI), que está dando óptimos resultados. El software es el acercamiento lógico que permite que la computadora automatice información. Se procesa la información con los Programas existentes.

CASO PRÁCTICO: Una Ferretería tiene una base de datos con toda la información de los stocks que posee, dispone de la documentación o catálogos de los materiales que expende. Reflexión el día viernes en la tarde la Secretaria no alcanza a procesar toda la información y se lleva a su casa el trabajo, copiando la información existente en un disquete, llega el lunes y la Secretaria copia todo el trabajo realizado por la computadora y actualiza la información. En resumen copia la información en disquete, lo lleva a su casa, actualiza los datos, regresa a la oficina y con su disquete traslada la información a la computadora de la oficina.

La computadora luego de horas, empieza a tener problemas, porque el Sistema Operativo no carga, es decir el disco duro, está dañado, incluyendo la información del stock, y es por lo tanto imposible recuperar la información. Se pierde tiempo, dinero y sobretodo no ha respaldado la información. Lo que sucedió es que la computadora de la Secretaria tenía virus y contagió a la computadora de la empresa. El responsable de la Ferretería, nunca conversó con la Secretaria acerca de sus responsabilidades que tienen que tener acerca de la información.

Reflexión: ¿Qué tipo de información se maneja? ¿Es función de la Secretaria llevarse la información a su casa? ¿Se debe tener niveles de información? ¿Tenemos que inventariar e identificar la información?

El impase ocurrido en la Ferretería, se lo podía solucionar de antemano, con políticas de seguridad para garantizar y controlar el acceso de la información.

La Secretaria, por más buena voluntad no debía llevar el trabajo a casa, razón por la cual merecerá ser sancionada, averiguando si existió afán de perjudicar a la Empresa, si existió o no dolo. Lo aconsejable es que

existan niveles de información para responsabilizar funciones a cada uno de los empleados.

Debe existir en caso de necesidad restricción de la información, debemos valorar la información que está almacenada en la computadora.

En nuestra actividad diaria, debemos meditar acerca de cómo evitar riesgos a la información que se pueden presentar. Para procesar la información, siempre se debe contar, con respaldos, con archivos. Es conveniente mantener programas originales con licencia a fin de evitar problemas legales y además evitar su contaminación.

CONCLUSIONES

La Informática Jurídica de Gestión se refiere a la actividad diaria del Jurista.

La Informática Jurídica de Gestión no es otra cosa que procesar la información relacionada con la actividad jurídica, esta información puede ser: escritos, pedidos, roles de pagos, etc.

El Jurista debe archivar o guardar la información que maneja cada persona.

El Jurista debe saber qué tipo de sistema de información maneja cada persona.

El Jurista debe proponer como solución un sistema de información.

En la Informática Jurídica de Gestión, requiere que el Jurista tenga conocimientos de Programas de Computación.

La Informática Jurídica de Gestión, es la automatización de la actividad jurídica en el lugar de trabajo, las bases de datos compilan información de leyes, jurisprudencia, casación y doctrina.

IV.- INFORMÁTICA JURÍDICA DECISIONAL

Tiene que ver con el procedimiento en la toma de decisiones del Jurista. Este tipo de Informática se ha extendido hacia la Administración de Justicia.

La Informática Jurídica Decisional, consiste en la integración de procedimientos dirigidos a sustituir o reproducir las actividades del Jurista. A proporcionarle dictámenes, decisiones y, a ofrecerle soluciones de problemas y no sólo documentación e información. Facilita solución a los problemas del Juez, Notario, Abogado, etc.

En este tipo de informática jurídica interviene la INTELIGENCIA ARTIFICIAL, que alude al conjunto de actividades informáticas que fueron realizadas por el hombre, considerándose estos aspectos técnicos como producto de su inteligencia.

La Inteligencia Artificial abarca:

La comprensión del lenguaje natural, el reconocimiento de las imágenes y sonidos.

La realidad virtual.

Las simulaciones, es importante para el Juez la reconstrucción de los hechos se puede fácilmente reconstruir un homicidio.

Sin embargo hay que reflexionar que la inteligencia y el poder sobre las máquinas, seguirá siendo del ser humano. Es imposible que la computadora desplace a la persona, nunca será autónoma. La inteligencia artificial, siempre estará bajo control del intelecto humano.

En cuanto a los SISTEMAS EXPERTOS, su desarrollo consiste en incorporar en forma práctica y operativa el conocimiento de un experto en la materia que se trate o se estudie.

Estos son los Programas que reproducen las actividades del EXPERTO que ha previsto y diseñado. Siempre se va a depender de los Informáticos y estos de los Juristas que tienen importancia ya que son los que crean el Lenguaje Jurídico.

Los SISTEMAS EXPERTOS están dirigidos o diseñados para resolver casos jurídicos complicados, como por ejemplo en el Sistema Tributario, el determinar liquidaciones por impuestos. En el Sistema Laboral a través de simulaciones se puede determinar lo que un empleado deberá recibir como indemnización, de acuerdo con la Ley.

Existe el SISTEMA EXPERTO DE PREVENCIÓN de las consecuencias de los impactos del medio ambiente.

Por último tenemos que señalar que hay Sistemas Expertos sobre las condiciones de nacionalidad y Derecho de Familia.

REFLEXIONES

Las máquinas procesan información y establecen datos lógicos, pero no pueden comprender la multiplicidad de circunstancias que concurren en la conducta humana. Sólo el ser humano posee conducta que se relaciona con la moral o la ética. Las leyes contienen normas de regulación. La máquina está al alcance del hombre, le debe obediencia a la conducta humana.

No es posible ni deseable una suplantación plena de razonamiento jurídico, del Juez o del Jurista por el cálculo informático del computador.

Nos preguntamos, si el Internet debe o no ser regulado. La encriptación en Internet, significa que las empresas dan la debida seguridad a la información.

Con el mal uso de la tecnología aparecen los delitos informáticos, campo de estudio por parte del derecho informático.

La tecnología como herramienta del Jurista es posible en tres aspectos:

a) Aspecto rutinario de su uso;
b) Estandarizar el uso y,
c) Sólo operaciones para dar soluciones operativas

El Juez y el Abogado no pueden adjudicar de responsabilidad de sus decisiones o dictámenes al computador. Jamás pueden trasladar responsabilidades propias a la máquina.

El Jurista debe procesar información con el verdadero conocimiento de los componentes de las nuevas tecnologías de la información y la comunicación.

(Ver Anexo 1)

V.- LENGUAJE DOCUMENTAL

La computadora funciona con un Sistema Operativo, cuyo contenido es en base a un Lenguaje Jurídico determinado. El problema está en que el Lenguaje Jurídico es especializado, tiene su propia semántica, la pregunta que nos hacemos es como construir el lenguaje jurídico si el sistema de computadora es binario, más aún cuando existen más de 240.000 normas legales.

En este capítulo estudiaremos:

Lenguaje Natural

Indización

Lenguaje Jurídico Documental

Tesauro

Lenguaje es la manifestación hablada o escrita de la lengua, nos expresamos a través de palabras o grafismos, es una forma de comunicación humana, que se diferencia de las otras formas de expresión que las personas han establecido, por ejemplo señales de humo o las señas a través de banderas.

El lenguaje es universal, por lo tanto es natural y se lo asimila en forma particular a cada ser humano, por la cultura, condición social o nivel intelectual, inclusive otro idioma puede ser traducido, por lo tanto el lenguaje es universal ya que todo es traducible.

En relación con la Tecnología no nos podemos dar el lujo de ingresar y descifrar todo lo que en el lenguaje natural existe. Debiendo señalar que la cantidad que representa no tiene límite.

Con la máquina hay que crear un lenguaje documental que pueda ser descifrado por la misma, de manera correcta.

La computadora es un instrumento creado con el objeto de traducir la información contenida en los documentos, haciéndola accesible y recuperable por distintas personas, sea cual fuere su modo de hablar o escribir. Las órdenes que damos a la Computadora es a través del Lenguaje Jurídico.

En el Aspecto Jurídico, es difícil el manejo del lenguaje documental. La Semántica Jurídica es complicada las palabras jurídicas se vuelven difíciles para crear descriptores (concepto de la palabra).

El lenguaje natural, es aquel conjunto de palabras, signos, símbolos orales o escritos por medio de los cuales el ser humano se comunica entre sí, transmite datos de la voz, imagen y sonido. Cuando en internet se transmite la voz, estamos en el campo de las telecomunicaciones.

Sobre la indización, cabe señalar que es indispensable crear un directorio principal, para luego organizar la información en carpetas y subcarpetas, relacionando a los temas que se selecciones, por ejemplo: trataremos de indizar la Constitución Política de la República, desde la "A" a la "Z".

En la A señalamos ÁMBITO y ponemos el Artículo que sobre el particular dice la Norma suprema. Luego pasamos a buscar Descriptores o Palabras, con el resto de letras B, C, en D, por ejemplo

DERECHOS CIVILES en la D, la palabra HÁBEAS DATA den la H, así sucesivamente hasta llegar a la letra Z.

TRABAJO ESTUDIANTIL: Escoger cualquier Tema e indizarlo.

Organizando un Directorio principal, con temas y subtemas, relacionando el contenido de la in formación por su objeto o su concepto, para que el descriptor refleje los datos indizados.

División del Lenguaje Natural

Existe en el Lenguaje Estructural Gramaticales el Lenguaje Natural, en su división más concreta, tiene las siguientes partes en la Estructuración Gramatical, para poder interpretar, escoger, y cambiar la información.

MONEMAS, que tiene una raíz que es el LEXEMA

SINTAGMAS, varias palabras o monemas y,

MORFEMAS, la terminación de las palabras.

Los MONEMAS, son palabras o signos que nos da a entender el idioma y tiene dos conceptos por el SIGNIFICADO y por EL SIGNIFICANTE de las palabras.

Por el SIGNIFICANTE, cuando la imagen, la acústica, o la gráfica está asociada a un concepto, mientras que POR EL SIGNIFICADO, cuando el concepto está asociado a una imagen.

EL LEXEMA, es la unidad mínima significativa del MONEMA.
Ejemplo: EL MONEMA ÁRBOL, el concepto está asociado a la imagen, si relacionamos el descriptor PENSAMIENTO, estamos asociando el concepto a la imagen.

EL SINTAGMA, es el elemento conceptual, formado por varias palabras o Monemas.

EL MORFEMA, es la terminación de las palabras
MONEMA - LEXEMA - MORFEMA

Aval (ar) Avalar

EL MONEMA Juicio - SINGTAMA, Enjuiciamiento.

Los descriptores, sirven para construir el Lenguaje Técnico Jurídico, Ejemplo si indizamos a través de descriptores, pueden adquirir un mismo término o palabra, diferentes conceptos lo que puede causar una confusión en el léxico jurídico, por ejemplo el descriptor DETENCIÓN de persona, en el sentido jurídico no puede referirse a la persona ya que estaríamos en el caso de APREHENSIÓN, ya que la primera se refiere a la detención del vehículo, y el otro descriptor a la persona.

Otro de los problemas con los descriptores es el uso de PREFIJOS y SUBFIJOS.

Cuando se asocian las palabras de acuerdo al significado profesional, también hay problemas, ya que existen en este plano especializaciones o títulos diferentes.

Diferencias entre Lenguaje Natural y Documental

EL LENGUAJE NATURAL es de origen antropológico, mientras que el DOCUMENTAL es un resultado de un Sistema Procesado.

EL LENGUAJE NATURAL, tiene influencia Sico-Social, el DOCUMENTAL, se reduce a la mínima expresión, es SENCILLO Y ESTRUCTURAL.

El LENGUAJE NATURAL, es una forma de comunicación ORAL, ESCRITA, o por SEÑALES o por CÓDIGOS, por lo tanto la comunicación es muy amplia. Utiliza bastante espacio, utiliza variedad de términos.

En cambio el DOCUMENTAL, es resultado de la APLICACIÓN DE LA TECNOLOGÍA, ocupa menos espacio, simplifica el lenguaje natural a través de los descriptores, en el que utiliza una parte de las palabras o términos.

Los descriptores funcionan a través de Códigos binarios, depende del tipo de lenguaje de programación utilizado.

La INDIZACIÓN es el proceso de extraer los términos o las palabras a través de los descriptores, que muestran el contenido del documento.

Una cosa es elaborar Software para alimentar bases de datos. Con la Informática Jurídica podemos crear bases de datos manuales, desde donde estemos trabajando, organizando, sistematizando la información que está a nuestro alrededor. Se puede desarrollar diferentes y variadas bases de datos, por ejemplo la de Modelos de Demanda en este caso se obtiene el modelo que de acuerdo a la necesidad que se tenga o se requiera según el caso, así puede ser una demanda laboral, civil, penal, etc.

Hay que señalar que los programas o Software ya existen, son parte del componente de la informática y de esta manera los aprovechamos para organizar y procesar información.

Con el trabajo individual y el uso de nuevas tecnologías podemos elaborar una base de datos.

La indización es el proceso de extraer el contenido de la información a través de los descriptores, que alimentan el Tesauro.

TESAURO es un conjunto de descriptores (palabras, términos y conceptos tomados del lenguaje natural), provistos de sus relaciones semánticas, para graficar podemos asimilar a una Enciclopedia.

El Tesauro tiene tres aspectos importantes:

- Un concepto elegido que son los descriptores

- Los términos del Lenguaje Natural que han sido trasladados a los descriptores; y,

- Las relaciones Semánticas

El Tesauro se divide POR LA FINALIDAD, cuando constituye una herramienta de control termino lógico y POR SU CONSTRUCCIÓN, cuando constituye un listado de términos que guardan relación semántica entre sí.

(Ver Anexo 2)

VI.- LOS DOCUMENTOS

Me refiero al tipo de documento que creamos y que está relacionado al contenido y se dividen en: Legal, Jurisprudencial; y, doctrinal.

Si es verdad que trabajamos con documentos electrónicos, la referencia es en el campo de la informática jurídica, posteriormente en el campo del derecho informático profundizaremos su estudio.

EL DOCUMENTO LEGAL, tiene dos aspectos importantes, en primer lugar es un documento que hace análisis de la información a través de un procedimiento de cuatro fases:

- Documento Anfitrión

- Documento Jurídico

- Unidad Informática propiamente dicha y,

- Texto

El segundo aspecto, se refiere a:
Bases de datos Generales y, Bases de datos Especiales

Documento Jurisprudencial

Tiene tres aspectos importantes:

- Unidad de base de datos puede ser general o especial

- Elaboración del Extracto (Todo juicio tiene su extracto) y,

- Asignación de descriptores al documento

Documento Doctrinal

Tiene tres situaciones importantes:

- Bases de datos y descriptores asignados

- Tipos de documentos especializados, pueden ser argumentativos, expositivos y socio-jurídicos y,

- Asignación de descriptores en el documento doctrinal

Con la base de datos, asignamos descriptores por cada documento doctrinal y al documento especial le asignamos descriptores para guardar la información. Cabe señalar que bases de datos doctrinales, existen muy pocas.

VII.- LA INFORMÁTICA JURÍDICA E INFORMACIÓN JURÍDICA

Se presenta la gran interrogante ¿el Jurista se aprovecha de la Tecnología para desarrollar la Informática Jurídica?

Causas del desarrollo de la Informática Jurídica

Los principios fundamentales para llamarle Informática Jurídica, es que hay autonomía con sus propias reglas y principios.

La Informática Jurídica se ha desarrollado porque: Existe un impacto de las ciencias de la Información sobre el Derecho, para almacenar y recuperar información.

La complejidad del Ordenamiento Jurídico, obliga al Jurista a estar actualizado.

La computación ha permitido la velocidad de cálculo y capacidad de almacenamiento de los datos jurídicos.

En derecho todo sirve, se tiene acceso inclusive a lo que está derogado, siempre existirá una referencia, más aún si se tiene concordancias y relaciones con las Leyes, con la Casación, con la Jurisprudencia y Doctrina.

Naturaleza de la Informática Jurídica

La Informática Jurídica, no es una rama del Derecho, porque únicamente procesa información jurídica, que no genera derecho porque no tiene causa ni efecto que fundamenta una Ley.

La Informática Jurídica es un aspecto de la Ciencia de Información, a través de esta ciencia, se introduce al contenido jurídico.

La Informática Jurídica es una rama autónoma individualmente estudiada dentro de las Ciencias de la Información. El Derecho regula a través de las leyes, para que exista normatividad en cuanto a los deberes y derechos, entonces hablamos de Derecho Informático.

Objeto de Estudio

La Informática Jurídica, tiene su ámbito de aplicación en el Derecho

La Informática Jurídica, se convierte en una herramienta técnica del Jurista

Se requiere tener conocimiento jurídico, ya que la Computación, nos da información que no es jurídica.

REFLEXIONES

La Informática Jurídica cuando analiza la norma jurídica desde la aplicación de la Tecnología queda fuera del ámbito del Derecho y se convierte en otra Ciencia Independiente, que el Derecho lo utiliza o se beneficia como objeto de análisis.

La Informática Jurídica es la posibilidad que nos da la Tecnología de usar la computadora en su máxima expresión y poder bajar información, hacer cuadros, etc.

Constitución de la Información Jurídica

La Compilación de la información jurídica por medios electrónicos con la intervención del Jurista y cuando el objeto de análisis es de índole jurídico centra su objeto en tres asuntos fundamentales:

- Tratamiento de la información

- Utilización de mecanismos automáticos; e,

- Información de carácter jurídico

Entre los autores de la Informática Jurídica podemos citar al español LOZANO, al mexicano MUÑOZ, al argentino ATMARK y, al chileno SAQUEL.

El papel de la Informática Jurídica en el Derecho es una herramienta de uso de su diaria profesión o tareas.

Concepto de Informática Jurídica

Entonces informática Jurídica es la posibilidad de utilizar todo el potencial del computador en auxilio de la recuperación de la información jurídica.

Constituye informática Jurídica la compilación de información jurídica por medios electrónicos con la intervención del jurista, y cuando

el objeto de análisis es de índole jurídica y centra su objeto en tres aspectos fundamentales:

- Tratamiento de la información

- Utilización de mecanismos automáticos

- Información de carácter jurídico.

LOSANO

"Informática jurídica consiste en aquellas técnicas informáticas generales que se han revelado como particularmente adecuados para el tratamiento electrónico de datos jurídicos".

HAYNA, LAGREZA Y MUÑOZ

"Consiste en los posibles aplicaciones de la informática en el ejercicio del derecho tanto en sus aspectos legislativos, como judiciales y profesionales".

ATMARK

"La informática Jurídica como aplicación concreta de la informática al derecho, comprende los sistemas de audio y documentación jurídica, de asistencia en las tareas administrativas de apoyo a las actividades jurídicas y la construcción de modelos para la comprensión del sistema jurídico".

LÓPEZ

"La técnica de utilización del ordenador electrónico para permitir memorizar la documentación jurídica y su recuperación, seleccionada por asuntos".

MARIO SAQUEL.

"Disciplina que se ocupa del almacenamiento y recuperación del dato jurídico, por medios computacionales".

Papel de la informática en el campo del Derecho.

La nueva reforma legal integral, fortalece el sistema de juicios orales, y el sistema adversarial en Ecuador. Los procesos son rápidos y eficientes que los juicios tradicionales, porque las pruebas ya no son dadas por documentos e informes periciales en papel. Ahora, en los juicios orales las pruebas se evacuan en Audiencia de manera oral, es decir, que todo el proceso se da directamente en los juzgados.

Para comprobar lo que se realiza en los procesos, se llevan a cabo grabaciones de videos, en los cuales queda documentado el juicio desde el inicio hasta el fin, por medios digitales, electrónicos, podemos decir entonces que con la integración de la firma electrónica, estamos en un proceso jurídico electrónico. Es una nueva forma de llevar un control adecuado de cada uno de los juicios y, además de disminuir el papeleo que se lleva en los juicios tradicionales.

Para James Goldschmidt, el juicio oral es "un nuevo proceso penal que transparenta y acerca la justicia a la sociedad, poniendo en evidencia el trabajo de jueces, ministerios públicos, policía investigadora, peritos y defensores".

La informática jurídica tiene un nuevo campo de estudio y de trabajo, algunas de las actividades que los informáticos jurídicos pueden desempeñar en estos juicios orales son:

- Equipamiento, licenciamiento de software, capacitación e instalación.
- Automatizar equipos para grabar videos, documentos electrónicos, para publicarse o para ser visualizado por las partes de un proceso a través de una intranet.
- Se aprovecha una funcionalidad del software para programar grabaciones según el calendario de juicios orales.
- Utilización de firma electrónica para seguridad (encriptación) y validez jurídica al proceso electrónico.

(Ver Anexo 3)

Cibernética

"Ciencia de las regularidades generales de los procesos de control y transmisión de la información en máquinas orgánicas vivos y sus conjuntos. Nos interesa la informática puesto que ella se refiere al tratamiento lógico y sistemático de la información".

La palabra Cibernética, derivada del griego Κυβερνήτης (kybernetes) y significa "arte de pilotar un navío" (timonel), apareció por primera vez con Platón, y fue usada en el siglo XIX por André Marie Ampere para referirse a los modos de Gobierno. En 1943 un grupo de científicos encabezados por el matemático Nobert Wiener había reconocido la necesidad de elegir un nuevo término para designar un cuerpo de teorías e investigaciones. En 1947 Wiener, adoptó la palabra Cybernetics que fue popularizada en su libro de 1948 titulado "Cybernetics, or the study of control and communication in the animal and machine".

"La cibernética, según el epistemólogo, antropólogo, cibernetista y padre de la terapia familiar, Gregory Bateson, es la rama de las matemáticas que se encarga de los problemas de control, recursividad e información. Bateson también afirma que la cibernética es "el más grande mordisco a la fruta del árbol del Conocimiento que la humanidad haya dado en los últimos 2000 años".

Para el profesor Dr. Stafford Beer, la cibernética estudia los flujos de información que rodean un sistema, y la forma en que esta información es usada por el sistema como un valor que le permite controlarse así mismo: ocurre tanto para sistemas animados como inanimados indiferentemente.

La cibernética es una ciencia interdisciplinar, estando tan ligada a la física como al estudio del cerebro como al estudio de los computadores, y teniendo también mucho que ver con los lenguajes formales de la ciencia, proporcionando herramientas con las que describir de manera objetiva el comportamiento de todos estos sistemas.

El propio Stafford Beer afirmó: "Probablemente la primera y más clara visión dentro de la naturaleza del control... fue que éste no trata de tirar

de palancas para producir unos resultados deseados e inexorables. Esta noción del control se aplica sólo a máquinas triviales¨.

Veamos:

(Ver Anexo 4)
(Ver Anexo 5)

Documento Jurídico

Es aquél soporte físico que se caracteriza por poseer información jurídica, sea esta mediata o inmediata, por lo tanto hay que distinguir aquél que contiene una norma jurídica, en cualquiera de sus presentaciones, de aquél que constituye una explicación científica, una interpretación, una recopilación o una sistematización de sus contenidos o el resultado de investigaciones empíricas acerca de su vigencia real y práctica.

Características:

Es la expresión de una norma jurídica
1. Derecho vigente o histórico
2. Utiliza un lenguaje técnico especializado y preciso.

Lenguaje Jurídico

Es un lenguaje científico que utiliza como herramienta insustituible el lenguaje común, lo que trae inconvenientes por la variada significación de una palabra sin embargo el lenguaje jurídico delimita el concepto.

Clases de lenguaje

Estrictamente jurídico. Eje. Hipoteca, gravamen.
Lenguaje técnico de otras ciencias, químico, física.
Lenguaje ciencia de padre, madre.

Lenguajes Jurídicos artificiales

1. Formulas simbólicas de la Lógica de las proposiciones de ALCHORNON Y BULYGIN.
2.El lenguaje jurídico normalizado de ALLEN
3. Algebra de los sistemas normativos

MAPA MENTAL INFORMÁTICA JURÍDICA

(Ver Anexo 6)

SEGUNDA PARTE
DERECHO Y NUEVAS TECNOLOGÍAS

Se trata de una nueva área de estudio que interrelaciona el derecho con la tecnología, disciplina que generalmente se la denomina "Derecho Informático", "Derecho telemático", "Iuscibernética", "Derecho de Internet", también "Derecho tecnológico", "Derecho de las nuevas tecnologías de la información y comunicación- TICS", o "Derecho de la sociedad de la información", etc.

Esta nueva materia en el campo del derecho tiene su propia autonomía, igual que el derecho civil o penal, por lo que tendremos que examinar algunos aspectos relativos a su estructura, en lo principal el objeto de estudio de las nuevas tecnologías y su impacto en el ámbito jurídico.

El estudio particularizado del derecho informático se lo aborda con el conocimiento de principios y fundamentos en métodos e instituciones propias, la autonomía radica en que esta nueva rama del derecho tiene características acreditadas en diversos campos.

En el campo de la legislación se ha desarrollado abundante normativa específica, tanto a nivel mundial, como internamente en cada país que ha regulado esta temática.

En el campo docente se realiza un estudio particularizado de la materia. (Ver: wikipedia.org. También en el campo científico se destaca la actividad de juristas investigadores y doctrinarios que abordan la problemática jurídica de las nuevas tecnologías. (Ver: http://www.alfa-redi.org. En el campo institucional se han creado entidades propias que no se encuentran en otras áreas del derecho. (Ver: www.cetid.abogados.ec).

El término "Derecho Informático" *(Rechtsinformatik)* fue acuñado por el Prof. Dr. Wilhelm Steinmüller, académico de la Universidad de Regensburg de Alemania, en los años 1970. (Ver: http://www.informaticsapplied-textbook.info/indexe.html).

Campo de estudio del Derecho Informático:

Acceso y protección a la información
Acceso y seguridad a las TICs
Administración de justicia y nuevas tecnologías.
Ciberjusticia -notificación por medios electrónicos
Aspectos tributarios. Impuestos e internet
Banca y dinero digital, pago y transferencia electrónica de fondos TEF
Censura en Internet. Libertad de expresión online
Comercio electrónico
Contratos informáticos
Compras públicas mediante el uso de las NTIC
Computo en la nube. Lex cloud computing LCC
Correo electrónico, email
Delitos informáticos
Derecho en la era digital. Derecho Digital
Derecho de las telecomunicaciones
Derecho laboral e informática. Teletrabajo
Documento electrónico, mensajes de datos, EDI y Factura electrónica
E-government
E-learning del Derecho y nuevas tecnologías
E-marketing. Publicidad e internet
Firma electrónica –digital– PKI
Hábeas data
Informática jurídica - forense
Manifestación de la voluntad por medios electrónicos
Medidas cautelares sobre equipos informáticos
Nombres de dominio y direcciones IP
Pericia digital forense
Protección de datos. Privacidad, intimidad
Propiedad Intelectual y Propiedad Industrial e Internet.
Programas: Software Jurídico. Bases de datos y de Gestión
Protección al consumidor. Condiciones generales de la contratación CGC
Prueba penal digital y prueba electrónica-digital
Seguridad informática
Sistemas alternativos de solución de conflictos ADR

Sociedad civil e internet
Sociedad de la información
Software libre
Telefonía y voz sobre IP
Wireless Application Protocol (WAP)

Desarrollemos las temáticas más relevantes de esta área del derecho.

COMERCIO ELECTRÓNICO

Ecuador como país no está ajeno al desarrollo e integración de las denominadas nuevas tecnologías de la información, instituciones públicas y privadas están creando páginas de información en Internet, así como promoviendo por este medio, actividades y comercialización de productos, por lo que en los últimos tiempos el crecimiento comercial en la web ha sido importante.

De esta realidad surge la necesidad de regular la actividad denominada "comercio electrónico", en su concepto más general se refiere a: "Toda transacción civil, comercial o financiera, contractual o no, que se efectúe a través del intercambio de mensajes de datos o medios similares". (Definición de la ley ecuatoriana).

Por ello los expertos dicen que el "Comercio electrónico es la integración de servicios de Comunicaciones, Administración de Datos y Seguridad para permitir que aplicaciones de negocios intercambien información automáticamente" (National Institute of Standards and Technology, NIST).

No se hace diferencia en esta definición, entre el manejo electrónico de transacciones de compra/venta y el simple intercambio de datos o documentos que ocurre en paralelo a alguna operación de negocios. Ambos aspectos de la actividad comercial se ven beneficiados por la aplicación de tecnología informática, de ahí la extensión de la definición.

Internet ha traído consigo diversas maneras de hacer negocios electrónicos a través de esta red de redes que está distribuida en todo

el planeta. Es por ello, que los cambios y las nuevas tecnologías se unen para revolucionar la forma en que se llevan a cabo los negocios.

La competitividad, conectividad, ha hecho del Internet una vía de desarrollo, en donde no sólo los ofertantes, sino también los usuarios son beneficiados, hoy en día los procesos comerciales sobrepasan límites, y es de esta manera que el Comercio Electrónico nace como una nueva herramienta para los negocios que provee de oportunidades a todos los involucrados.

A más de ser el Comercio Electrónico "la forma propia de Internet en la que se realizan transacciones financieras o económicas, y se mantienen relaciones comerciales de manera directa entre comprador y vendedor", dando la posibilidad de que las comunicaciones y los equipos de tecnología estén al alcance de todos.

La principal característica de esta forma de comercio es la rapidez con la que se pueden realizar las transacciones de productos o servicios, sin que la distancia, el tiempo y los costos lo limiten. De esta manera, el Comercio Electrónico se convierte en la herramienta del mundo globalizado.

El Comercio Electrónico permite que los inmersos en esta tecnología puedan comprar bienes y servicios variados, que van desde un seguro de vida o software, hasta dulces o flores, por ello se habla del nuevo "boom mundial", que para América latina significa un potencial de desarrollo pues las posibilidades en Internet son infinitas.

El Comercio Electrónico toma parte en un mercado, donde quienes se ven involucrados en la transacción (consumidores, proveedores, clientes, empresas, suministradores de tecnología, gobiernos, etc.) pueden satisfacer sus necesidades electrónicamente, y se desenvuelven en un medio de operaciones y de transacciones que van desde el contacto del cliente y del proveedor inicial, hasta la compra-venta electrónica con el consumidor final.

Esta nueva modalidad de realizar negocios, se desenvuelve en un medio en el que se han desarrollado sistemas de seguridad para garantizar la

transferencia de datos confidenciales (número de tarjeta de crédito, domicilio o la empresa, gasto de la compra, costo, etc.). "Son dos los tipos de tecnologías las que garantizan la seguridad del comercio electrónico, Secure Sockets Layer (SSL) y Secure Electronic Transaction (SET). Ambas tecnologías encriptan (codifican) la información de compra antes de ser enviada a través de internet".

Cualquier transacción financiera se realiza de la cuenta del proveedor o suministrador del producto o servicio, a la cuenta del consumidor o cliente que lo adquiere y viceversa. La transacción se lleva a cabo automáticamente a través de entidades bancarias que intervienen para validar la información de las tarjetas de crédito y los datos que intervienen en la compra - venta.

Entonces, los aspectos jurídicos del comercio electrónico son importantísimos, algunos países han seguido muy de cerca la Ley modelo de Comercio Electrónico elaborada por la UNCITRAL, que nació vinculada al entorno tecnológico del EDI (Electronic Data Interchange), en cambio la Unión Europea, tiende a legislar en forma individualizada cada tema, como por ejemplo: firma electrónica, o la protección de datos, a través de Directivas.

El profesor Davara Rodríguez, nos dice que: "Para saber qué es el comercio electrónico es necesario analizar dicho concepto, de manera que debe entenderse por comercio toda aquella actividad que tenga por objeto o fin realizar una operación comercial, y es electrónico cuando ese comercio se lleva a cabo utilizando la herramienta electrónica de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial, o en el resultado de la actividad que se está desarrollando. Por tanto, el comercio electrónico supone la realización de transacciones comerciales, y por tanto con un determinado fin económico, mediante la utilización de medios electrónicos, en particular de redes de telecomunicación o comunicación electrónica como Internet, permitiendo la contratación de bienes o servicios a través de dichos medios. Dentro del concepto de comercio electrónico pueden llevarse a cabo diversas clasificaciones en función de un criterio determinado, pudiendo ser éste la realización completa de la transacción a través del medio electrónico utilizado para la contratación, pudiendo ser éste

directo o indirecto, en función de si se suministran los bienes o servicios a través de dicho medio. Si se atiende a los sujetos que intervienen en la realización de una operación de comercio electrónico, este criterio puede dar lugar a la aparición de múltiples combinaciones en función de las partes que intervienen en la misma, pudiendo señalarse a modo de ejemplo: A2*; B2* o C2*". (Ver: http://www.davara.com/default.html).

El Comercio electrónico abarca como estudio la siguiente temática: mensajes de datos, documentos electrónicos, contratación electrónica, firma electrónica, gobierno electrónico, protección de datos, protección al consumidor, resolución alternativa de conflictos, pago electrónico, factura electrónica, transferencia electrónica de fondos y de datos, intercambio electrónico de información, seguridad en las transacciones electrónicas.

Esta temática esta regularizada por la normativa de cada país, por su incidencia directa o indirecta en el comercio electrónico, la actividad en las redes esta regularizada, inclusive el mal uso de la prestación de servicios está compilado en la norma positiva de las infracciones electrónicas.

(Ver Anexo 7)

En el caso del Ecuador por iniciativa privada, se ha impulsado la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de Datos, aprobada en el año 2002, que es la que a continuación realizo un breve estudio y doy mi opinión y observaciones sobre la misma.

DOCUMENTOS ELECTRÓNICOS

I.- DOCUMENTOS ELECTRÓNICOS Y MENSAJES DE DATOS

En el objeto de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del Ecuador[1], el Art. 1, estipula que "Esta ley

[1] Ley No. 67 R.O.S. 557 del 17 de Abril de 2002.

regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos servicios".

Es decir el documento electrónico es contenido en un mensaje de datos, es por ello que el Art. 2 de la Ley le da reconocimiento jurídico al mensaje de datos, cuando norma que "Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su Reglamento".

Entonces, es inevitable que todas las instituciones, especialmente las gubernamentales, así como las privadas y las personas en general, tomen conciencia de las posibilidades para implementar de forma ágil y diligente la utilización de medios tecnológicos, especialmente, del documento electrónico.

Vamos a la construcción de la sociedad de la información, de aquella en la que la tecnología es el medio que facilita toda transacción pública o privada, en la que la tendencia es la de desaparecer el documento papel, y se impone el documento electrónico, lo que abarata costos, y permite fluidez en la comunicación de todo negocio y prestación de servicio por medios electrónicos.

Al respecto a nivel internacional se ha legislado en este sentido, es así, como la primera ley que ha regulado los aspectos jurídicos de la firma digital como documento electrónico e instrumento probatorio, fue en los Estados Unidos, se aprobó en 1997 en Utah. Posteriormente surgieron proyectos legislativos en Georgia, California y Washington. En Europa, el primer país que ha elaborado una ley sobre la materia ha sido Alemania.

Es evidente que la eficacia de estas leyes radica en su uniformidad, ya que si su contenido difiere en cada Estado, será difícil su aplicación a un entorno global como Internet. Por ello, el esfuerzo a realizar a partir de ahora deberá centrarse en la consecución de un modelo supraestatal,

que pueda ser implantado de manera uniforme en las leyes nacionales. Tal tarea puede encomendarse a organismos internacionales como UNCITRAL, que ya dispone de experiencia en iniciativas similares en materia de EDI[2].

Definición

El documento electrónico debe entenderse como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

En las disposiciones generales de la Ley ecuatoriana, se define a Mensaje de datos como: "Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes documentos electrónicos, registros electrónicos, correo electrónico, servicio web, telegrama, télex, fax e intercambio electrónico de datos".

Entonces nos referimos a todos los Documentos que son emitidos por medios electrónicos, magnéticos, digitales o informáticos.

Los documentos soportados en medios magnéticos no responden al concepto tradicional o restringido de documento manuscrito en soporte en papel, sino al amplio. Por exclusión, entendemos que constituye un documento no electrónico aquel que es elaborado por las formas tradicionales, sean éstas manuales, mecanográficas, micrograbadas, microcopiadas o fotográficas.

Al hablarse de documentos electrónicos se alude a casos en que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad quizás ya expresada en las formas

[2] Intercambio electrónico de datos.

tradicionales, y en que la actividad de un computador o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales.

Los documentos electrónicos poseen los mismos elementos que un documento escrito en soporte en papel:

a) Constan en un soporte material (cintas, diskettes, circuitos, chips de memoria, redes, etc.);
b) Contiene un mensaje, el que está escrito usando el lenguaje convencional de los dígitos binarios o bits, entidades magnéticas que los sentidos humanos no pueden percibir directamente;
c) Están escritos en un idioma o código determinado;
d) Pueden ser atribuidos a una persona determinada en calidad de autor mediante una firma digital, clave o llave electrónica.

Una cuestión importante es tener presente que eventualmente será necesario imprimir o traspasar a soporte en papel los documentos digitales o electrónicos. Se trata de casos de necesidad práctica, como ocurre y para citar un ejemplo con las declaraciones aduaneras de importación de mercancías que deben imprimirse para retirar las mercancías desde los recintos portuarios o para pagar en los bancos los derechos de aduana.

El problema surge porque en los diferentes casos la firma digital de los documentos electrónicos desaparece, y al no intervenir el nombre carecerá de firma manuscrita y será difícil determinar su autoría o atribuir responsabilidades.

Otro tema de gran interés, relacionado con los documentos digitales o electrónicos, es el de los documentos enviados o transmitidos a distancia vía telefax o facsímile. ¿Puede decirse que se trata de un documento soportado magnéticamente? Ocurre que aunque los fax

son transmisores vía telefónica magnéticamente almacenados en la memoria del fax receptor para su ulterior impresión en papel. Creemos que la transmisión de la moción en el momento es la oportunidad de establecer, con algunas precisiones, que la fotocopia o documento nuevo que resulta de la transmisión a distancia vía telefónica y que emana del fax receptor tenga legalmente el mismo valor que el original "enviado, pasado, leído o barrido" por el fax transmisor.

II.- VALIDEZ JURÍDICA DE LOS DOCUMENTOS ELECTRÓNICOS

Conforme aumenta el uso de Internet para celebrar contratos, van surgiendo controversias y conflictos, mismos que en muchas ocasiones requieren de una intervención judicial para llegar a un acuerdo entre las partes.

Generalmente se trata de los mismos problemas que se presentan en el comercio tradicional, pero ahora aplicados a situaciones relacionadas con el ciberespacio, donde la comunicación se realiza por medio de mensajes electrónicos.

Este es probablemente uno de los temas que pudieran tener la mayor trascendencia en las transacciones electrónicas. Hoy en día muchos dudan sobre la validez de utilizar documentos electrónicos como medio de prueba y, lo que es más grave, en ocasiones son los mismos jueces quienes se cuestionan la validez probatoria de los acuerdos y demás documentos que no constan en papel; o documentos digitales.

Probablemente, la mayoría de las legislaciones establecen restricciones estrictas o taxativas a los medios de prueba, y, considerando el carácter novedoso y reciente de las tecnologías de la informática y el Comercio Electrónico, obviamente no contemplan entre sus medios de prueba a los documentos electrónicos.

El problema se acrecienta al recordar el retraso tecnológico en el Poder Judicial de muchos países. Así, se dificulta enormemente la utilización

de los documentos electrónicos como medio de prueba, debido a que los funcionarios no tienen, en la mayoría de las ocasiones, la más mínima preparación técnica para operar computadores y, consiguientemente, trabajar con este tipo de documentos.

De aquí que una de las prioridades en la reglamentación del Comercio Electrónico es, precisamente, reconocer el valor probatorio de este tipo de documentos, a manera de garantizar la posibilidad de exigir el cumplimiento, por lo menos en el caso de los acuerdos electrónicos, por la vía judicial.

Debemos considerar que en la valorización de las pruebas que realizan los jueces, ellos recurren necesariamente a apreciaciones y opiniones que, hasta cierto punto, pudieran calificarse como subjetivas, siempre y cuando lo hagan basándose en la razón y su experiencia. Así, entrarán a analizar ciertos elementos de la prueba, como su integridad, inalterabilidad, veracidad y exactitud.

Y, como ya observamos, gracias a los avances tecnológicos es innegable que los documentos electrónicos pueden llegar a cumplir de hecho con los requisitos de las pruebas que analizarán los jueces. E incluso más, las superan en integridad e inalterabilidad. Es por eso que en esa valorización "subjetiva" el juez deberá considerar estas características de los documentos electrónicos.

El impacto que está teniendo el Comercio Electrónico en el funcionamiento de la sociedad, hace indispensable el adecuado reconocimiento legal de los acuerdos y demás contratos celebrados electrónicamente, de manera que sea posible utilizar los documentos digitales, o aquellos que no constan en el "papel tradicional", como medio probatorio, perfectamente válido, en cualquier procedimiento judicial.

En muchas ocasiones, con meras inserciones en la legislación probatoria bastará para incluir y reconocer legalmente a los documentos electrónicos como medio de prueba.

Estas modificaciones deberán ser flexibles para adaptarse a la evolución de los mercados electrónicos, de manera que éstos en todo momento puedan considerarse como vías seguras de contratación, y proteger la obligatoriedad jurídica de los acuerdos alcanzados en el ciberespacio. Refuerza esta conclusión el artículo 113 del Código de Procedimiento Penal Chileno, en el que existe una enumeración abierta de los modernos medios de prueba.

Sin embargo, en la realidad muchas veces esta regulación no será suficiente, ya que las personas que van a aplicar la ley necesariamente deben conocer los límites y capacidades de las tecnologías de la informática, para lograr una adecuada valorización de los documentos electrónicos. Asimismo, será indispensable contar con la infraestructura física de herramientas, como computadores actualizados, que permitan recibir las pruebas que consten en documentos electrónicos.

III.- ¿QUÉ ES LA FIRMA DIGITAL Y EL DOCUMENTO ELECTRÓNICO?

Profundizaremos el tema en el capítulo correspondiente cuando abordemos todo sobre la firma digital y entidades de certificación. Por el momento nos referiremos en el contexto de firma digital y su relación con el documento electrónico.

La Firma ológrafa o manuscrita, es una expresión de voluntad en un medio o soporte en papel.

La Firma Digital, es el reemplazo de la firma ológrafa utilizada en medio papel, que manifiesta la misma intención y expresión de voluntad para el medio electrónico.

Partiendo de la premisa de cumplimentar con el paradigma de seguridad mencionado, la utilización de técnicas surgidas de la criptografía permiten fácilmente cumplir con la:

Integridad: la información contenida en el mensaje o transacción electrónica que no ha sido modificada luego de su firma.

Autenticación: la información del documento y su firma se corresponden indubitablemente con la persona que ha firmado.

No Repudio: la persona que ha firmado no puede decir que no lo ha hecho.

Confidencialidad: la información contendida ha sido cifrada y la voluntad del emisor, sólo permite que el receptor que él determine pueda descifrarla.

El Documento Electrónico se encuentra íntimamente ligado a la Firma Digital, pero independiente de las teorías que particularmente se expresan filosóficamente sobre el mismo, es la Firma Digital la que transforma en realidad la posibilidad de obviar el medio papel, por el medio electrónico firmado adecuadamente, por cuantas firmas sean necesarias. Es de destacar que el documento electrónico firmado digitalmente, conlleva la garantía de la integridad del documento al momento de la firma, cosa que en papel se debe determinar con costos de tiempo y dinero.

IV.- TIPOS DE DOCUMENTO ELECTRÓNICO

¿Para qué sirven?

La Firma Digital, en concreto, sirve para la Identificación Indubitable de una persona que emite un mensaje, transacción o documento en medios electrónicos. Es en definitiva, según la finalidad particular, el pasaporte, la llave del vehículo, la casa, la oficina, la identificación de autoría de un documento, un plano, una investigación científica, un software, el carnet de un club, y tantas otras aplicaciones como se pueda imaginar, con el importante incremento de la impersonalización que se produce día a día, imaginándonos que ciertas actividades se han realizado durante años por la simple emisión verbal y hoy requieren de un respaldo mayor, adicionándole la facilidad de ahorros importantes en el tiempo, costos y exactitud en la trasmisión.

Es así que vistos los tiempos en que vivimos, es aplicable entre otras a:

• Identificación como usuario ante redes Internas o Externas.
• Correos Electrónicos.
• Sitios de Internet.
• Comercio Electrónico.
• Transacciones EDI (Electronic Data Interchange).
• Información que se obtenga de Internet.
• Transacciones Financieras.
• Software y Hardware.
• Análisis y Mediciones realizados con instrumental electrónico corroborado por un especialista.
• Comercio Exterior.
• Comercio Interno.
• Toda documentación que precise movilizarse rápidamente o por el contrario que posea un alto costo de movilización.

APLICACIONES EN PARTICULAR

Sobre la Firma Digital

• Firma y/o Cifrado de Correo Electrónico, tanto Interno como Externo.
• Firma y/o Cifrado de Documentos (Pericias, Dictámenes, Planos, Software, Políticas, Procedimientos, Normativas, Minutas, y otros).
• Identificación de Personas ante Sistemas Internos en redes locales y abiertas (Intranets), Sitios Web (sin necesidad de registrar datos).
• Determinación implícita del Perfil de Usuario. Identificación de Sistemas ante el Usuario (¿Cómo sé que es el sistema que dice ser?). Auditoría de Transacciones.
• Seguridad al operar Comercialmente (Compra-Venta de Acciones, Transacciones Bancarias, Operaciones con Tarjeta de Crédito, y otras).
• Identificación de los componentes físicos de una red (Computadores, Ruteadores, Teléfonos Celulares, y otros).
• Mediciones realizadas por instrumental electrónico que deba ser corroborado por un especialista.

Sobre el documento Electrónico Firmado Digitalmente

• Fidelización de Documentos digitalizados.
• Cotizaciones de Bienes y Servicios (tanto el pedido como la cotización y condiciones del proveedor).
• Resúmenes de cuenta.
• Recibos de pago.
• Adjudicaciones.
• Factura electrónica.
• Cheque electrónico.
• Invitaciones.
• Promociones.
• Acreditaciones de puntaje.
• Remitos de entrega.
• Órdenes de compra.
• Solicitudes de adhesión
• Contratos.
• Actas.
• Planos.
• Planificaciones.
• Circulares internas y/o externas.
• Reservas o Turnos para distintas prestaciones (Talleres, Médicos, Hoteles, Pasajes, etc.).
• Confirmaciones.
• Autorizaciones de prestaciones médicas.
• Receta médica electrónica.
• Historia clínica única.
• Declaraciones juradas.
• Solicitudes de prestación de servicios.
• Proyectos.
• Diseños.
• Tarjetas de Crédito (sin utilizar el número y consecuentemente disminuir el fraude).
• Otros.

(Ver Anexo 8)

SEGURIDAD ELECTRÓNICA

I.- SEGURIDAD Y CRIPTOGRAFÍA

Historia de la encriptación

La criptografía es tan antigua como la escritura. Desde que el homo sapiens inició su recorrido sobre este planeta, ha necesitado comunicarse con sus semejantes, pero en ocasiones no quiere que otros se enteren. Las razones son evidentes, especialmente como una estrategia de guerra ya que a ninguno le gustaría que el enemigo conociera su estrategia si lograse interceptar un mensaje.

Se dice que las primeras civilizaciones que usaron la criptografía fueron la egipcia, la Mesopotamia, la India y la China. Los espartanos, 400 años antes de Cristo, utilizaban un sistema secreto de escritura, el cual consistía en un cilindro al cual se colocaba un papiro en forma de espiral. Se escribía entonces el texto en cada una de las vueltas del papiro, pero de arriba hacia abajo. Una vez desenrollado, sólo se podía leer una serie de letras aparentemente inconexas. Para descifrar el mensaje era necesario colocar el papiro exactamente en la misma posición en la que había sido escrito. Antiguos textos judíos fueron encriptados siguiendo el método de sustituir la primera letra del alfabeto por la última y así sucesivamente. En la Biblia (Jeremías 25:26) el nombre de Babilonia aparece encriptado como "Sheshech".

Pero a quien se atribuye el primer método de encriptado con su debida documentación es al general romano Julio César, quien creó un sistema simple de sustitución de letras, que consistía en escribir el documento codificado con la tercera letra que siguiera a la que realmente correspondía. La A era sustituida por la D, la B por la E y así sucesivamente. En la Edad Media el uso de la escritura codificada se incrementó. Un libro de astronomía escrito en 1390 y atribuido a Geoffrey Chaucer contiene trozos cifrados.

En 1470, León Battista Alberti publicó "Tratado de cifras" en donde describe una cifra capaz de encriptar un pequeño código. No obstante se considera al abate Johannes Trithemius es el padre de la criptografía

moderna. Este religioso escribió en 1530 "Poligrafía", el primer libro impreso sobre el tema. Trithemius introdujo el concepto de tabla ajustada, en el cual el alfabeto normal es permutado para codificar los mensajes. Son legendarios los mapas de tesoro escondidos durante los siglos XVII y XVIII. En ellos los piratas supuestamente encriptaban la localización de enormes tesoros, basándose principalmente en métodos de sustitución de alfabeto.

El principal uso de la criptografía en la era moderna ha sido militar. En 1917, por ejemplo, el servicio de Inteligencia Naval de Inglaterra entregó a los Estados Unidos un mensaje que había sido enviado al embajador alemán en Ciudad de México por el gobierno germano. En el mismo se autorizaba al diplomático a negociar un acuerdo con México para entrar a favor de Alemania en la Primera Guerra Mundial. A cambio, los mexicanos recibirían los territorios de Nuevo México, Arizona y Texas, en el caso de que resultasen vencedores. El texto -conocido como el telegrama Zimmermann impulsó a los norteamericanos a participar en esa guerra contra Alemania.

Los códigos de la máquina Enigma, usada por los mismos alemanes durante la Segunda Guerra, fueron rotos por los analistas norteamericanos, al igual que los códigos usados por los japoneses.

Y ahora que la informática se ha apoderado de los hogares, como no, se han de introducir sistemas que sean seguros para realizar operaciones.

La actividad humana que ha dado más impulso al derecho, es sin duda el comercio, actualmente se realiza no sólo comercio presencial, sino que, al estar ocurriendo una revolución en la informática y las comunicaciones, se hace necesario que los contratos se lleven a cabo con personas que están muy distantes geográficamente, pero para que el contrato tenga validez jurídica debe cumplir una serie de requisitos, uno de los principales es que demostremos nuestra identidad y conformidad con dicho contrato.

Las firmas tradicionales (escritas) indican el acuerdo que tiene una persona con los términos de un contrato o documento en general, esa firma es única y auténtica. Las firmas digitales realizan la misma función

pero en documentos electrónicos, utilizando diversas tecnologías que permitan al receptor del documento tener la certeza de la identidad de la persona que envía el documento.

Las Firmas Digitales se basan en matemáticas aplicadas y utilizan algoritmos de criptografía, que son procesos por los cuales se oculta la información a enviar de un emisor a un receptor, evitando de ésta manera la visualización, manipulación o modificación de la misma en el caso de una interceptación. Si alguien ajeno intercepta éste documento y lo quiere imprimir, lo único que obtendrá será una serie de códigos y símbolos sin una secuencia lógica, que no podrá interpretar, esto da seguridad al envío.

Un elemento importante en este proceso es un intermediario llamado "Entidad de Certificación" quien haría las veces de un Notario, cuya labor es establecer el nexo entre el firmante y las llaves utilizadas para crear la firma digital. En esencia, la Entidad de Certificación revisa los documentos de identificador del firmante, como licencia, pasaporte, o cualquier documento que ratifique su persona y posteriormente certifica que la persona que está utilizando la llave sea realmente la persona que dice ser. Cualquiera que desee verificar una firma digital debe de confiar en la autoridad de certificación en lugar de personalmente revisar los documentos de identificación del firmante.

La incorporación de nuevas tecnologías de la información, como es el caso del uso del Internet como medio de comunicación, E-Commerce (Comercio Electrónico), E-Bussiness (Negocios Electrónicos), hace que, en muchas ocasiones, los conceptos jurídicos tradicionales resulten poco idóneos para interpretar las nuevas realidades. Lo cual indica que se deben realizar modificaciones y actualizaciones a leyes que tengan implicancia con este tipo de contrataciones.

ANTECEDENTES

Firma Convencional ("Analógica")

La Real Academia de la Lengua define la firma como: "nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un

documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido o para obligarse a lo que en él se dice".

En el Vocabulario Jurídico se define como: "Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse en lo que en ellos se dice".

En Roma, los documentos no eran firmados. Existía una ceremonia llamada *manufirmatio,* por la cual, luego de la lectura del documento por su autor o el *notarius,* era desplegado sobre una mesa y se le pasaba la mano por el pergamino en signo de su aceptación. Solamente después de cumplir esta ceremonia se estampaba el nombre del autor.

En el Sistema Jurídico Visigodo existía la confirmación del documento por los testigos que lo tocaban, signaban o suscribían. La firma del que da el documento o librador es corriente, pero no imprescindible. Las leyes visigodas prestaron atención a las formalidades documentales, regulando detalladamente las suscripciones, signos y comprobación de escrituras.

La *"subscriptio"*, representaba la indicación del nombre del signante y la fecha, y el *"signum"*, un rasgo que la sustituye si no sabe o no puede escribir. La *"subcriptio"* daba pleno valor probatorio al documento y el *"signum"* debía ser completado con el juramento de la veracidad por parte de uno de los testigos. Si falta la firma y el signo del autor del documento, éste es inoperante y debe completarse con el juramento de los testigos sobre la veracidad del contenido.

En la Edad Media, la documentación viene garantizada en su autenticidad por la implantación del sello real. Sello que posteriormente pasó a las clases nobles y privilegiadas.

La firma es definida en la doctrina como el signo personal distintivo que, permite informar acerca de la identidad del autor de un documento, y manifestar su acuerdo sobre el contenido del acto.

La firma acredita la autoría del documento subscrito normalmente al pie del mismo y representa la formalización del consentimiento y la aceptación de lo expuesto, y es por tanto origen de derechos y obligaciones.

La firma será válida siempre que no sea falsificada o se haya obtenido con engaño, coacciones o de cualquier otro ilícito proceder.

Criptografía

La etimología de la palabra criptografía es: *Kriptos* (oculto) y *graphos* (escribir)

Del diccionario enciclopédico se tomará como una definición bastante adecuada, la que dice: "escritura secreta realizada mediante clave, de manera que sea imprescindible conocer ésta para descifrarla". Asimismo, criptograma está definido como "documento cifrado" o bien "documento escrito con alguna escritura secreta".

La criptografía o ciencia criptográfica estudia los procesos de cifrado y descifrado de los mensajes, así como el análisis de los criptogramas para descubrir la clave y texto original. Este último aspecto de la ciencia criptográfica recibe el nombre de criptoanálisis.

El primer empleo de la escritura secreta o cifrada de que se tiene constancia histórica es el caso de un esclavo que sirve como portador de un mensaje en la guerra entre Atenas y Esparta (Siglo V a.C.). El general Lysandro recibe en una lista una serie de letras con aparente falta de sentido. Esta lista al ser enrollada en un determinado rodillo de madera, mostraba longitudinalmente los símbolos dispuestos de tal manera que podía leerse el mensaje, que en esta ocasión histórica sirvió para salvar un imperio y un general. El cifrado consistía en una simple alteración incluyendo símbolos innecesarios que desaparece al descifrar, enrollando la lista en el rodillo. Este es el método que describe Plutarco con el nombre de "escítalo lacedemonio".

A través de la historia, son muchas las instituciones y personajes que han hecho uso de algún sistema criptográfico, para el envío seguro de

sus comunicaciones privadas, desde la época romana en tiempos de guerra, hasta hoy en día, en donde se hace necesario para asegurar las transacciones electrónicas.

Un empuje decisivo fue dado por Leon Battista Alberti (1404 - 1472), se le considera el padre de la criptología. El método de Alberti, es un cifrado de sustitución simple que es efectuado por un par de círculos concéntricos con eje común, dividido en 24 casillas. En el anillo mayor están 20 letras del alfabeto (no aparecen H, J, K, U, Ñ, Y). En el anillo menor hay 23 letras, las 20 del exterior, más H, K, Y, y la conjunción francesa et, en cualquier orden. El cifrado se efectúa enfrentando una casilla del anillo exterior con otra del anillo interior. Esta pareja constituye la clave del cifrado, y con esta correspondencia entre ambos anillos se efectúa el cifrado. El propio Alberti recomienda cambiar la clave cada cierto tiempo.

Hasta el siglo XIX, los sistemas de escritura secreta se fundamentan en sustituciones con uno o varios alfabetos, transposiciones y empleo de palabras código, con algunas particularidades especiales en casos concretos.

Es impulso decisivo de la ciencia de la criptografía, fue dado por las dos guerras mundiales. El progreso del criptoanálisis fue formidable, poseyendo los Estados Unidos su propio departamento critoanalítico denominado M18. Durante la Primera Guerra Mundial, los franceses consiguieron averiguar la clave del cifrado alemán ADFGX y los ingleses el del telegrama Zimmerman. El telegrama Zimmerman usaba un código que asignaba cifras a las palabras de acuerdo a un libro de códigos que poseían emisor y receptor del mensaje. Otro sistema empleado, el ADFGX, usaba únicamente esas cinco letras para sustituir una combinación de ellas por cada símbolo del mensaje en claro. El cifrado sigue siendo de sustitución de cada letra por un par de símbolos, de acuerdo a una matriz.

La aparición de los trabajos sobre criptoanálisis, como el debido a los hermanos Friedman titulado "Elements of Cryptoanalysis", apoyó la necesidad de construir métodos de cifrado más complejos, que

puedan escapar a los conocimientos criptoanalíticos existentes hasta el momento.

Las máquinas que reciben el nombre de PURPLE y ENIGMA fueron las precursoras de las utilizadas en la Segunda Guerra Mundial, y que fueron notables mejoras de las usadas durante la primera mitad de los años 30. A partir de este momento, el incremento continuado en el uso de las telecomunicaciones y después la comercialización de ordenadores desde los años 50, amplían el ámbito de la criptografía mejorando las técnicas de cifrado y proporcionando potentes herramientas en los análisis criptoanalíticos.

ESTRUCTURA DE UN SISTEMA SECRETO

La protección de la información en un sistema automático de tratamiento de la información se aplica mediante técnicas criptográficas, tanto a los datos almacenados en el soporte, discos o cintas, como a la información transmitida a través de algún canal de comunicación. De esta forma un acceso indebido a los soportes, o una escucha realizada interceptando un canal de comunicación, presentará información en forma de criptogramas, resultando incomprensibles al que no posea el resto de la información necesaria para su descifrado. Es preciso destacar que la aplicación de técnicas criptográficas al almacenamiento de la información no previene contra destrucción física, pero disminuye fuertemente el riesgo de su obtención no controlada.

El esquema de funcionamiento de un sistema secreto es idéntico, tanto si se trata de un sistema de comunicación, como si es un sistema de almacenamiento. En un sistema secreto hay dos funciones elementales que intervienen, que se denominan función de cifrado o proceso de cifrado, y función de descifrado o proceso de descifrado. Las funciones de cifrado y descifrado se suponen conocidas por el oponente (ladrón de información). Si el sistema fuera dependiente únicamente de las funciones de cifrado y descifrado (E y D respectivamente), el oponente tendría suficiente información para vulnerar el sistema, por tanto es preciso la existencia de algo que siendo desconocido impida al oponente obtener la información. Ese algo es la clave, necesaria para descifrar el mensaje.

La función de cifrado E, es tal que combina de alguna manera el mensaje original, o mensaje en claro, con la clave K, para obtener el mensaje cifrado o criptograma. Consecuentemente, la función de descifrado, D, combina el mensaje cifrado o criptograma, con la clave K, para obtener el mensaje original o mensaje en claro.

De este funcionamiento se deducen dos cosas al menos: La primera, que las funciones E y D provocan unas transformaciones en los mensajes, que son inversas una de la otra. La segunda, que la clave empleada en la función de descifrado, debe ser la misma que fue empleada en la función de cifrado, por lo tanto, pensando en un sistema secreto donde hay un emisor y un receptor, éste debe poseerla, habiéndola recibido mediante algún sistema no interceptable.

Sin embargo, no siempre sucede esto, es decir, la clave utilizada también puede ser interceptada, si nos vamos a un caso extremo.

Existen sistemas de seguridad simétricos y asimétricos, el primero maneja una sola clave para todo el sistema, con lo que se corre el riesgo de interceptación de la misma; su contrapartida son los sistemas secretos asimétricos, en donde el transmisor y el receptor manejan claves diferentes (llamadas clave privada para el transmisor y clave pública para el receptor), siendo alguna de ellas imposible de calcular a partir de la otra.

Por convenio se considera al sistema criptográfico como información pública, permaneciendo la seguridad en el hecho de mantener la clave secreta. Este hecho, aunque criticado, se basa en una regla importante en los estudios de seguridad: "La seguridad de un sistema no debería depender del nivel de secreto de algo que no puede ser cambiado fácilmente si está comprometido".

Puede considerarse a un sistema criptográfico como una combinación variable usada en las cajas de seguridad, en las que la estructura y funcionamiento de los sistemas de bloqueo son conocidos, ya que cualquiera puede adquirir una, mientras que la combinación (clave)

permanece secreta, pudiendo ser cambiada con la frecuencia que se desee.

SISTEMAS DE CLAVE PÚBLICA

Los sistemas de Clave Pública, proponen un sistema de comunicación privado que emplea un directorio de claves públicas, de tal manera que cada utilizador fija un procedimiento de cifrado, para que sea usado por otros usuarios cuando cifren mensajes que vayan dirigidos a él, mientras que guarda en secreto su propio procedimiento de descifrado (clave privada).

La principal diferencia que existe entre un sistema de clave pública respecto de otros sistemas, que pudieran denominarse de clave secreta, es precisamente la característica de asimetría. Podría afirmarse que los sistemas asimétricos pueden ser sistemas de cifrado de clave pública, en los que las claves para cifrar y descifrar son distintas y prácticamente imposible de obtener una a partir de la otra. Son relativamente fáciles de cifrar, pero de gran dificultad de descifrar, si no se conoce la segunda clave.

VERIFICACIÓN DE AUTENTICIDAD

La verificación de autenticidad incide sobre la seguridad que el transmisor desea para la integridad del mensaje, tratando de que no se altere o no se modifique, mientras que para el receptor lo importante es asegurarse que el mensaje proviene de ese transmisor.

Existe un ejemplo transaccional en el que el transmisor y el receptor tienen los mismos intereses perseguidos por la certificación de autenticidad, por ejemplo el envío de un cheque. El emisor del cheque, transmisor, no está preocupado por la autenticidad del documento, pero sí lo está por la posible alteración de la cantidad que él escribe en su cheque. El receptor del cheque sin embargo, está preocupado por la autenticidad del documento, y no le importa demasiado si la cantidad fue o no alterada. Un tercero, intermediario que acepta el cheque, estará muy atento a que ambos aspectos considerados, sean auténticos. Al

último receptor, el banco, que puede comprobar la firma de la persona que escribió el cheque, también le importan ambos aspectos, como a cualquier intermediario.

Si tomamos el caso en que se intercepte un mensaje cifrado y que se genere con él un mensaje en claro, con una clave en ASCII de cuatro caracteres (es decir, en total 32 bits), entonces la probabilidad de que el mensaje generado pertenezca al conjunto de posibles mensajes que puedan ser el original, es de 0.000015% y se puede asegurar un error de 16,3 bits.

Cualquier conocedor de claves públicas de A, podría reproducir un mensaje y enviárselo a B, pero con este esquema es difícil que eso ocurra porque está cifrado con claves de A y luego con claves de B, teniendo seguridad al descifrado, de que el mensaje M sólo puede proceder de A.

Una importante característica de los sistemas asimétricos para certificación de autenticidad, es que el receptor puede descifrar, pero no puede cifrar.

II.-TRANSMISIÓN SEGURA DE DOCUMENTACIÓN-FIRMA DIGITAL.

Descripción

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Es la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras dieron lugar al concepto. Pero sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas (jurídicas o reales).

Se intenta hacer coincidir el modelo de firma digital con los requerimientos y virtudes que debe tener una firma y así darle validez a esta mecánica. El fin es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado.

El papel es el medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito, etc.). Esta cualidad física le da entidad al documento, contiene sus términos, conceptos y sentidos de una manera perdurable, y al ser un elemento físico cualquier alteración dejará "señales" identificables.

Pero estas mismas cualidades traen aparejados inconvenientes que el uso de sistemas de computación podría evitar. Ciertamente los papeles ocupan lugar y pesan demasiado, resulta complejo y molesto buscar información en ellos (requiriendo de la acción humana ya sea al archivarlos y/o al rescatarlos), y el compartir los documentos también resulta inconveniente.

Ventajas ofrecidas por la Firma Digital

El uso de la firma digital satisface los siguientes aspectos de seguridad:

• Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese, un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor.

De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.
• Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code). El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.
• No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Aspectos técnicos

A diferencia de la firma manuscrita, que es un trazo sobre un papel, la firma digital consiste en el agregado de un apéndice al texto original, siendo este apéndice, en definitiva, la firma digital; al conjunto formado por el documento original, más la firma digital se lo denominará mensaje.

Este apéndice o firma digital es el resultado de un cálculo que se realiza sobre la cadena binaria del texto original. En este cálculo están involucrados el documento mismo y una clave privada (que, generalmente, pertenece al sistema de clave pública-privada o sistema asimétrico) la cual es conocida sólo por el emisor o autor del mensaje, lo que da como resultado que para cada mensaje se obtenga una firma distinta, es decir, a diferencia de la firma tradicional, la firma digital cambia cada vez con cada mensaje, porque la cadena binaria de cada documento será distinta de acuerdo a su contenido.

A través de este sistema podemos garantizar completamente las siguientes propiedades de la firma tradicional:

• Quien firma reconoce el contenido del documento, que no puede modificarse con posterioridad (integridad).
• Quien lo recibe verifica con certeza que el documento procede del firmante. No es posible modificar la firma (autenticidad).
• El documento firmado tiene fuerza legal. Nadie puede desconocer haber firmado un documento ante la evidencia de la firma (no repudio).

El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. Este sistema utiliza dos claves diferentes: una para cifrar y otra para descifrar. Una es la clave pública, que efectivamente se publica y puede ser conocida por cualquier persona; otra, denominada clave privada, se mantiene en absoluto secreto ya que no existe motivo para que nadie más que el autor necesite conocerla y aquí es donde reside la seguridad del sistema.

Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas que algo que es encriptado con la privada, sólo puede ser desencriptado por la clave pública.

Resumiendo, la clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma. Si bien, no se trata de un tema estrictamente técnico, es conveniente aclarar que en tiempo de generación de cada par de claves, pública y privada, podría intervenir otra clave que es la de la Autoridad Certificante que provee la garantía de autenticidad del par de claves generadas, así como también, su pertenencia a la persona cuya propiedad se atribuye.

Este esquema se utiliza en intercambios entre entidades cuando se trata de transferencias electrónicas de dinero, órdenes de pago, etc. donde es indispensable que las transacciones cumplan con los requisitos de seguridad enunciados anteriormente (integridad, autenticidad y no

repudio del origen), pero no se satisface el concepto de confidencialidad de la información (secreto).

En las reformas realizadas al Código Civil argentino no se ha tratado en forma expresa el problema de las nuevas tecnologías y en especial la utilización de documentos digitales. En los últimos años, principalmente en Europa y en Estados Unidos, las leyes han sido modificadas para adaptar el sistema de firmas digitales. Ciertas normas especiales como la ley de sociedades o de procedimiento tributario autorizaron el registro de datos en medios informáticos o la emisión de certificados de deuda con firma mecanizada, pero en principio y como regla de nuestro derecho, la forma de los actos jurídicos, cuando se trata de documentos escritos, no puede desligarse del papel y de la firma tradicional.

Los obstáculos para el reconocimiento del documento electrónico son:

• Escritura: la escritura puede ser impresa, mecanografiada o manuscrita, salvo la firma que, por su índole, tendrá que ser de esta última calidad.
• Firma: el Art. 1012 del Código Civil argentino dice que la firma es condición esencial para la existencia de todo acto bajo forma privada. La firma es el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad.

De esto se desprende que no puede sostenerse que un conjunto de claves pública-privada por la cual se encripta un documento digital constituye la "firma" que requiere nuestra legislación civil.

Aunque siempre queda la posibilidad que las partes, mediante un convenio de derecho privado, establezcan las características de un sistema informático por el cual se vincularán electrónicamente, la falta de generalidad de esta norma (ese convenio solo rige para el caso particular) y la inseguridad jurídica que sugiere el uso de medios no contemplados por la ley ha obstaculizado el desarrollo de esta nueva tecnología de firma digital.

Esos límites que impone la ley se solucionarían con una reforma integral de nuestro sistema de derecho privado que incorpore el mecanismo de firma digital equiparándolo a la firma tradicional.

La necesidad de un marco seguro de transmisión de la información fue puesta de manifiesto por primera ocasión en USA, concretamente en el Estado de UTAH en 1996. El éxito de esta iniciativa provocó su incorporación al Código de Comercio de USA (Uniform Comercial Code), que estableció las bases para que las relaciones comerciales pudieran desarrollarse en este marco. En 1997, a iniciativa de UNCITRAL se aprobó la Ley modelo de Comercio Electrónico, que ha servido de base al desarrollo normativo en este ámbito.

En Europa, la necesidad de establecer un marco seguro de comunicaciones vía electrónica se ha puesto de manifiesto en repetidas ocasiones. La Cumbre de Lisboa de Jefes de Estado y de Gobierno de marzo de 2002, consideró que la armonización del marco jurídico regulador del comercio electrónico y la seguridad en el mismo, era un pilar fundamental para la construcción de la economía de la Unión Europea. El proceso se inicia de modo estable con la aprobación de la Directiva 1999/93 del Parlamento Europeo y del Consejo, por la que se establece un marco jurídico comunitario para la firma electrónica. España, consciente de la necesidad de aprobar un marco jurídico básico regulador de los aspectos más urgentes de la materia, se anticipó a la citada Directiva, y publicó su RD. Ley 14/1999, de 17 de septiembre. En la actualidad se está desarrollando un nuevo Proyecto, que en principio no va a aportar novedades sustanciales, salvo en lo relativo al DNI electrónico.

Antes de analizar los aspectos más técnicos del funcionamiento de la firma electrónica, creo conveniente aclarar algunos puntos básicos de lo que se entiende por seguridad en las comunicaciones telemáticas. Existen cuatro grandes bloques normativos:

1º Seguridad Técnica, que permita obtener comunicaciones privadas, auténticas e íntegras Inter.-partes y que garantice que los sitesestán a salvo de piratas informáticos o "hackers".

2º Seguridad Jurídica, entendiendo por tal, un marco jurídico regulador de las eventuales responsabilidades que pueden dimanar de conductas o actos ilícitos a través de la red.

3º Seguridad mercantil o económica, que sería la aplicación del concepto anterior para garantizar un marco seguro de transacciones financieras a través de la red.

4º Seguridad a los consumidores, evitando el abuso de las grandes empresas de su posición de dominio y la utilización de cláusulas abusivas.

III.- ALGORITMOS

Los algoritmos más utilizados son:

El mecanismo más básico es el denominado criptosistema o algoritmo de encriptación, que define dos transformaciones:

La encriptación: conversión el texto en claro (plaintext) en el texto cifrado o criptograma (ciphertext) mediante el empleo de la denominada clave de encriptación; y

La desencriptación: proceso inverso que se emplea la llamada clave de desencriptación.

La aplicación más inmediata de un algoritmo de encriptación (aunque no la única) es asegurar el servicio de confidencialidad: la información transmitida no se podrá desencriptar sin el conocimiento de la clave de desencriptación.

La seguridad de un sistema de cifrado radica casi totalmente en la privacidad de las claves secretas. Por ello, los ataques que puede realizar un criptoanalísta enemigo están orientados a descubrir dichas claves.

La principal diferencia de los sistemas criptográficos modernos respecto a los clásicos está en que su seguridad no se basa en el

secreto del sistema, sino en la robustez de sus operadores (algoritmos empleados) y sus protocolos (forma de usar los operadores), siendo el único secreto la clave (los operadores y protocolos son públicos).

El cifrado es, en su forma más simple, hacer ininteligible un mensaje de modo que no pueda leerse hasta que el receptor lo descifre. El emisor utiliza un patrón algorítmico o clave, para cifrar el mensaje. El receptor tiene la clave de descifrado.

Existen dos tipos de clave que pueden utilizarse para el cifrado (así como para la firma digital y autenticación):

- Claves simétricas
- Claves asimétricas

Las claves simétricas siguen un modelo antiguo en que el emisor y el receptor comparten algún tipo de patrón. Por lo tanto, el mismo patrón lo utilizan el emisor para cifrar el mensaje y el receptor para descifrarlo.

El riesgo que implican las claves simétricas es que deberá buscar un método de transporte seguro para utilizarlo cuando comparta su clave secreta con las personas con las que desea comunicarse.

Con las claves asimétricas se crea una pareja de claves. La pareja de claves está compuesta de una clave pública y una clave privada, que son distintas entre sí. La clave privada contiene una parte mayor del patrón cifrado secreto de la clave pública.

Como emisor, podrá difundir su clave pública a cualquier persona con la que desee comunicarse de forma segura. De este modo, conserva la clave privada y la protege con una contraseña.

A diferencia de las claves simétricas, la clave privada y la clave pública no son iguales. Como resultado, el mensaje que se ha cifrado con una clave pública sólo puede ser descifrado por la persona que lo ha cifrado, ya que dicha persona es el único propietario de la clave privada.

Un protocolo como el protocolo SSL (Secure Sockets Layer) utiliza tanto el cifrado de claves públicas como el cifrado de claves simétricas. El cifrado de claves públicas se utiliza para el protocolo de conexión TCP/IP. Durante el protocolo de conexión, la clave maestra se pasa del cliente al servidor. El cliente y el servidor crean sus propias claves de sesión utilizando la clave maestra. Las claves de sesión se utilizan para cifrar y descifrar los datos del resto de la sesión.

Para enviar un mensaje con firma digital, por ejemplo, al texto se le hace un hashing: de un texto se genera un número más chico con un algoritmo, de tal forma que es casi imposible que de otro texto se cree el mismo número. Al resultado se lo encripta usando la clave privada: ésa es la firma digital, que se envía con el mensaje original.

El destinatario recibe el texto y la firma: primero hace su propio hashing del mensaje y luego, con la clave pública del emisor, desencripta la firma: si ambos mensajes son iguales, significa que el remitente es válido y que el mensaje no sufrió alteraciones en el trayecto de un lugar al otro. Todo este proceso es invisible para el usuario; la firma digital aparece como una cadena de caracteres.

Cifrado Simétrico o de Secreto Compartido

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico o de clave secreta. Estos sistemas son mucho más rápidos que los de clave pública, y resultan apropiados para el cifrado de grandes volúmenes de datos.

Su principal desventaja es que hace falta que el emisor y el receptor comparta la clave, razón por la cual se hace inseguro el envío de la clave, ya que de cualquier forma que ésta se envíe, es posible que alguien la intercepte.

Este tipo de cifrado se utiliza para encriptar el cuerpo de los mensajes en el correo electrónico o los datos intercambiados en las comunicaciones digitales.

Para ello se emplean algoritmos como:

Data Encryption Standard (DES)

DES fue el primer algoritmo desarrollado comercialmente y surgió como resultado de la petición del Departamento de Defensa de EE.UU. a IBM.

Es un cifrador en bloque que utiliza una clave de 64 bits de longitud (de los cuales 8 son de paridad) para encriptar bloques de 64 bits de datos. Debido al actual desarrollo tecnológico, la seguridad proporcionada por una clave de sólo 56 bits de longitud está siendo cuestionada, lo que ha llevado a la búsqueda de otros sistemas simétricos alternativos como el Triple-DES que utiliza una clave de 168 bits o el IDEA que usa una clave de 128 bits.

Métodos Asimétricos o de Clave Pública

La criptografía asimétrica usa dos claves, una para encriptar y otra para desencriptar, relacionadas matemáticamente de tal forma que los datos encriptados por una de las dos sólo pueden ser desencriptados por la otra. Cada usuario tiene dos claves, la pública y la privada, y distribuye la primera.

La desventaja de este método es su lentitud para encriptar grandes volúmenes de información. En comparación con los métodos simétricos es 100 veces más lento.

Estos algoritmos se pueden utilizar de dos formas, dependiendo de sí la clave pública se emplea como clave de encriptación o de desencriptación.

Algunos algoritmos de encriptación asimétrica son:

§ RSA (RIVEST-Shamir-Adelman)

§ DSA (Digital Signature Algorithm)

RSA

Este algoritmo fue inventado por R. Rivest, A. Shamir y L. Adleman (de sus iniciales proviene el nombre del algoritmo) en el Massachusetts Institute of Technology (MIT). RSA emplea las ventajas proporcionadas por las propiedades de los números primos cuando se aplican sobre ellos operaciones matemáticas La robustez del algoritmo se basa en la facilidad para encontrar dos números primos grandes frente a la enorme dificultad que presenta la factorización de su producto. Aunque el avance tecnológico hace que cada vez sea más rápido un posible ataque por fuerza bruta, el simple hecho de aumentar la longitud de las claves empleadas supone un incremento en la carga computacional lo suficientemente grande para que este tipo de ataque sea inviable. Sin embargo, se ha de notar que, aunque el hecho de aumentar la longitud de las claves RSA no supone ninguna dificultad tecnológica, las leyes de exportación de criptografía de EE.UU. imponen un límite a dicha longitud.

Digital Signature Algorithm (DSA)

Un algoritmo muy extendido es el Digital SignatureAlgorithm (DSA) definido en el Digital Signature Standard (DSS), el cual fue propuesto por el U.S. National Institute of Standards and Technology (NIST). Este algoritmo se basa en la función exponencial discreta en un campo de elementos finito, la cual tiene la característica de ser difícilmente reversible (logaritmo discreto).

Para aplicaciones únicamente de autenticación e integridad, no firma, se puede añadir una clave simétrica a la generación del resumen. De esta manera no es necesario encriptar, esta clave ya demuestra que el usuario es auténtico y el resumen propiamente demuestra la integridad del texto. El problema es utilizar una clave simétrica y, por lo tanto, se debe transmitir por un canal seguro, el sistema utilizado actualmente es el de claves de sesión encriptadas mediante la clave privada del emisor.

IV.- SEGURIDAD EN LA RED

La red informática, que es el medio por el cual se lleva a cabo el comercio electrónico, no brinda aún las garantías necesarias, para la protección de la información que por ella circula. Esto significa una gran desventaja para este medio, dado que la seguridad es un elemento imprescindible para las transacciones comerciales, tanto en lo que hace a su privacidad, como en confiabilidad. Esta situación ha llevado al estudio de los medios requeridos para la protección del comercio electrónico. En la actualidad se implementa la **CRIPTOGRAFÍA.**

¿Qué es la Criptografía con Clave Privada?

La criptografía con clave privada, es el método utilizado para el intercambio seguro de mensajes, por el cual las partes contratantes deben conocer la clave secreta que van a utilizar. El que envía el mensaje, lo encripta con la clave secreta y el que lo recibe, lo desencripta con la misma clave.

¿Cómo Funciona la Criptografía con Clave Privada (Simétrica)?

La criptografía con clave privada es el método por el cual, los mensajes han sido enviados a lo largo de los años. Y así funciona: Juan tiene una clave privada. Si Ana le quiere enviar a Juan un mensaje, deberán seguir los siguientes pasos:

- Juan le envía a Ana una copia de su clave privada.
- Ana encripta el mensaje con la clave privada de Juan.
- Juan desencripta el mensaje con su clave privada.

Este método acarrea algunos inconvenientes. Primero, Juan debe encontrar un medio seguro para hacerle llegar a Ana su clave privada. Si la clave es interceptada, todos los mensajes de Juan se van a ver comprometidos. Segundo, Juan necesita confiar en Ana. Si Ana es una doble agente, ella podría revelar la clave privada de Juan a sus enemigos o podría leer todos los mensajes privados de Juan imitándolo.

Limitaciones de la Criptografía con Clave Privada

La protección a la privacidad, mediante el uso de algoritmos simétricos, es relativamente simple en una red pequeña de trabajo, que requiere el intercambio de las claves secretas entre cada una de las partes. Pero cuando la red de trabajo se expande, el intercambio seguro de las claves secretas se torna extremadamente caro y dificultoso. Es así, que esta solución se vuelve insuficiente para aplicarse en grandes redes de trabajo.

Una mejor solución: Criptografía con Clave Pública

El problema de la autenticación y de la protección de la privacidad en extensas redes de trabajo, fue superado teóricamente en 1976, por Whitfield Diffie y Martin Hellman, cuando publicaron sus conceptos sobre el método para el intercambio de mensajes secretos sin intercambiar claves secretas. El método fue llevado a la práctica en 1977, bajo la denominación de la RSA Public Key Cryptosystem, por Ronald Rivest, Adi Shamir y Len Adleman. El nombre se debe a las siglas de los apellidos de sus creadores, quienes eran profesores del Instituto de Tecnología de Massachusetts.

Más que la utilización de una misma clave para encriptar y desencriptar un mensaje, el sistema RSA combina un par de claves para el encriptado y desencriptado. Cada una de las claves ejecuta una vía de transformación de las claves. Una implica la función inversa de la otra. Lo que una hace, sólo la otra puede deshacer.

¿Cómo funciona la Criptografía con Clave Pública?

Con la criptografía con clave pública, se han superado varios de los inconvenientes de la criptografía con clave privada (simétrica). En la criptografía con clave pública, un individuo o una organización tienen dos claves complementarias. Una llamada clave pública y otra llamada clave secreta. Cualquier información encriptada, utilizando una clave secreta, puede ser desencriptada únicamente utilizando la clave pública.

E inversamente, cualquier información encriptada utilizando una clave pública, puede solamente ser desencriptada utilizando la clave secreta.

Por ejemplo:

• Juan tiene dos claves complementarias.
• Una de las cuales encripta lo que la otra puede desencriptar.
• Juan mantiene una clave secreta (CLAVE PRIVADA).
• Juan convierte a la otra clave como disponible para el público (CLAVE PRIVADA).
• Ana necesita enviarle a Juan un mensaje.
• Juan le envía a Ana una copia de su clave pública.
• Ana encripta el mensaje con la clave pública de Juan.
• Juan desencripta el mensaje con su clave privada.

¿Cuáles son las Ventajas de Trabajar con este Sistema?

• Juan no tiene que preocuparse por su seguridad, enviándole a Ana su clave pública. Si alguien encuentra su clave pública, solamente van a poder utilizarla enviándole a Juan un mensaje privado. Pero no van a poder desencriptar los mensajes enviados por Juan o imitarlo a Juan. Entonces, Juan va a poder enviar a Ana su clave pública por medio de un e-mail. O la va a poder publicar en un directorio público.
• Juan no se tiene que preocupar por si Ana es una doble agente. Ana no va a poder interceptar los mensajes enviados a Juan, ni lo va a poder imitar.
• Juan va a poder firmar sus mensajes. Es la única persona que tiene su clave privada, si el encripta un mensaje con su clave privada, es equivalente a utilizar una firma digital.

La Clave Pública y los Certificados

Los certificados son documentos electrónicos, también llamados Digital Ids, a través de los cuales, una persona que necesita enviar un mensaje utilizando una clave pública, puede verificar, que esa clave pública pertenece a la persona a quien le va a mandar el mensaje.

Esto se lleva a cabo a través de una tercera parte confiable, llamada Autoridad Certificante.

Esta Autoridad Certificante, es la encargada y responsable, por la utilización, renovación, revocación y provisión de las direcciones para la obtención de los certificados digitales.

Un certificado digital contiene, el nombre de la organización o persona, algún otro dato identificatorio, su clave pública, la fecha del vencimiento, el nombre de la autoridad certificante proveedora de la ID, y una numeración.

La principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad de que la correspondiente clave privada es detentada por el firmante.

En términos sencillos, las firmas electrónicas son medios o métodos electrónicos que permiten atribuir un mensaje de datos a una persona determinada (lo que se denomina *función de identificación).* Tal es el caso de los passwords, los PIN (Personal Identification Numbers), el escaneo de la firma autógrafa, y otros.

Existe cierto tipo de firmas electrónicas que permite, además, la *privacidad* de la comunicación, y *la seguridad e integridad* del mensaje transmitido. Las firmas electrónicas que reúnen estas tres funciones (identificación, privacidad e integridad) son conocidas como firmas electrónicas *avanzadas.* Debe tenerse en cuenta que, en el estado actual de la tecnología, las únicas firmas electrónicas *avanzadas* son las llamadas firmas digitales (digital signatures), según la expresión extendida en la doctrina y en algunas leyes estadounidenses (Arizona Revised Statutes, Florida Electronic Signature Act, Illinois Electronic Commerce Security Act, Indiana Code Annotated Electronic Digital Signature Act, Iowa Electronic Commerce Security Act, Kansas Uniform Electronic Transactions Act, etc.).

Las firmas digitales son aquellas que se basan en la infraestructura de clave pública (criptosistemas de claves asimétricas o *PKI*). Como es bien sabido, la criptografía asimétrica recurre al juego de una clave privada, que es usada por el signatario para firmar y encriptar digitalmente un documento, y una clave pública, que se utiliza para verificar dicha firma y para desencriptar el mensaje.

Sin embargo, la gran dificultad del PKI consiste en determinar si la persona que utiliza dichas claves es realmente la persona que dice ser. Recuérdese que Internet es una red abierta, por lo que las personas que negocian entre sí no siempre tienen una relación previa de confianza.

El certificado digital resuelve este problema. Las autoridades de certificación son terceros de confianza (Trusted Third Parties o TTP) que distribuyen las claves pública y privada, y emiten un certificado digital en el que dan fe de la vinculación de dichas claves a una persona determinada. En algunos casos, estos certificados digitales contienen además sellos temporales, que prueban el momento de creación o envío del mensaje.

En otras palabras, la única forma para saber al día de hoy que un mensaje proviene de cierta persona determinada, que ha llegado completo, y que no ha sido visto por nadie más, es exigiendo la utilización de un sistema de firma electrónica avanzada y la exhibición de un certificado digital reconocido. Este es, a grandes rasgos, el fenómeno objeto de regulación en la Ley en comentario.

FIRMA ELECTRÓNICA, ENTIDADES DE CERTIFICACIÓN

I.- INTRODUCCIÓN

El tránsito del comercio tradicional al comercio electrónico nos introduce en un ambiente en el que la firma no sólo se hace prácticamente imposible sino que conspira contra la automatización de las actuaciones

Ello es más claro aún en el nuevo contexto del comercio electrónico abierto, basado en Internet, ya que, mientras el tráfico se realizó entre empresarios a través de redes cerradas, la utilización de éstas

implicó que los participantes pactaran previamente en soporte papel cómo se estructurarían las operaciones entre ellos. Por consiguiente, ambas partes disponían de una prueba de sus relaciones análoga a la emergente de negocios plasmados sobre papel.

En cambio, la actual contratación de bienes y servicios a través de redes informáticas y telemáticas facilita relaciones ocasionales entre las partes, sin necesidad de contactos previos. Ello apareja múltiples ventajas pero también encarta un conjunto de riesgos e incertidumbres ya que cualquier tercero puede "pinchar" la red e interceptar el tráfico electrónico que fluye a través de ella.

Como bien se ha destacado, los riesgos más importantes derivados de un intercambio de información a través de redes abiertas son: que el autor y fuente del mensaje sea suplantado; que el mensaje sea alterado, de forma accidental o de forma maliciosa, durante la transmisión; que el emisor del mensaje niegue haberlo transmitido o el destinatario haberlo recibido; y que el contenido del mensaje sea leído por una persona no autorizada.

Por lo tanto, desde el punto de vista jurídico, es necesario asegurar: que el mensaje proviene de la persona que se dice que lo envía; que no ha sido alterado en el camino; que el emisor no podrá negar su envío ni el destinatario su recepción; y, en su caso, garantizar su confidencialidad. La satisfacción de estas exigencias jurídicas se consigue con la aplicación de determinadas soluciones técnicas, que aportan los siguientes servicios de seguridad: la autenticación, que asegura la identidad del remitente del mensaje y permite asegurar que un mensaje procede de quien dice que lo envía; la integridad, que garantiza que el mensaje no ha sido alterado en el tránsito; el no rechazo o no repudio en origen y en destino, que garantiza que una parte interviniente en una transacción no pueda negar su actuación; y la confidencialidad, que protege los datos de revelaciones o accesos de terceros no autorizados

La función de la firma electrónica apunta precisamente a que las partes en un negocio electrónico puedan autenticar todos y cada uno de los mensajes que hayan intercambiado.

II.- CONCEPTO DE FIRMA

La Real Academia Española define la firma como el nombre y apellido, o título de una persona, que esta pone con rubrica al pie de un documento, escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido, o para obligarse a lo que en él se dice.

Dice nuestro Código Civil ": (...) La firma no es la simple escritura que una persona hace de su nombre o apellido; es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad".

III.- EVOLUCIÓN

En un comienzo, las manifestaciones de voluntad de las partes contratantes, se materializaban y asentaban, por medio del papel. Habiéndose arribado a un acuerdo, las partes confirmaban su contenido y aceptación a través de la firma.

A través de los años, las circunstancias fácticas, se han modificado por la incursión, cada vez mayor y en más ámbitos, (casi se podría decir que en todas las áreas), de la tecnología.

Es así, como hoy en día el tema de la firma requiere de nuevos estudios e investigaciones. Ya no alcanza con lo previsto por la doctrina, las legislaciones, los usos y costumbres respecto a la firma ológrafa. La tecnología requiere de nuevos preceptos, definiciones y alcances.

IV.- FIRMA DIGITAL Y FIRMA ELECTRÓNICA

El flujo comercial llevado a cabo por medios electrónicos, presenta particularidades, que plantean la necesidad, de establecer el medio a través del cual, las partes contratantes, van a expresar su conformidad, tanto en el contenido del contrato como a la sujeción del mismo; y a la vez, que brinde seguridad con respecto a su autenticidad y a la identidad del suscriptor, de esto se trata la

FIRMA DIGITAL

La firma digital, funciona para los documentos electrónicos, como la firma ológrafa lo hace en el papel. Se trata de una infranqueable pieza de datos, por la cual queda asegurada tanto la identidad de la persona que lo ha suscrito, como el contenido del documento mismo, en el cual la firma ha sido estampada.

En la actualidad, la firma digital, provee un mayor grado de seguridad, que la firma ológrafa. El receptor de un mensaje firmado digitalmente, puede verificar que el mensaje proviene de la persona que lo ha firmado y que el mismo no ha sido alterado, sea accidentalmente o intencionalmente, desde que ha sido firmado. Y más aún, la persona que ha firmado un documento digitalmente no va a poder renegar de él sosteniendo que la misma ha sido falsificada.

Para entender el funcionamiento de la firma digital, se dará el siguiente ejemplo:

Ana quiere enviarle un mensaje a Juan. Ella crea el mensaje electrónico, utilizando una *hash function,* sobre el mismo. Esto será como una "huella digital" para el mensaje. Si ninguna parte del mensaje es modificado, la *hash function,* nos dará un resultado que nos indica la correcta emisión del mismo. Ana encriptó su mensaje digital con una clave privada. Este mensaje digital encriptado, es la firma digital del mensaje. Ana le envía a Juan los dos, el mensaje y la firma digital. Cuando Juan los recibe, desencripta la firma utilizando la clave pública de Ana, la cual le va a revelar, el mensaje digital. Para verificar el mensaje, Juan va a mezclarlo con la misma *hash function,* utilizada por Ana. Si resulta ser equivalente, Juan va a poder confiar en que el mensaje realmente proviene de Ana, y que no ha sido alterado, desde que el mismo fue firmado. Si el mensaje es diferente, entonces el mismo se originó en algún otro lugar, o fue alterado luego de su firma.

V.- ¿QUÉ ES UNA FIRMA ELECTRÓNICA?

(Ver Anexo 9)

Para definir a la llamada firma electrónica, es necesario determinar qué le agrega al concepto clásico de "firma" la calificación de "electrónica".

En tal sentido, en el Derecho positivo, se ha definido a la "firma" como el "trazado gráfico, conteniendo habitualmente el nombre, apellido y rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y obligarse con lo que en ellos se dice" Así, en la ley de cheques establece que "Toda firma debe contener el nombre y apellido del que se obliga". Y agrega: "También es válida la suscripción en la cual el nombre sea abreviado o indicado solamente con una inicial. Debajo o a lado de la firma se agregará el nombre del librador estampado o manuscrito, con caracteres de imprenta". Reglamento Notarial prevé que "La firma deberá comprender el nombre y apellido o apellidos de uso habitual por el firmante y la rúbrica. Los otorgantes, testigos, intérpretes o lectores a ruego firmarán sólo con iniciales o con el apellido o apellidos que usen, o con grafías ilegibles, si es que así lo hacen habitualmente".

A partir de tal caracterización doctrinaria y positiva, bien se ha dicho que la firma se puede componer del nombre y apellido de la persona y eventualmente de su rúbrica, o bien puede consistir en otro "trazado gráfico" o en "iniciales" o en "grafías ilegibles". Lo que se requiere es la nota de habitualidad como elemento vinculante de esa grafía con su autor. Igualmente, se ha planteado la interrogante de si la firma tiene que ser siempre autógrafa u ológrafa, es decir, puesta de puño y letra por el firmante, respondiéndose que la firma autógrafa no es la única manera de firmar ya que hay otros mecanismos que no son la firma autógrafa pero que constituyen "trazados gráficos" que dan autoría y obligan, como es el caso de las claves, los códigos, los signos y, en algunos casos, los sellos. Se concluye que la firma no es un elemento esencial del documento sino que atañe a su eficacia y valor probatorio.

En la medida que la firma puede realizarse por medio de signos, códigos, claves u otros elementos similares, puede decirse que la expresión "firma electrónica" en sentido amplio, alude a "cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una

parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones de la firma manuscrita".

Tal caracterización recoge el llamado criterio del "equivalente funcional" plasmado, por ejemplo, en la Ley Modelo sobre Comercio Electrónico, confeccionada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI). Al tenor de su Art. 7°, se prevé que "Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y b) si ese método es tan fiable como sea apropiado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente".

Una especie de firma electrónica es la firma digital, entendida como aquella que se crea usando un sistema de criptografía asimétrica o de clave pública.

La criptografía es la ciencia que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlas en su forma original. Generalmente, utiliza un algoritmo matemático para cifrar datos con el fin de hacerlos incomprensibles para cualquiera que no posea su clave, o sea, la información secreta necesaria para descifrar los datos cifrados.

La criptografía puede ser simétrica (o de clave secreta) y asimétrica (o de clave pública).

En el primer caso, en el proceso de cifrado y descifrado, las partes deben compartir una clave común previamente acordada. Dicha clave debe ser secreta para impedir el acceso no autorizado por terceros, por lo que la protección de la clave es esencial. Si bien la criptografía de clave secreta es un medio idóneo de autenticación entre las partes, presenta el inconveniente del intercambio de claves entre ellas ya que si se realiza en redes abiertas, existe la posibilidad de vulneración o interceptación.

Además, el sistema no sirve frente a terceros que carezcan de la clave.

En el segundo caso, es decir, el de la criptografía asimétrica, el sistema se basa en el uso de un par de claves asociadas: una clave privada en poder del titular, conocida únicamente por éste o aún desconocida por éste (si se mantiene en una tarjeta inteligente a la que se accede mediante un número de identificación personal o un dispositivo de identificación biométrica); y una clave pública, que se relaciona matemáticamente con la clave privada, y que puede ser accesible para cualquiera. Así, mediante el uso de la clave pública del destinatario, el remitente puede estar seguro de que sólo el destinatario, poseedor de la clave privada correspondiente, podrá descifrar su mensaje.

Conforme a lo indicado, cuando una parte desea verificar la firma digital generada por otra, la parte verificadora necesita tener acceso a la clave pública del firmante con la seguridad de que se corresponde realmente con la clave privada del firmante. Igualmente, necesita la clave pública del destinatario el emisor de un mensaje que desea cifrarlo. Ambos son usuarios de claves públicas: quien desea verificar una firma digital, y quien desea emitir un mensaje cifrado.

La accesibilidad a las claves públicas puede satisfacerse mediante la simple distribución manual (intercambiando papeles firmados o disquetes que contienen las claves públicas respectivas) pero tal sistema no se compadece con las exigencias del comercio electrónico de ámbito mundial.

Para superar tal dificultad, la distribución de claves públicas se ha implementado a través de tres vías diferentes, a saber:

a) El registro de claves públicas;
b) El llamado "web-of-trust"; y
c) La intervención de terceras partes de confianza o autoridades

Como hemos visto la seguridad es uno de los elementos clave en el desarrollo positivo de las redes de información mundial y

particularmente en el comercio electrónico, ésta genera confianza, y hace que los usuarios al depositar sus datos en la red, estén seguros de que no serán alterados ni desviados a usuarios no autorizados.

Entonces podemos definir a la firma electrónica como aquél conjunto de datos, códigos o claves criptográficas privadas, en forma electrónica, que se asocian inequívocamente a un documento electrónico (es decir, contenido en un soporte magnético -disquete o disco duro de un ordenador- y no de papel), que permite identificar a su autor. Cuando esta identificación es altamente fiable y permite detectar cualquier alteración del documento no autorizada merced a que los dispositivos empleados en la creación de la firma son seguros, por cumplir ciertas exigencias técnicas, y porque el Prestador de Servicios de Certificación que ha intervenido esta "acreditado", entonces se habla de "firma electrónica avanzada".

Otro concepto: "La firma electrónica es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge".

Nuestra legislación define a la firma en el Art. 13, manifiesta: "son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos"[3].

La firma electrónica tiene la misma validez y se le reconocen los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y es admitida como prueba en caso de juicio, según lo estipula el Art. 14 de la ley de comercio electrónico.

[3] Ibídem, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

La firma electrónica tiene los siguientes requisitos, que lo estipula el Art. 15 de LCE:

"Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular;
b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y,
e) Que la firma sea controlada por la persona a quien pertenece".

La Ley en el Titulo Segundo, en cuatro capítulos tipifica los siguientes temas:

a) De las Firmas Electrónicas Certificados de Firma Electrónica

Se define a la Firma Electrónica como: "(...) los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos" (Art. 13),

Aclarando el concepto en el Art. 16.- "La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las

obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la ley".

Validez de la Firma Electrónica

Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular,
b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,
e) Que la firma sea controlada por la persona a quien pertenece. (Art. 15 LCE)

Obligaciones del titular de la Firma Electrónica

El titular de la firma electrónica deberá:

a) Cumplir con las obligaciones derivadas del uso de la firma electrónica;
b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
d) Verificar la exactitud de sus declaraciones;
e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia,

f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
g) Las demás señaladas en la ley y sus reglamentos. (Art. 17 LCE)

Duración y Extinción

La duración de la firma electrónica es indefinida, podrán ser revocadas, anuladas o suspendidas.

La firma electrónica se extinguirá por:

a) Voluntad de su titular,
b) Fallecimiento o incapacidad de su titular;
c) Disolución o liquidación de la persona jurídica, titular de la firma; y,
d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso. (Art. 19 LCE)

Los Certificados de Firma Electrónica

Se refiere al mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad. (Art. 20 LCE)

Cumple los siguientes requisitos:

a) Identificación de la entidad de certificación de información,
b) Domicilio legal de la entidad de certificación de información;
c) Los datos del titular del certificado que permitan su ubicación e identificación;
d) El método de verificación de la firma del titular del certificado;
e) Las fechas de emisión y expiración del certificado;
f) El número único de serie que identifica el certificado;
g) La firma electrónica de la entidad de certificación de información;
h) Las limitaciones o restricciones para los usos del certificado; e,
i) Los demás señalados en esta ley y los reglamentos. (Art. 22 LCE)

La Duración se establecerá en el reglamento que aun no se puede suspender, extinguir y revocar conforme a las pautas establecidas en la Ley.

Se establece el reconocimiento internacional de certificados de firma electrónica.

VI.- DIFERENCIA ENTRE FIRMA ELECTRÓNICA Y FIRMA DIGITAL

La firma electrónica es un género, caracterizado por el soporte: todo modo de identificación de auditoría basado en medios electrónicos es firma; luego vienen las especies, que en general, se caracterizan por agregar elementos de seguridad que la sola firma electrónica no posee. Las legislaciones reconocen el género de la firma electrónica y luego eligen una especie que denominan "firma electrónica avanzada" o "firma digital", que es la que utiliza un sistema, generalmente criptográfico, que da seguridad. La gran diferencia estriba en que cuando se utiliza la firma digital se aplican presunciones *iuris tantum* sobre la identidad del firmante y la integridad del documento que firmó.

Elementos de la Firma Digital

Independientemente de la criptografía, la firma digital se caracteriza por los siguientes elementos:

Elemento objetivo-soporte: En un sentido negativo, el soporte no es escrito y no hay una elaboración manual del autor. En un sentido positivo, la firma es cualquier símbolo o procedimiento de seguridad usado por una persona que incluye medios electrónicos, digitales, magnéticos, ópticos o similares. Puede advertirse, entonces, que la firma electrónica no necesariamente debe ir anexa a un documento, como ocurre en el caso de la firma ológrafa.

Elemento subjetivo: Los símbolos asentados en medios electrónicos tienen un propósito específico: se hacen para identificar a la persona e indicar su aprobación del contenido de un mensaje electrónico.

Con estos dos elementos hay firma electrónica pero no firma digital, pues para que se le asigne los efectos de presunción se requiere más seguridad.

Esfera de control del titular: Siendo un elemento de imputación de autoría, es lógico que se requiera que esté bajo el control del titular, ya que sólo él es quien decide qué declaraciones de voluntad son suyas. Por ello, es necesario que la firma pertenezca únicamente a su titular y se encuentre bajo su control exclusivo.

Derechos de verificación del receptor: Es necesario que los sistemas utilizados puedan ser verificados por el receptor para asegurarse de la autoría.

VII.- EXPLICACIÓN DEL USO DE FIRMA ELECTRÓNICA

Expliquemos a continuación como utilizamos la firma electrónica.

Debemos contar con un computador con conexión con Internet y con un dispositivo lector de tarjetas de firma electrónica.

A continuación debemos acudir a un Prestador de Servicios de Certificación, que procederá a nuestra identificación personal. Tras ello generará nuestras claves, pública y privada, y nos entregará la tarjeta o disquete que contenga esta clave privada, así como la aplicación informática o programa necesario para su uso, que se ha de instalar en nuestro ordenador. Con ello ya estamos listos para la firma de un documento o archivo que hayamos creado, el cual podremos además encriptar, y lo enviaremos por correo electrónico a su destinatario, junto con el certificado de nuestro Prestador en el que se avala nuestra identidad.

La clave privada (secreta), generalmente, según hemos indicado se encuentra incorporada en tarjetas inteligentes, similares a las de crédito, que incorporan un chip que contiene información de su titular, la entidad que la ha emitido y el conjunto de bits en qué consiste la clave.

Estas tarjetas son de uso personal e intransferible por estar protegida por un código secreto que sólo su titular conoce.

Dentro de la categoría genérica de firma electrónica, es necesario hacer una subdivisión entre firma electrónica en general y firma electrónica segura, refrendada o firma digital. Esta distinción tiene su origen en la cifra de la firma electrónica, en la tecnología que se ha aplicado para poder calificar a la firma como segura o no. Además, tiene repercusiones posteriores, puesto que la legislación prima a las firmas digitales o firmas electrónicas seguras (tanto a nivel internacional como nacional).

La diferencia principal entre ambos tipos de firma, radica en el sistema criptográfico que se ha utilizado: para las firmas electrónicas en general se utilizan un sistema criptográfico simétrico o de clave secreta; mientras que para la firma digital el método utilizado es asimétrico o de clave pública.

Una firma digital es una cadena de datos creada a partir de un mensaje, o parte de un mensaje, de forma que sea imposible que quién envía el mensaje reniegue de él (repudio) y que quien recibe el mensaje pueda asegurar que quién dice que lo ha enviado es realmente quien lo ha enviado, es decir, el receptor de un mensaje digital puede asegurar cual es el origen del mismo (autenticación). Así mismo, las firmas digitales pueden garantizar la integridad de los datos (que no se hayan modificado los datos durante la transmisión).

Los sistemas de clave pública permiten además cumplir los requisitos de integridad del mensaje, autenticación y no repudio del remitente utilizando **firmas digitales**. El procedimiento de firma digital de un mensaje consiste en extraer un **"resumen"** *(o hash en inglés)* del mensaje, cifrar este resumen con la clave privada del remitente y añadir el resumen cifrado al final del mensaje. A continuación, el mensaje más la firma (el resumen cifrado) se envían como antes cifrados con la clave pública del destinatario. El algoritmo que se utiliza para obtener el resumen del mensaje debe cumplir la propiedad de que cualquier modificación del mensaje original, por pequeña que sea, dé lugar a

un resumen diferente. (Nótese que la firma digital de un usuario no es siempre la misma secuencia de bits, sino que depende del mensaje firmado.).

El proceso de firma es el siguiente:

• El usuario prepara el mensaje a enviar.
• El usuario utiliza una función hash segura para producir un resumen del mensaje.
• El remitente encripta el resumen con su clave privada. La clave privada es aplicada al texto del resumen usando un algoritmo matemático. La firma digital consiste en la encriptación del resumen.
• El remitente une su firma digital a los datos.
• El remitente envía electrónicamente la firma digital y el mensaje original al destinatario. El mensaje puede estar encriptado, pero esto es independiente del proceso de firma.
• El destinatario usa la clave pública del remitente para verificar la firma digital, es decir para desencriptar el resumen adosado al mensaje.
• El destinatario realiza un resumen del mensaje utilizando la misma función resumen segura.
• El destinatario compara los dos resúmenes. Si los dos son exactamente iguales el destinatario sabe que los datos no han sido alterados desde que fueron firmados.

(Ver Anexo 10)

Cuando el destinatario recibe el mensaje, lo descifra con su clave privada y pasa a comprobar la firma. Para ello, hace dos operaciones: por un lado averigua la clave pública del remitente y descifra con ella el resumen que calculó y cifró el remitente. Por otro lado, el destinatario calcula el resumen del mensaje recibido repitiendo el procedimiento que usó el remitente. Si los dos resúmenes (el del remitente descifrado y el calculado ahora por el destinatario) coinciden, la firma se considera válida y el destinatario puede estar seguro de la integridad del mensaje: si el mensaje hubiera sido alterado a su paso por la red, el resumen calculado por el destinatario no coincidiría con el original calculado por el remitente.

Además, el hecho de que el resumen original se ha descifrado con la clave pública del remitente prueba que sólo él pudo cifrarlo con su clave privada. Así el destinatario está seguro de la procedencia del mensaje (autenticación del origen) y, llegado el caso, el remitente no podría negar haberlo enviado (no repudio) ya que sólo él conoce su clave secreta.

Los inconvenientes de este sistema son la lentitud de los algoritmos de clave asimétrica (típicamente varias veces más lentos que los de clave simétrica) y la necesidad de las autoridades de certificación ya mencionadas.

Las funciones Hash sirven para comprimir un texto en un bloque de longitud fija. Se utilizan en autenticación y firma digital para:

1. No tener que encriptar todo el texto en los servicios de autenticación y firma digital, ya que este proceso es lento con los algoritmos asimétricos. El resumen sirve para comprobar si la clave privada del emisor es auténtica, no es necesario encriptar todo el texto si no se quiere confidencialidad.
2. Para poder comprobar automáticamente la autenticidad. Si se encripta todo el texto, al desencriptar sólo se puede comprobar la autenticidad mirando si el resultado es inteligible, evidentemente este proceso debe realizarse de forma manual.

Utilizando un resumen del texto, se puede comprobar si es auténtico comparando el resumen realizado en el receptor con el desencriptado.
3. Para comprobar la integridad del texto, ya que si ha sido dañado durante la transmisión o en recepción no coincidirá el resumen del texto recibido con la desencriptación.

(Ver Anexo 11)

Las funciones Hash son públicas e irreversibles. No encriptan, sólo comprimen los textos en un bloque de longitud fija. Son diferentes de

las funciones clásicas de compresión de textos, como ZIP, Huffman, V-42, etc., estas funciones son reversibles e intentan eliminar la redundancia de los textos manteniendo el significado. Las funciones Hash no son reversibles, es decir, no se puede recuperar el texto desde el resumen, pero deben cumplir las siguientes condiciones:

1. Transformar un texto de longitud variable en un bloque de longitud fija.
2. Ser irreversibles.
3. Conocido un mensaje y su función Hash debe ser imposible encontrar otro mensaje con la misma función Hash. Esto se debe cumplir para evitar que los criptoanalistas firmen un mensaje propio como si fueran otra persona.
4. Es imposible inventar dos mensajes cuya función Hash sea la misma.

(Ver Anexo 12)

ENTIDADES DE CERTIFICACIÓN Y CERTIFICADOS ELECTRÓNICOS

Entidades de Certificación de Información

Son las empresas unipersonales o personas jurídicas que emiten

Certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.

Son obligaciones de las entidades de certificación de información acreditadas:

a) Encontrarse legalmente constituidas, y estar registradas en el Consejo Nacional de Telecomunicaciones;
b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;

c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información;
d) Mantener sistemas de respaldo de la información relativa a los certificados;
e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en esta ley;
f) Mantener una publicación del estado de los certificados electrónicos emitidos;
g) Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;
h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados; e,
i) Las demás establecidas en esta ley y los reglamentos. (Art. 30 LCE)

Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información. (Art. 31 LCE)

Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley. (Art. 32 LCE)

b) Organismos de Promoción de los servicios electrónicos

El Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior. (Art. 36 LCE)

El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas. (Art. 37 LCE)

La Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas. (Art. 38 LCE).

Como anexo adjunto el Instructivo para el procedimiento administrativo sancionador de la superintendencia de telecomunicaciones -SUPERTEL- Resolución ST-2012-0026

Infracciones administrativas:

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos, clasifica a las infracciones en Leves y Graves y se establecen las siguientes sanciones:

La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

a) Amonestación escrita;
b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;

c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y,
d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica. (Art. 41 LCE)

El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones. (Art. 43 LCE)

Instructivo para el procedimiento administrativo sancionador de la superintendencia de telecomunicaciones -SUPERTEL- Resolución ST-2012-0026.

Capítulo I. ÁMBITO, OBJETO Y PRINCIPIOS FUNDAMENTALES.

Art. 1.- El presente instructivo tiene por objeto normar la sustanciación del procedimiento administrativo sancionador, para el ejercicio de la potestad sancionadora atribuida constitucional y legalmente a esta Superintendencia, respecto de las materias normadas conforme a la Ley Especial de Telecomunicaciones; la Ley de Radiodifusión y Televisión; la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; sus reglamentos generales; demás normativa infralegal establecida en: decretos, regulaciones emitidas por el Consejo Nacional de Telecomunicaciones, por el Consejo Nacional de Radiodifusión y Televisión, extinguido, en lo que estuvieren vigentes; y, en los diversos títulos habilitantes, autorizaciones o condiciones generales. Se aplicará a los procedimientos contemplados en contratos de concesión vigentes, en lo que sea compatible.

TTP.

Según se ha destacado con acierto, "tercera parte de confianza (trusted third party o TTP) es cualquier entidad de confianza de las partes intervinientes en una transacción para proporcionar servicios de

seguridad; aquella específica tercera parte de confianza que desempeña de forma fundamental la función de emisión de certificados se conoce, entre otras expresiones, como autoridad de certificación, entidad de certificación, proveedor o prestador de servicios de certificación o simplemente certificador. Como un juego de claves usado para crear una firma digital no tiene una asociación intrínseca con nadie, la solución es que una o más terceras partes, de confianza para las dos primeras partes, certifiquen la persona realmente asociada con un par de claves. La criptografía necesita pues, de una tercera parte de confianza: una entidad de certificación que debe realizar tal asociación vinculando una persona debidamente identificada con un par de claves determinadas. Por ello, para asociar un par de claves con un potencial firmante, una entidad de certificación emite un certificado, un registro o documento electrónico que liga una clave pública con el sujeto del certificado, y confirma que el potencial firmante identificado en el certificado tiene la correspondiente clave privada".

De lo dicho se desprende que la principal función del certificado es asociar (directamente) la identidad de una persona determinada a una clave pública concreta e (indirectamente) a una clave privada. Así, el destinatario de un certificado que desee comprobar la firma digital creada por la persona que consta como titular del certificado puede usar la clave pública incluida en el mismo para verificar que la firma digital fue creada con la correspondiente clave privada. Tal verificación ofrece una razonable seguridad de que la correspondiente clave privada es poseída por la persona mencionada en el certificado, y que la firma digital fue creada por esa persona determinada.

Quiere decir que el certificado es un documento electrónico que contiene un conjunto de información que vincula una clave pública con una persona o entidad determinada.

Consecuentemente, el sistema de certificados de clave pública supone la participación de los siguientes sujetos:

a) La entidad de certificación;

b) El titular del certificado; y
c) El usuario o persona que confía en el certificado.

Por lo que refiere a la entidad de certificación, es una institución dedicada a proveer servicios de certificación mediante la emisión de certificados firmados digitalmente por dicha autoridad, usando una clave privada de firma.

En cuanto a su naturaleza, el Derecho comparado exhibe casos en los que se ha optado porque sean privadas y casos en los que se ha preferido darles un estatuto de Derecho público, distinguiéndose en esta última alternativa entre las que certifican al resto de las entidades de certificación privadas y las que se limitan a certificar las relaciones entre la Administración y los administrados.

Por otra parte, las entidades certificadoras pueden constituirse libremente o requerir de un acto de autorización por parte de un órgano estatal. De todos modos, es valor generalmente aceptado que deben reunir unos requisitos mínimos indispensables de carácter técnico, referidos a su personal, de solvencia, de fiabilidad, y referentes a planes de contingencia, entre otros.

En cuanto al titular del certificado, también llamado sujeto o suscriptor, es la persona o entidad incluida en el certificado, que tiene legítimamente la clave privada correspondiente a la clave pública que contiene el certificado.

La relación del titular del certificado con la entidad de certificación puede ser de dos tipos, según responda a una comunidad cerrada (en que exista alguna vinculación entre la entidad certificadora y los suscriptores) o abierta (en que la entidad certificadora es independiente de los suscriptores).

Finalmente, el usuario del certificado es la persona que obtiene la clave pública del suscriptor a través del certificado y que actúa basándose en él y en la clave pública que contiene.

Ordinariamente, lo que se ha llamado el "ciclo vital" del certificado, reconoce tres aspectos principales: la generación y emisión, la distribución y la vigencia del mismo.

En primer lugar, en cuanto a la emisión del certificado, cabe distinguir las siguientes fases:

a) Solicitud y registro del solicitante;
b) Comprobación de la solicitud;
c) Emisión del certificado;
d) Envío de copia al solicitante y, en su caso, aceptación por éste; y,
e) Publicación y archivo del certificado.

En segundo lugar, por lo que refiere a la distribución del certificado, ella se verifica a través de una serie de sistemas tendientes a posibilitar la verificación de una firma digital de una parte lejana o a cifrar datos de una persona destinados a una parte lejana, mediante la comunicación de la clave pública correspondiente.

En tercer lugar, la cuestión de la vigencia del certificado se relaciona con el hecho de que el certificado, como instrumento de distribución segura de claves públicas, no puede tener una validez indefinida, sin perjuicio de la eventual revocación anticipada o suspensión del mismo si mediaren razones que así lo impusieren.

(Ver Anexo 13)

DERECHO COMPARADO

El tema de la firma electrónica ha sido objeto de específica regulación en muchos países en los últimos años, comenzando por aquellos donde el desarrollo del comercio electrónico obligó a incorporar soluciones concretas al Derecho positivo.

En los Estados Unidos, corresponde destacar, como ejemplo pionero, el caso de la "Utah Digital Signature Act" de febrero de 1995, revisada en marzo de 1996, la cual consta de cinco partes.

La primera de ellas trata de la interpretación de la ley y enuncia los siguientes propósitos:

a) Facilitar el comercio por medio de mensajes electrónicos confiables;
b) Minimizar la incidencia de falsificaciones de firmas digitales y fraudes en el comercio electrónico; y
c) Establecer reglas uniformes relacionadas con la autenticación y confiabilidad de los mensajes electrónicos.

También contiene una serie de definiciones, entre las que se encuentran las de "sistema de criptografía asincrónica", "par de claves" y "firma digital".

Se entiende por sistema de criptografía asincrónica un algoritmo o serie de algoritmos que proveen un par de claves seguras. El par de claves se define como una clave privada y su correspondiente clave pública en un sistema de criptografía asincrónica, que tiene la propiedad de que la clave pública puede verificar la firma digital que la clave privada ha creado. Firma digital significa, en el concepto que aporta la ley, la transformación de un mensaje usando un sistema de criptografía asincrónica tal que una persona, teniendo el mensaje inicial y la clave pública del firmante, puede determinar con precisión si la transformación ha sido creada usando la clave privada que corresponde a la clave pública, y si el mensaje ha sido alterado desde que se ha hecho la transformación.

La segunda parte trata sobre la concesión de licencias y la regulación de las autoridades certificantes, estableciendo los requisitos que deben reunir quienes aspiren a desempeñarse en tal carácter.

La tercera parte se ocupa de los deberes de las autoridades certificantes y del contenido de los certificados.

La parte cuarta regula los efectos de la firma digital disponiendo que donde una regla legal requiere una firma o prevé ciertas consecuencias en su ausencia, esta regla será satisfecha por una firma digital si está

verificada como referida a una clave pública contenida en un certificado válidamente extendido por una autoridad certificante, o si esa firma digital ha sido estampada por el firmante con la intención de firmar el mensaje.

La quinta parte refiere a los servicios estatales de archivo de claves públicas y los requisitos que deben reunir.

En Europa, Italia fue el primer país en regular normativamente sobre la firma digital, a través del "Regolamentocontenentemodalitá di applicazionedell' artícolo 15, comma 2, dellalege 15 marzo 1997, N° 59, in formazione, archivazione e trasmissione di documenti con strumentiinformatici e telematici".

El Art. 1° de dicho Reglamento establece los conceptos de "firma digital", "par de claves asimétricas", "clave privada" y "certificado", entre otros. El Art. 2° establece la validez y eficacia del documento electrónico. El Art. 11 dispone que los contratos concluidos por medios informáticos y transmitidos con instrumentos telemáticos son válidos y efectivos si están firmados usando firma digital, y el art. 16 contempla un sistema de firma digital autenticada.

A diferencia de la ley de Utah, el Reglamento italiano bajo examen no regula las terceras partes de confianza, limitándose a definirlas como sujetos públicos o privados que certifican y guardan las claves públicas de firma por diez o más años.

En Alemania rige la ley aprobada el 13 de junio de 1997, con la cual, a través de un texto breve y conciso, se procura la creación de condiciones generales para el uso seguro de la firma digital.

De acuerdo a su Art. 2°, se define a la firma digital como "un sello creado con una clave privada de firmas sobre información digital que permite, mediante el uso de la clave pública asociada rotulada por un certificado de clave de un certificador, (...) que sean verificados el propietario de la clave de firma y el carácter de no falsificada de la

información". En su mérito, se regula minuciosamente la actuación de una autoridad de certificación, que da fe de la atribución de claves públicas (Art. 3° y sigtes.).

En Portugal, el decreto-ley N° 290-D/99 de 2 de agosto de 1999 procura, a través de 41 artículos, la regulación de la validez, eficacia y valor probatorio de los documentos electrónicos y de la firma digital, sin perjuicio de su extensión a otras formas de firma electrónica que satisfagan exigencias de seguridad idénticas a las de la firma digital.

Tras establecer las definiciones básicas (Art. 2°) y regular la fuerza probatoria de los documentos electrónicos y la firma digital (Art. 3°), regula el régimen jurídico de las firmas digitales (Arts. 7° y 8°) y la actividad de certificación, tanto en su vertiente subjetiva (relativa a las entidades certificadoras: Arts. 10 a 28 y 33 a 37) como objetiva (referente a los certificados: Arts. 29 a 33).

En España se ha aprobado el decreto-ley N° 14/1999 de 17 de setiembre de 1999, el cual se estructura en cinco títulos que refieren respectivamente a Disposiciones generales, Prestación de servicios de certificación, Dispositivos de firma electrónica y evaluación de su conformidad con la normativa aplicable, Tasa por el reconocimiento de acreditaciones y certificados, e infracciones y sanciones.

Conforme a esta normativa, se distingue entre firma electrónica y firma electrónica avanzada (Art. 2°, Lits. a y b). La primera se define como "el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge", en tanto que la segunda "es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos".

En materia de certificación de firmas, se prevé que la prestación de dicho servicio "no está sujeta a autorización previa y se realiza en régimen de libre competencia" (Art. 4º). En cuanto a los certificados (entendidos como registros electrónicos que atestiguan que una clave pública pertenece a determinado individuo o entidad), el Art. 8º exige los siguientes requisitos principales:

a) La indicación de que se expide como tal;
b) El código identificativo único del certificado;
c) La identificación del prestador del servicio de certificación;
d) La firma electrónica avanzada del prestador del servicio de certificación;
e) La identificación del signatario;
f) Los datos de verificación de firma equivalentes a aquellos de creación de firma;
g) El plazo de validez del certificado; y
h) Los límites de uso del certificado y del valor de las transacciones para las que puede utilizarse, si se establecen.

Respecto a los prestadores de servicios de certificación, junto con las eventuales responsabilidades civil y penal en que pueden incurrir, la norma prevé asimismo la responsabilidad administrativa, disciplinada en el Título V, Infracciones y sanciones, en el cual se clasifican las infracciones en muy graves, graves y leves (Arts. 24 y 25), se prevén las sanciones aplicables (Art. 26), se contempla la adopción de medidas cautelares específicas (Art. 27), y se fijan las bases del procedimiento sancionador (Art. 28).

Evidentemente, las exigencias de la globalización del comercio electrónico imponen la necesidad de normas uniformes y generales, lo que explica el esfuerzo actual por adoptar normas comunitarias en el ámbito de los espacios integrados, así como esfuerzos de uniformización encarados por organismos internacionales, tales como la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI).

GUÍA ACADÉMICA DE LA FIRMA ELECTRÓNICA

REAFIRMANDO LOS CONCEPTOS

Cuando hablamos de firma digital en realidad nos estamos refiriendo a muchos conceptos relacionados, entre los cuales figuran documentos electrónicos, claves criptográficas, certificados digitales, funciones matemáticas, autoridades certificantes, infraestructuras de clave pública y muchos otros nombres que pueden resultarnos complicados o desconocidos.

Las siguientes preguntas intentan aclarar estos términos:

¿Qué es la firma digital?

La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, permitiendo que éstos gocen de una característica que únicamente era propia de los documentos en papel.

Una firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. 1

La firma digital no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

La firma digital es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

¿Cómo funciona?

La firma digital funciona utilizando complejos procedimientos matemáticos que relacionan al documento firmado con información

propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse que los contenidos no han sido modificados.

El firmante genera, mediante una función matemática, una huella digital del mensaje. Esta huella digital se cifra con la clave privada del firmante, y el resultado es lo que se denomina firma digital la cual se enviará adjunta al mensaje original. De esta manera el firmante va a estar adjuntando al documento una marca que es única para ese documento y que sólo él es capaz de producir.

Para realizar la verificación del mensaje, en primer término el receptor generará la huella digital del mensaje recibido, luego descifra la firma digital del mensaje utilizando la clave pública del firmante y obtendrá de esa forma la huella digital del mensaje original; si ambas huellas digitales coinciden, significa que el mensaje no fue alterado y que el firmante es quien dice serlo.

¿Claves privadas y claves públicas?

En la elaboración de una firma digital y en su correspondiente verificación se utilizan complejos procedimientos matemáticos basados en criptografía asimétrica (también llamada criptografía de clave pública).

En un sistema criptográfico asimétrico, cada usuario posee un par de claves propio. Estas dos claves, llamadas clave privada y clave pública, poseen la característica que si bien están fuertemente relacionadas entre sí, no es posible calcular la clave privada a partir de los datos de la clave pública, ni tampoco a partir de los documentos cifrados con la clave privada.

El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma.

En consecuencia, si es posible descifrar un mensaje utilizando la clave pública de una persona, entonces puede afirmarse que el mensaje lo generó esa persona utilizando su clave privada (probando su autoría).

¿Qué son los certificados digitales?

Los certificados digitales son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad. De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

En algunos casos, puede ser necesario crear una cadena de certificados, cada uno certificando el previo, para que las partes involucradas confíen en la identidad en cuestión.

¿Qué contiene un certificado digital?

En su forma más simple, los certificados contienen una clave pública y un nombre. Habitualmente, un certificado también contiene una fecha de expiración, el nombre de la Autoridad Certificante que emitió ese certificado, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del certificado.

El formato de los certificados está definido por el estándar internacional ITU-T X.509. De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el mencionado estándar.

¿Qué valor legal tiene la firma digital?

Se debe tener en cuenta lo siguiente:

Que para la legislación argentina los términos "Firma Digital" y "Firma Electrónica" no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada uno de ellos, dado que en el caso de la "Firma Digital" existe una presunción *"iuris tantum"* en

su favor; esto significa que si un **documento firmado digitalmente** es verificado correctamente, se presume **salvo prueba en contrario** que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de **la firma electrónica,** en caso de ser desconocida la firma por su titular corresponde a quien la invoca acreditar su validez.

Por otra parte, para reconocer que un documento ha sido firmado digitalmente se requiere que el certificado digital del firmante haya sido emitido por un **certificador licenciado** (o sea que cuente con la aprobación del **Ente Licenciante).**

Es por esto que, si bien entendemos que en los ambientes técnicos se emplea habitualmente el término Firma Digital para hacer referencia al instrumento tecnológico, independientemente de su relevancia jurídica, solicitamos a todos los proveedores de servicios de certificación, divulgadores de tecnología, consultores, etc. que empleen la denominación correcta según sea el caso, a fin de no generar confusión respecto a las características de la firma en cuestión.

La legislación argentina emplea el término "Firma Digital" en equivalencia al término "Firma Electrónica Avanzada" utilizado por la Comunidad Europea o "Firma Electrónica" utilizado en otros países como Brasil o Chile.

En el Caso del Ecuador el término es Firma Electrónica.

Esta es la relación de Prestadores de Servicios de Certificación acreditados por CONATEL

Banco Central del Ecuador (Entidad Certificadora pública).
Security Data.
ANF Ecuador.

Para revisar iniciativas internacionales ver:

http://www.pki.gov.ar/index.php?option=com_content&view=article&id=120&Itemid=132

Ver anexo: Reglamento para la organización y funcionamiento del Registro Público Nacional de entidades de certificación de información y servicios relacionados acreditadas y terceros vinculados. (Rs. 479-20-CONATEL-2008. RO 455:28-oct-2008)

CONTRATOS ELECTRÓNICOS

1.- Acercándonos a una conceptualización

Las nuevas tecnologías de la información se han desarrollado en la actualidad en forma rápida y oportuna, lo que permite que gracias a este avance tecnológico se beneficie entre otras actividades el comercio, pues es muy fácil comprar y vender bienes, servicios desde un escritorio en la oficina o desde el hogar.

Esta actividad nueva se la ha denominado "Comercio Electrónico", varios países, incluido el Ecuador disponen de normativas que regulan la actividad del denominado "E Commerce".

Aparece como elemento importante el contrato, que es un negocio jurídico entre vivos, en el cual sus participantes hacen una declaración conjunta de voluntades con la finalidad de reglar sus relaciones jurídicas presentes y futuras, por ello la importancia de conocer los denominados contratos informáticos.

Aquellos negocios jurídicos que no sólo hacen relación a la informática, sino a toda la actividad comercial de contratación de bienes y servicios por Internet.

En la doctrina, existen tres teorías que conceptualizan a los contratos informáticos de diferente manera:

La primera de éstas, considera como elemento determinante para su conceptualización el objeto al cual están referidos dichas contrataciones;

La segunda, toma como elemento caracterizador las diversas relaciones jurídicas que emanan del mismo acto. Estas dos teorías coinciden en

establecer que los contratos informáticos son contratos particulares (e individuales) y difieren del resto de los contratos.

La tercera teoría, se basa en establecer que el objeto es determinante pero no suficiente como para considerarse que se han creado nuevos tipos de contratos, por consiguiente, delimita a los contratos informáticos como contratos tradicionales, pero con matices particulares por el objeto.

Con la finalidad de delimitar lo qué se entiende por contrato informático, nos haremos partícipes de la teoría que pretende definirlo en virtud de su objeto, por ello, será contrato informático todo aquel que tenga como objeto un bien o un servicio informático.

Mientras, por contrato electrónico se entiende a todo aquel contrato (tradicional o no) que se haya realizado por ese medio (electrónico), lo cual no sólo se limita a Internet sino a tecnologías anteriores como el Fax o posteriores aun en desarrollo. Al Contrato Electrónico también se le conoce como: "Contratos a Distancia", "Contratos Telemáticos", "Contratos por medio de las nuevas tecnologías", etc.

Como se puede inferir de estas definiciones, los contratos informáticos se refieren al "fondo" de la contratación, mientras que los segundos se refieren a la "forma" de la misma.

2.- Hacia una clasificación

El Profesor español Davara Rodríguez, los divide en cuatro clases de contratos:

a) Contrato de Hardware;
b) Contratos de Software;
c) Contratos de instalación llave en mano; y
d) Contratos de servicios auxiliares.

Otros autores los clasifican en:

a) Por su objeto: Abarcan los de software, hardware, llave en mano, etc.
b) Por el negocio jurídico: Abarcan compra venta, arrendamiento, etc., y,
c) Complejos: Abarcan tales como Outsourcing, Jointventure, etc.

En General los contratos que se derivan de los derechos, deberes y obligaciones entre Productores, Distribuidores y Usuarios, de bienes y servicios relacionados con la tecnología.

Lo que nos da una clasificación de varios tipos de contratos que numéricamente son cuantiosos.

3.- Elementos constitutivos del Contrato Informático

Por ser un tema relacionado a la tecnología aparecen principios y elementos nuevos, como por ejemplo cláusulas especiales que no recoge la normativa tipificada en los códigos de los países, por lo que amerita actualizar la legislación con estos contenidos.

A modo de conclusión de esta primera aproximación al tema, es de destacar que la contratación informática afecta tanto las relaciones contractuales de carácter interempresarial (business to business), como las que vinculan a Empresas y consumidores (business to consumer), y como tal debe realizarse su interpretación de acuerdo con la normativa aplicable a cada tipología.

En fin el tema es amplio e interesante ES IMPORTANTE realizar con profundidad conocer y aclarar todas las interrogantes de este nuevo tipo de contratación que involucra las nuevas tecnologías de la información, y que los profesionales deben conocer estos contenidos para el desempeño y actualización de conocimientos de un mundo globalizado, en donde predomina el uso de la tecnología y se desarrolla un comercio por medios electrónicos.

¿QUÉ SON LOS CONTRATOS INFORMÁTICOS?

Es todo acuerdo de dos o más personas que crea o transfiere derechos y obligaciones de contenido informático, ya sea porque su objeto

sean bienes y servicios informáticos o bien porque ese acuerdo de voluntades se exteriorizo de manera informática.

Contrato Informático: Orden Civil o Mercantil

Problemas informáticos: podemos señalar el problema de determinar que constituye un vicio oculto en un bien informático.

El profesor español Dr. Davara Rodríguez los define como: "es aquella que se realiza mediante la utilización de algún elemento electrónico que tiene, o puede tener incidencia real y directa sobre la formación de la voluntad, el desarrollo o la interpretación futura de un acuerdo".

UNA NUEVA FORMA DE CONTRATACIÓN

Desaparece el contacto físico de las partes.

Se realizan transacciones de bienes y servicios en forma electrónica, o por cualquier medio magnético

Contrato celebrados por internet entre nacionales de distintos países, pues dos personas celebran el mismo contrato al mismo tiempo pero en dos naciones diferentes y bajo dos legislaciones diferentes.

El problema se agrava si uno de los números de los cibernavegantes es menor.

Otro problema importante es el que implica el riesgo de contratar con personas ficticias o empresas virtuales.

Ley de comercio electrónico

ESPAÑA. Sociedad de la información: Directiva

Información previa a la contratación: Antes de que el usuario realice ningún pedido, la Directiva establece que los prestadores de servicios deben informarle de los siguientes aspectos:

a) Los pasos técnicos que deben darse para la celebración del contrato.
b) Si va a registrar el contrato celebrado y si puede ser accesible.
c) Los medios técnicos para corregir los errores de introducción de datos antes de efectuar el pedido.
d) Las lenguas ofrecidas para la celebración del contrato.

Obligación de proporcionar la información

Realización de un pedido: Una vez que haya realizado el usuario un pedido, la Directiva exige a los prestadores de servicios unos determinados requisitos:

Acuse de recibo sin demora y por vía electrónica. Asimismo se considera que se ha recibido el pedido y el acuse de recibo cuando las partes a que se dirigen puedan tener acceso a los mismos.

Solución de controversias

Ley aplicable
Jurisdicción

Este es el caso del Convenio de Roma de 19 de Junio de 1980, aplicable a las obligaciones contractuales en el marco de la Unión Europea. (Art. 3: "Los contratos se regirán por la ley elegida por las partes").

El artículo 5.2 del Convenio de Roma establece que, "sin perjuicio de lo dispuesto en el artículo 3, la elección por las partes de la ley aplicable no podrá producir el resultado de privar al consumidor de la protección que le aseguren las disposiciones imperativas de la ley del país en que tenga su residencia habitual.

OECD y la UNCITRAL, emprendiendo una iniciativa reguladora del Comercio Electrónico en el mercado interno.

Por tanto, igualmente recomendable, el redactar una cláusula de sumisión a una jurisdicción pertinente y, paralelamente, no proyectar

publicidad u ofertas que tengan como objeto al consumidor en jurisdicciones indeseadas procesalmente.

El Arbitraje Internacional (solución adecuada).

Ley de Comercio Electrónico.

MARCO JURÍDICO ECUADOR

Ley de Comercio Electrónico
Ley de Defensa del Consumidor
Ley de Propiedad Intelectual
Código de Comercio
Código Civil
Código Orgánico Integral Penal COIP

En la doctrina, existen TRES teorías que conceptualizan a los contratos informáticos:

1. Considera como elemento determinante para su conceptualización el objeto al cual están referidos dichas contrataciones;
2. Toma como elemento caracterizador las diversas relaciones jurídicas que emanan del mismo acto. Estas dos teorías coinciden en establecer que los contratos informáticos son contratos particulares (e individuales) y difieren del resto de los contratos.
3. Se basa en establecer que el objeto es determinante pero no suficiente como para considerarse que se han creado nuevos tipos de contratos, por consiguiente, delimita a los contratos informáticos como contratos tradicionales, pero con matices particulares por el objeto.

Con la finalidad de delimitar lo que se entiende por contrato informático, nos haremos partícipes de la teoría que pretende definirlo en virtud de su objeto, por ello, será contrato informático todo aquel que tenga como objeto un bien o un servicio informático contrato electrónico se entiende a todo aquel contrato (tradicional o no) que se haya realizado por ese medio (electrónico), lo cual no sólo se limita a

Internet sino a tecnologías anteriores, como el Fax o posteriores aun en desarrollo. Al Contrato Electrónico también se le conoce como: "Contratos a Distancia", "Contratos Telemáticos", "Contratos por medio de las nuevas tecnologías", etc.

CLASIFICACIÓN

El Profesor español Davara Rodríguez, los divide en cuatro clases de contratos:

a) Contrato de Hardware;
b) Contratos de Software;
c) Contratos de instalación llave en mano; y
d) Contratos de servicios auxiliares

Otros autores los clasifican en:

a) Por su objeto: Abarcan los de software, hardware, llave en mano, etc.
b) Por el negocio jurídico: Abarcan compra venta, arrendamiento, etc., y,
c) Complejos: Abarcan tales como Out sourcing, Joint venture, etc.

Elementos constitutivos del Contrato Informático:

Por ser un tema relacionado a la tecnología aparecen principios y elementos nuevos, como por ejemplo cláusulas especiales que no recoge la normativa tipificada en los códigos de los países, por lo que amerita actualizar la legislación con estos contenidos.

a)**Consentimiento:** El consentimiento, es la voluntad de las partes para comprometerse en alguna obligación jurídica para con la otra parte firmante del acuerdo. Este consentimiento debe ser exteriorizado por ambas partes, sin embargo, el contrato para su validez no tiene que constar por escrito, convirtiéndose los actos o hechos que realicen las partes medios de prueba de la existencia del contrato verbal (o de cualquier otro que no conste en papel, como por ejemplo el contrato electrónico).

Con respecto a la manifestación de las voluntades, Larroumet expresa: "Para que haya coincidencia de las voluntades de los contratantes es necesario que cada uno haya conocido la voluntad del otro, lo cual supone que dichas voluntades hayan sido manifestadas, esto es, que hayan sido exteriorizadas y no hayan permanecido en el fuero interno de cada uno de las partes que la acepta. Por consiguiente, es la coincidencia de la oferta y de la aceptación lo que constituye la celebración del contrato". Tres son las condiciones para determinar que el consentimiento no es válido, y por ende, el contrato sería nulo, estos son: la violencia, el error y el dolo.

b)**El Objeto:** El objeto de todo contrato debe ser "posible, lícito, determinado o determinable".

Todo producto o conducta que sea factible de realización puede ser objeto de un contrato, siempre y cuando, no sea prohibido su comercio o conducta por alguna norma jurídica.

Las conductas de imposible ejecución, como por ejemplo: "se realizará un software para que el usuario pueda comunicarse directamente con Dios" o aquellas que pretenden comercializar bienes que están fuera del dominio privado: "las parcelas del cielo o un campo determinado del océano", no tendrán validez jurídica. Igualmente, no basta que el objeto pertenezca al dominio privado, sea de comercialización lícita y pueda ser ejecutable, sino que además deberá de determinarse concretamente las obligaciones que surgen del contrato o que sea posible determinarse en un futuro.

c)**La Causa lícita:** La causa puede definirse como: "(...) función económico - social del contrato considerado en su totalidad y alude a la necesidad de que existe conformidad entre ella y el intento".

El Código de Obligaciones y Contratos Libanés, en su Art. 200 establece: "la causa del contrato reside en el móvil individual que ha incitado a la parte ha celebrarlo y que no forma parte integrante del acto: ella varía de un caso a otro para una misma categoría de contrato"

Para concluir, Larroumet considera que la causa se analiza "(...) en función de todas las circunstancias particulares que han determinado el acto de voluntad de cada uno de los contratantes" y ya no se "(...) analiza la causa por el lado de la obligación del deudor".

CARACTERÍSTICAS PRINCIPALES

a) Que las operaciones se realizan por vía electrónica o digital:

En una economía digital, el comercio electrónico renace, y adquiere importancia vital para el desarrollo del comercio mundial. Aunque no podemos limitar la utilización del concepto del comercio electrónico a Internet, es definitivamente la llegada de la "red" la que nos hace profundizar en la importancia del este tipo de comercio.

b) Que se prescinde del lugar donde se encuentran las partes:

La utilización de medios electrónicos en las comunicaciones con fines comerciales, se realiza con los sujetos en lugares distintos, tanto a nivel nacional como internacional.

El comercio electrónico no puede desarrollar su potencial sino hasta la revolución digital, pues con ello se facilita el transporte de las comunicaciones y la inmediatez que de ello se deriva crea en los individuos un ambiente propicio para intercambiar información. Al encontrarnos con sujetos en distintas localizaciones geográficas, surge el problema de cuál jurisdicción será la apropiada para regular la transacción comercial, lo que debe resolverse por las reglas del derecho internacional privado.

c) Que no quedan registros en papel (p.ej. facturas):

Depende del sistema que se utilice, el soporte en papel no existirá. En los envíos de faxes, es muy obvio que al menos se cuenta con la prueba impresa de que se envió el documento, y la otra parte recibe directamente la comunicación en papel, por lo que no se aplicaría esta

característica. Sin embargo, como ya se ha explicado, en la era digital el papel pierde importancia aunque esto no significa que su utilización haya desaparecido. Estamos cambiando de una economía de papel a una digital, en donde los documentos serán seguros aunque no se encuentren impresos (seguridad documental informática).

Nos encontramos en un período en el que los contratos digitales reemplazan a los contratos en papel, con la consiguiente consecuencia de reducciones de costos y mayor eficiencia en las empresas. Una vez digitalizada la información, ésta puede ser reproducida ilimitadamente y enviada simultáneamente a grandes distancias y diferentes destinatarios. La desaparición de las facturas de papel, lleva a la necesidad de creación de nuevos mecanismos adaptados a su entorno tecnológico, que brinden seguridad y soporte a la transacción electrónica.

d) Que la importación del bien no pasa por las aduanas (en el comercio electrónico directo):

Para comprender esto, es necesario saber que el comercio electrónico directo es en el cual se envían los productos directamente por Internet. Es clara la referencia a un envío de software directo, o a venta de información, la cual no debe pasar por ninguna frontera geográfica, sino que se realiza dentro del ciberespacio.

e) Que se reducen drásticamente los intermediarios:

Es importante notar, que las empresas productoras de bienes o de ofrecimiento de servicios, pueden excluir la utilización de los intermediarios que anteriormente eran necesarios para la distribución del producto.

f) Que se efectivizan más rápidamente las transacciones (compresión del ciclo transaccional):

La distancia entre las partes, no influye en la velocidad en la cual las comunicaciones son enviadas y recibidas. Se crea un entorno en que

el tiempo se reduce drásticamente y el comercio encuentra un nuevo espacio para expandirse.

LOS NUEVOS CONTRATOS INFORMÁTICOS

Entre los nuevos contratos informáticos tenemos los contratos de licencia de uso de software, que son aquellos por los cuales los usuarios de software pueden utilizar el programa de ordenador respetando los derechos de autor protegidos por la licencia.

Estos contratos debido a su distribución masiva son contratos de adhesión, por lo cual sus cláusulas son prestablecidas por el licenciante y aceptadas por el licenciatario.

Este tipo de contratación genera desigualdad entre los contratantes, por lo cual los proponentes aprovechan esta situación para colocar cláusulas abusivas dentro de los contratos, como sucede en algunos contratos de licencia de software donde las cláusulas generan presunciones abusivas para la aceptación del usuario. Para evitar esto, la doctrina y la jurisprudencia condicionan el consentimiento contractual al cumplimiento del deber de información previo por parte del licenciante.

Las principales licencias de software son los shrink-wrap, browse-wrap y click-wrapagreements.

El primer tipo de licencia, shrink-wrap, es netamente de adhesión, por lo cual su práctica genera inconvenientes en la presunción de aceptación contractual, por el desconocimiento previo del contrato.

En browse-wrapagreementla validez es relativa, por cuanto el consentimiento está condicionado al acceso previo a la aceptación presuntiva establecida en el contrato.

Por último los click-wrapagreements son plenamente válidos en cuanto condicionan el acceso al software a una aceptación previa ya conocida por el usuario.

1. EDI
2. Shrinkwrap y Webwrap
3. Contrato de Servicios por Internet

1. EDI (Electronic Data Interchange)

Desde la década de los 70, las transacciones vía EDI, han sido utilizadas como una forma ágil y automatizada para las relaciones comerciales entre las empresas que favorece la producción "just in time". Puede definirse a las comunicaciones vía EDI, como el intercambio entre computadoras de información negocial, en formatos estandarizados. Mediante el EDI las interacciones entre las partes tienen lugar por medio de aplicaciones informáticas que actúan a modo de interfaz con los datos locales y pueden intercambiar información comercial estructurada

2. Shrinkwrap y Webwrap

Con su utilización, se permite a las compañías desarrollar un procesamiento automatizado de datos, el cual genera, transmite, recibe y procesa información electrónicamente, en substitución de los tradicionales documentos en papel el término Shrinkwrap hace referencia a un acuerdo de licencia de uso, sin firmar, el cual estipula que la aceptación por parte del usuario de los términos, se presenta en el momento de abrir el empaque "shrinkwrap", u otro empaque del software, por el uso del software, o por otro mecanismo especificado. En palabras más sencillas, un acuerdo shrinkwrap, son aquellos acuerdos de licencia de uso, que traen consigo los productos de software que se adquieren. Tradicionalmente éste acuerdo expresa que "al romper éste empaque "shrinkwrap", se aceptan los términos aquí contenidos". Hay otras maneras de acordar la aceptación de la licencia de uso, entre las cuales se puede mencionar la aceptación de las condiciones que aparecen en el monitor de la computadora a la hora de instalar el software, o el acuerdo que viene adjunto al soporte físico del software, en donde se establecen las cláusulas.

Si pretendemos definir y entender las compraventas en Internet, es indispensable comprender los webwrap, lo cual no se lograría sin haber estudiado anteriormente el contrato shrinkwrap.

Los contratos webwrap, incluyen varios tipos de transacciones en línea. Una de estas son las transacciones de venta de software, que requieren que el usuario o consumidor final, acepte los términos de una licencia de uso, previo al envío del software en línea. Esta forma de utilizar el contrato webwrap es muy común, y se asemeja a las características del shrinkwrap. Algunos sitios utilizan acuerdos webwrap para prevenir que los usuarios de la Web puedan navegar en sus páginas, sin antes aceptar varios términos que los dueños del sitio establecen (como restringir el uso de la información de la página a uso personal, prohibir la reproducción del contenido del sitio, etc.). Las transacciones webwrap, también llamadas clickwrap, son las convenciones electrónicas que más se utilizan en Internet.

3. Contrato de Servicios por Internet

Convención de las Naciones Unidas sobre los contratos de compraventa internacional de mercaderías.

La Organización Mundial del Comercio en el Acuerdo General sobre el Comercio de Servicios (GATS), define la forma en la cual puede presentarse las prestación de servicios internacionalmente, lo cual crea una perspectiva independiente del tema, y lo diferencia del comercio de bienes, y esto confirma el diferente tratamiento que debe darse al tema de los servicios con respecto a las compraventas de bienes.

La validez de los documentos electrónicos

LOS CONTRATOS MÁS INDISPENSABLES

1. Contratos sobre Prestaciones del Hardware
   1.1 Proveedor de materiales – Fabricante de Hardware

1.2 Contrato entre Importador - Distribuidor
1.3 Distribuidor - Mayorista
1.4 Mayorista - Minorista
1.5 Minorista - Usuario (particular)

2. Contratación para la elaboración de Bienes Informáticos
2.1 Contratación para la elaboración del Software
2.1.2 Software desarrollado bajo relación laboral
2.1.2 Software desarrollado por encargo
a)Relación Empresa – Empresa (B2B)
b)Contratación directa con un profesional independiente
2.2 Contratación para la elaboración de una Base de Datos
2.3 Contratación para la elaboración de una página Web

3. Licenciamientos de Software
a.)Las Licencias para Usuarios Finales
b)El Paquete de Licencias Microsoft / Open License (Versión 6.0)
c)La Licencia Select (Versión 6.0)
d)Enterprise Agreement Suscripcion (Versión 6.0)
1. Copia de Respaldo o Copia de "Back up"
2. Adaptaciones
3. Reproducción lícita del código para la interoperabilidad de un programa
4. Copia en la Memoria Rom y en la Memoria Ram
5. Prestación de Servicio y Soporte Técnico
6. Hardware
7. Software
8. Bases de Datos
9. Páginas web

INFRACCIONES ELECTRÓNICAS CÓDIGO PENAL ECUADOR

Se consideran infracciones informáticas, las de carácter administrativo y las que se tipifican como tales, según la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, publicada en el suplemento del registro oficial No. 557 del 17 de abril del 2002.

INTRODUCCIÓN

La sociedad de la información está influenciada en la vida diaria por la informática, personas, organizaciones, y la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, la justicia, etc., son aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

Frente al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, «infracciones electrónicas», o Delitos informáticos.

"Para que cualquier acto sea considerado como delito, se exige la concurrencia de los siguientes elementos integrados:

a) Un sujeto activo, esto es, un individuo que quebrante la norma jurídica y que siendo imputable incurre por ello en la condicional punitiva determinada por el Legislador.
b) Un objeto que se determina por el derecho violado, bien sea que éste pertenezca a personas naturales o jurídicas;
c) Un sujeto pasivo, esto es, la víctima, en otras palabras la persona que sufre el agravio;
d) Un fin, esto es, la perturbación del orden jurídico

La noción de delito, por su parte, está compuesta también por tres elementos básicos:

1. El elemento material;
2. El elemento moral; y
3. El elemento jurídico

El *elemento material,* lo conforma a su vez la acción que desarrolla el autor; es el resultado de la acción, y la relación de casualidad que debe haber entre la acción del autor y el resultado.

El *elemento moral* lo constituyen la imputabilidad y la culpabilidad.

El *elemento jurídico,* a su vez, está conformado por la antijuricidad y la tipicidad".

(Gaceta Judicial N' 9, Serie XV,1990, págs. 2732.2733)

CONCEPTO DE DELITO:

Acción u omisión voluntaria castigada por la ley. (Diccionario Jurídico Ambar. Pág. 64)

COUTURE
Delito Penal:

Calificación jurídica de una conducta de acción u omisión, dolosa o culpable, determinada típicamente y castigada como tal por la ley penal

JULIO TELLEZ (México)

Infracciones electrónicas son actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y, culpables en que se tienen a las computadoras como instrumento o fin (concepto típico).

PRINCIPALES CARACTERÍSTICAS

1. Son conductas criminógenas de cuello blanco (white collar crimes), en tanto que sólo determinado número de personas con ciertos conocimientos (en este caso técnicos)Pueden llegar a cometerlas.
2. Son acciones ocupacionales en cuanto que muchas veces se realizan cuando el sujeto trabaja.
3. Son acciones de oportunidad en cuanto que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
4. Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que los realizan.
5. Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a cometerse.

6. Son muchos los casos y pocas las denuncias y todo ello debido a la misma falta de regulación por parte del derecho.
7. Son sumamente sofisticados y relativamente frecuentes en el ámbito militar.
8. Presentan grandes dificultades para su comprobación, esto, por su mismo carácter técnico.
9. En su mayoría son imprudenciales y no necesariamente intencionales.
10. Ofrecen facilidades para su comisión a los menores de edad. Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.
11. Por el momento siguen siendo ilícitos manifiestamente impunes ante la ley.

El 10 de agosto del 2014 entro en vigencia el nuevo código penal integral COIP, en relación a los delitos informáticos o infracciones electrónicas vamos a realizar un estudio pormenorizado en la parte cuatro de este texto.

RÉGIMEN JURÍDICO DE PROTECCIÓN DE DATOS EN EL ECUADOR

INTRODUCCIÓN

La tecnología informática está al alcance de todos, la actividad del ser humano se desarrolla y se desenvuelve por medios automáticos, por lo que se ha determinado una serie de ventajas y desventajas, que en lo principal pueden afectar a los derechos fundamentales de las personas, como por ejemplo lesionar la "intimidad" y la "privacidad" de los "datos" que se procesan electrónicamente.

Por ello la necesidad de precautelar, "regular", proteger, controlar y sancionar los actos y hechos que afecten negativamente a los sujetos sin que estos hayan tenido conocimiento[4]de lo que ha sucedido con los datos y mensajes proporcionados electrónicamente.

Esta tarea le compete al Derecho Informático como una nueva rama del derecho de las nuevas tecnologías de la información.

La doctrina utiliza la expresión "protección de datos"[5] en lo referente a la protección jurídica de la persona frente a la tecnología que automatiza sus datos.

Pero que es lo que se protege, al respecto la mayoría de autores coinciden en los siguientes aspectos:

Proteger al individuo ante el "manejo o manipulación, no autorizada, de sus datos personales"[6] que se encuentren en medios o formas electrónicas.

---

[4] YÁNEZ, Pablo, *Introducción al estudio del Derecho Informático e Informática Jurídica*, abril 1999. Escuela Politécnica Javeriana del Ecuador, p. 168.

[5] DAVARA, Miguel, *Manual de Derecho Informático*, Edt. Aranzadi 1997, p. 47.

[6] Ibídem. p. 47

Los resultados de procesamientos informáticos, "deben ser identificable con el titular de los mismos"[7]puesto que es muy fácil conocer características de la personalidad y de la intimidad de las personas.

Y, por último, el consentimiento no autorizado del uso de los datos, para fines en los que el titular no autorizo o fue obligado a darlos[8].

MARCO JURÍDICO GENERAL

Constitución de la República del Estado
Ley de Propiedad Intelectual
Ley de defensa y Protección del Consumidor
Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

En la constitución[9] vigente del Ecuador

La información de las personas por medios digitales o informáticos, se ha convertido en una práctica necesaria para tomar cualquier determinación sobre políticas públicas. Es por ello que cualquier entidad pública o privada elabora y desarrolla sistemas de información conformados por redes de telecomunicaciones y bases de datos que se recogen diariamente y se alimentan bases de datos personales.

Esto es común, si bien el tratamiento de datos personales juega un rol importante para el cumplimiento de actividades de interés general, no debe perderse de vista que la protección de los derechos humanos es condición connatural para, entre otras, materializar la dignidad humana.

La realidad ha demostrado ciertos beneficios de estos sistemas de información pero, también se ha constatado una serie de injusticias

[7] Ibídem. p. 48
[8] Ibídem. p. 48
[9] Constitución de la República del Ecuador 2008.

que suceden con los ciudadanos debido al tratamiento indebido de su información referida a lo personal.

La protección de datos personales **(data protection) ver:** www.agpd.es comprende, entre otras, el conjunto de normas y principios que regulan el tratamiento de dicha información en todas sus etapas (recolección, almacenamiento, circulación, publicación y transferencia nacional e internacional).

La importancia se evidencia en la incorporación de este "nuevo Derecho" en algunas constituciones y normas de los países. Representa un derecho fundamental y una herramienta jurídica del ciudadano para que se proteja frente al tratamiento indebido o ilegal que reciban sus datos personales por parte de los administradores de bases de datos o de archivos de entidades públicas y privadas

CONSTITUCIÓN ECUATORIANA

Art. 40.- Se reconoce a las personas el derecho a migrar. No se identificará ni se considerará a ningún ser humano como ilegal por su condición migratoria. El Estado, a través de las entidades correspondientes, desarrollará entre otras las siguientes acciones para el ejercicio de los derechos de las personas ecuatorianas en el exterior, cualquiera sea su condición migratoria:

5. Mantendrá la confidencialidad de los datos de carácter personal que se encuentren en los archivos de las instituciones del ecuador en el exterior.

Capítulo sexto: Derechos de libertad

Art. 66.- Se reconoce y garantizará a las personas:

11. El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas,

filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica.

19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

20. El derecho a la intimidad personal y familiar.

Sección quinta: Acción de hábeas data

Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

Art. 329.- Las jóvenes y los jóvenes tendrán el derecho de ser sujetos activos en la producción, así como en las labores de autosustento,

cuidado familiar e iniciativas comunitarias. Se impulsarán condiciones y Para el cumplimiento del derecho al trabajo de las comunidades, pueblos y nacionalidades, el Estado adoptará medidas específicas a fin de eliminar discriminaciones que los afecten, reconocerá y apoyará sus formas de organización del trabajo, y garantizará el acceso al empleo en igualdad de condiciones.

Se reconocerá y protegerá el trabajo autónomo y por cuenta propia realizado en espacios públicos, permitidos por la ley y otras regulaciones.

Se prohíbe toda forma de confiscación de sus productos, materiales o herramientas de trabajo.

Los procesos de selección, contratación y promoción laboral se basarán en requisitos de habilidades, destrezas, formación, méritos y capacidades. Se prohíbe el uso de criterios e instrumentos discriminatorios que afecten la privacidad, la dignidad e integridad de las personas.

El Estado impulsará la formación y capacitación para mejorar el acceso y calidad del empleo y las iniciativas de trabajo autónomo. El Estado velará por el respeto a los derechos laborales de las trabajadoras y trabajadores ecuatorianos en el exterior, y promoverá convenios y acuerdos con otros países para la regularización de tales trabajadores.

DISPOSICIONES TRANSITORIAS

PRIMERA.- El órgano legislativo, en el plazo máximo de ciento veinte días contados desde la entrada en vigencia de esta Constitución aprobará la ley que desarrolle el régimen de soberanía alimentaria, la ley electoral, la ley reguladora de la Función Judicial, del Consejo de la Judicatura y la que regula el Consejo de Participación Ciudadana y Control Social.

En el plazo máximo de trescientos sesenta días, se aprobarán las siguientes leyes:

8. Las leyes que organicen los registros de datos, en particular los registros civil, mercantil y de la propiedad. En todos los casos se establecerán sistemas de control cruzado y bases de datos nacionales.

LEY DEL SISTEMA NACIONAL DE DATOS PÚBLICOS DE LOS REGISTROS DE LA PROPIEDAD, MERCANTILES Y DE PRENDAS ESPECIALES DE COMERCIO

(Publicado en el Registro Oficial 162, 31 de Marzo de 2010. Ver: http://www.asambleanacional.gov.ec/tramite-de-las-leyes.html)

LEY DE PROPIEDAD INTELECTUAL

"Art. 26.- También Constituyen violación de los derechos establecidos en este Libro cualquiera de los siguientes actos:

a) Remover o alterar, sin la autorización correspondiente, información electrónica sobre el régimen de derechos; y,
b) Distribuir, importar o comunicar al público el original o copias de la obra sabiendo que la información electrónica sobre el régimen e derechos ha sido removida o alterada sin autorización.

Se entenderá por información electrónica aquella incluida en las copias de obras, o que aparece en relación con una comunicación al público de una obra, que identifica la obra, el autor, los titulares de cualquier derecho de autor o conexo, o la información acerca de los términos y condiciones de utilización de la obra, así como número y códigos que representan dicha información.

Reglamento de la Ley de Defensa del Consumidor[10].

Protección Contractual

Art. 38.- Para los efectos previstos en el Art. 41 de la Ley, tanto los contratos de adhesión como los textos a los que éstos se remitan, o

[10] Reglamento a Ley de Defensa Consumidor.-R.O No. 287 - Quito, Lunes 19 de Marzo del 2001

formen parte del mismo, deberán tener un tamaño de fuente no menor de diez puntos, salvo lo previsto en regulaciones internacionales.

Art. 39.- Se entenderán incorporadas al léxico aquellas palabras que den a entender su significado como vocablos de uso frecuente y de general aceptación por parte de toda la comunidad, y no sólo por los entendidos en la materia de que se trate.

Art. 40.- El consentimiento expreso del consumidor de someterse a los procedimientos de arbitraje y mediación en los contratos de adhesión, se podrá manifestar mediante una ratificación impresa debajo de la cual suscriba el consumidor, o con una señalización en un casillero, de la que se desprenda la aceptación para someterse a arbitraje, o cualquier fórmula que permita entender inequívocamente la aceptación expresa de cualquiera de estos procedimientos por parte del consumidor.

Art. 43.- Para el cumplimiento del inciso segundo del Art. 44, el abonado o usuario podrá exigir el cese inmediato de la provisión del servicio contratado, debiendo cumplir con las obligaciones indicadas en el citado artículo.

HÁBEAS DATA Y MENSAJE DE DATOS

La nueva ley de Comercio Electrónico, hace énfasis en el "Mensaje de Datos", como vamos a profundizar más adelante.

Doctrinariamente el hábeas Data protege a la integridad moral de las personas, frente a informaciones referidas a su personalidad, donde prima la "intimidad" y la "privacidad" y su "entorno familiar".

Si es verdad que el Hábeas Data, nació con el desarrollo tecnológico del mundo contemporáneo, gracias a ese avance "los mensajes de Datos" han requerido especial tipificación, pues muchos países han adoptado regímenes jurídicos propios, autónomos con leyes especiales sobre el tema, generando infraestructura física, personal especializado, y procedimientos con instancias administrativas para atender las necesidades del usuario.

Naturaleza del hábeas data

Es una garantía que protege varios derechos, tales como, la honra, la buena reputación, la intimidad y también el derecho a la información.

Enrique Falcón, dice que el Hábeas Data es un remedio urgente para que las personas puedan obtener el conocimiento de los datos a ellos referidos, y de su finalidad, que "conste en el registro o banco de datos públicos o privados y en su caso para exigir la supresión, rectificación, confidencialidad o actualización de aquellos"[11].

Doctrinariamente el Hábeas Data protege a la integridad moral de las personas, frente a informaciones referidas a su personalidad, tales como: su afiliación política, gremial, religiosa, su historia laboral, sus antecedentes crediticios, policiales e informaciones similares que constan en registros o bancos de datos. Hábeas Data "resguarda la intangibilidad de la reserva de la vida privada del individuo y su entorno familiar".

La acción de Hábeas Data nace con el desarrollo tecnológico del mundo actual. Hoy nuestra vida está registrada en instituciones públicas y privadas y, en la mayoría de los casos, no conocemos exactamente el contenido de esa información sobre nosotros mismos o sobre nuestros bienes. Muchas veces es información incorrecta por falta de actualización de tales registros o bancos de datos y. así circular esa información incorrecta, perjudica su honra y buena fama, siendo real, es información relacionada a hechos privados e íntimos que, así divulgare, vulnera el ámbito de la privacidad, precisamente, por el carácter de confidencialidad de tal información.

El Hábeas Data obliga al funcionario que dispone la información, a presentar la información, a explicar el uso que se le está dando y con qué propósitos la entidad tiene esa información.

El Hábeas Data nos garantiza a accesar y verificar la información y como consecuencia pedir que se actualice los datos, rectificarlos o

[11] Op. Cit.

anulados si fueren erróneos o afecten a sus derechos fundamentalmente a su honra o intimidad.

En relación a esta garantía se desprenden tres derechos: derecho de acceso; derecho de conocimiento; derecho a la actualización, rectificación, eliminación o anulación de datos.

Estos tres derechos confirman el objetivo básico del Hábeas Data, evitar que el uso incorrecto de la información pueda lesionar el honor el buen nombre y el ámbito de la privacidad de la persona, como consecuencia de la difusión de esos datos erróneos, incompletos o inexactos.

Si no se analiza este objetivo básico de la garantía constitucional del Hábeas Data se presenta como de hecho se da, una perniciosa confusión entre el Hábeas Data con la exhibición figura típica del procedimiento civil.

La acción de Hábeas Data sirve para proteger al ciudadano de que el Estado o los particulares hagan uso de una información incorrecta inexacta u obsoleta y que al difundir tal información se produzcan discrímenes calificaciones deshonrosas.

El Hábeas Data nos permite ingresar a la información y descubrir el contenido de ella y a exigir su rectificación si ésta es errónea o afecte ilegalmente sus derechos. Con qué propósito. Evitar que dicha información incorrecta equivocada circule y afecte su intimidad, honra, buena reputación, o pueda causar un daño moral. En definitiva se defiende derechos concretos propuestos en la Constitución.

En el Hábeas Data, no se obtienen pruebas, se acceso a la información, se verifica la exactitud de la información del que la posee, se verifica que uso está dando el poseedor a dicha información, se le impide que la difunda si ésta es errada se cambia la información si es equivocada y se difunde la verdadera información entre aquellos a quien el poseedor de ella la remitió o circuló con el propósito de garantizar eficazmente

derechos constitucionales vinculados al honor, de la intimidad y a la buena fama.

El Hábeas Data no es una acción procesal civil, es una garantía constitucional con objetivos muy piensos que busca que el accionante sepa:

1. Por qué motivos legales el poseedor de la información llegó a ser tenedor de la misma,
2. Desde cuándo tiene la información.
3. Qué uso ha dado a esa información y que hará con ella en el futuro,
4. Conocer a qué personas naturales o jurídicas el poseedor de la información le hizo llegar dicha información. Por qué motivo o con qué propósito y la fecha en la que circuló la información.
5. Qué tecnología usa para almacenar la información.
6. Qué seguridades conoce el tenedor de la información para precautelar que la misma no sea usada indebidamente.

El Hábeas Data no puede ser usado en la obtención de información propia del sigilo profesional, tampoco puede usarse como un medio que pueda obstruir la acción de la Justicia, esto es, no puede usarse el Hábeas Data como medio de liquidar obligaciones civiles, bancarias, comerciales, crediticias, etc. No puede ser un medio de prueba de existencia o no de tales obligaciones. Para probar éstas, el Código de Procedimiento Civil le franquea la posibilidad de juicio de exhibición, que sí es un medio de prueba.

Autoridad Competente

Con la nueva constitución, la autoridad ante quien se debe recurrir la información es al funcionario respectivo, posteriormente si no son atendidos se recurre a los jueces quienes no han perdido competencia para tramitar la acción de Hábeas Data.

Por cierto no es la única garantía a los derechos constitucionales que se exige su cumplimiento ante organismos extraños a la Función Judicial, ocurre lo mismo con el Hábeas Corpus que como sabemos, se lo

interpone ante los jueces de garantías constitucionales, antes era ante el Alcalde.

La tramitación del Hábeas Data ante el funcionario que tiene la información es, además de legal, lógica, pues el ciudadano que requiere ejercer la acción, lo hace directamente ante quien la posee, pues así lo ordena el Art. 92 de la Constitución.

En el Pacto Internacional de Derechos Civiles y Políticos, en (a Parte II artículo 2, numeral 3 dice: "La autoridad competente judicial, administrativa o legislativa. o cualquier otra autoridad competente prevista en el sistema legal del Estado decidirá sobre los derechos de toda persona que interponga tal recurso"

PRINCIPIOS DE LOS MENSAJE DE DATOS

Anotemos el concepto que la ley define a MENSAJE DE DATOS: "Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos".

La ley considera los siguientes Principios generales relativos al mensaje de datos:

a) Valor jurídico, el mensaje de datos tiene igual valor que los documentos escritos;
b) El principio de Incorporación por remisión, entendiéndose a la validez jurídica de la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico;
c) Propiedad Intelectual, los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos al régimen de Propiedad Intelectual,

d) Confidencialidad y reserva, para los mensajes de datos, cualquiera sea su forma, medio o intención;
e) Información escrita, cuando la ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta,
f) Información original, cuando la ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la ley, puede comprobarse que ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.
g) Conservación de los mensajes de datos, se debe archivar el mensaje de datos, siempre que se reúnan las siguientes condiciones
g.1. Que la información que contenga sea accesible para su posterior consulta;
g.2. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida
g.3. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y,
g.4. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley, y,
g.5. Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo. (Art. 8 LCE)
h) Protección de datos, 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,
i) Procedencia e identidad de un mensaje de datos, Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe,

Envío y recepción de los mensajes de datos, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos, son los siguientes:

a) Momento de emisión del mensaje de datos.- Cuando el mensaje de datos ingrese en un sistema de información o red electrónica que no esté bajo control del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto;
b) Momento de recepción del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información orad electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos; y,
c) Lugares de envío y recepción.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos.
d) Duplicación del mensaje de datos, Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

Prueba

Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se

presumirá que ésta reúne los requisitos determinados en la ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectúe con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos. Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Y por último sobre las notificaciones electrónicas

Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo electrónico, de un abogado legalmente inscrito, en cualquiera de los Colegios de Abogados del Ecuador, o Foro de Abogados.

Las notificaciones a los representantes de las personas jurídicas del sector público y a los funcionarios del Ministerio Público que deben intervenir en los juicios, se harán en las oficinas que estos tuvieren o en el domicilio judicial electrónico en un correo electrónico que señalaren para el efecto.

INFRACCIONES RELACIONADAS A LOS MENSAJES DE DATOS

Infracciones administrativas

Clasifica en infracciones Leves y Graves. Se establecen las siguientes sanciones:

La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

a) Amonestación escrita;
b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;
c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y,
d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica.

El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones.

Ver: Instructivo para el procedimiento administrativo sancionador de la superintendencia de telecomunicaciones -SUPERTEL- Resolución ST-2012-0026

LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS

En el Registro Oficial número 162 del pasado 31 de Marzo de 2010, se publica la Ley del Sistema Nacional de Registro de Datos Públicos, ley, que fundamenta gran parte de su creación, en lo establecido en la Constitución vigente, específicamente en lo dispuesto en el artículo 18 numeral segundo, que dice lo siguiente:

"Art. 18.- Todas las personas, en forma individual o colectiva, tienen derecho a:

...Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen

funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información."

Pero esta Ley no sólo fundamenta su creación en lo antes detallado, sino, a nuestro modo de entender, lo hace mayormente en concordancia al derecho universal de acceso a las tecnologías de información y comunicación, tema que congruente al avance del desarrollo tecnológico mundial, hace imperativo su crecimiento de forma geométrica en los temas relacionado.

Finalidad de la ley:

Esta Ley, tiene como finalidad, a más de las antes detalladas, regular de forma clara y expresa el sistema de registro de datos públicos, su forma y método de acceso, ya sean en entidades públicas o privadas que administren dichas bases o registros, y es así que de su finalidad se puede entender que su objeto es garantizar la seguridad jurídica, organizar, regular, sistematizar e interconectar la información, así como: la eficacia y eficiencia de su manejo, su publicidad, transparencia, acceso e implementación de nuevas tecnologías.

Debido a lo antes señalado es que el objeto al cual está sujeta la presente ley, rige tanto para las instituciones del sector público como privado, y que actualmente o en el futuro administren bases o registros de datos públicos, sobre las personas naturales o jurídicas, sus bienes o patrimonio y para las usuarias o usuarios de los registros públicos.

Para esta ley, es importante señalar la conceptualización que hace en razón de la accesibilidad y la confidencialidad, temas tan importantes dentro del conjunto de derechos propios de una persona, que se permite nombrar entre los más importantes a la ideología, afiliación política o sindical, etnia, estado de salud, orientación sexual, religión, condición migratoria y todos los demás atinentes a la intimidad personal y en especial aquella información cuyo uso público atente contra los derechos humanos consagrados en la Constitución e instrumentos internacionales.

Acceso a los datos públicos:

Por tanto el acceso a estos datos sólo será posible, dice esta ley, con autorización expresa del titular de la información, por mandato de la ley o por orden judicial, es decir como se ha venido practicando anteriormente. También son confidenciales los datos cuya reserva haya sido declarada por la autoridad competente, los que estén amparados bajo sigilo bancario o bursátil, y los que pudieren afectar la seguridad interna o externa del Estado.

De todo lo antes dicho, los asambleístas promotores y autores de esta ley, definen a manera taxativa de donde vienen y quiénes son los motivadores de los datos públicos (artículo 13), y es así que dice que "Son registros de datos públicos: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes, de propiedad intelectual y los que en la actualidad o en el futuro determine la Dirección Nacional de Registro de Datos Públicos, en el marco de lo dispuesto por la Constitución de la República y las leyes vigentes".

Los Registros que habla la presente ley son dependencias públicas, desconcentrados, con autonomía registral y administrativa, sujetos al control, auditoría y vigilancia de la Dirección Nacional de Registro de Datos Públicos en lo relativo al cumplimiento de políticas, resoluciones y disposiciones para las bases de datos y de información pública, conforme se determine en el Reglamento que expida la Dirección Nacional, es decir el Gobierno Central.

Cuestionamientos a la nueva ley:

Se cuestiona mucho que esta ley permita que cualquier persona tenga acceso a cualquier tipo de información detallada de otra persona, incluso con fines delincuenciales. Para contrarrestar este temor, se deberá reglamentar de manera adecuada pero sobre todo proteger con lo último en sistemas de protección de datos, a toda aquella información que repose en instituciones públicas y privadas pero que sean de carácter confidencial o sensible y que pueda ser confundida con información pública.

Mi apreciación sobre el tema es que, la historia del Ecuador no cambia, pese a los más de ciento cincuenta años de existencia del país, prima la coyuntura política, más no los principios de una verdadera política de Estado.

La Ley en su Artículo 1, de entrada es inconstitucional, puesto que prescribe que la Ley "es de naturaleza ordinaria", sin embargo al ser un cuerpo normativo que regula el ejercicio de los derechos y garantías constitucionales, debe tener el carácter de Ley Orgánica, conforme lo dispone la Constitución Política.

La Ley mezcla contenidos de información de distinta naturaleza, confunde la información de carácter personal con datos de carácter público, lo que contraviene lo dispuesto la Constitución Política.

Derecho de privacidad de las personas

La información sobre el patrimonio de las personas, este proyecto dice que será de libre acceso, de acuerdo a lo previsto en el artículo 6 de la ley, atenta al derecho de privacidad de las personas, ya que las condiciones que se establecen en la referida norma, permitirán de igual manera que cualquier persona tenga conocimiento, sin autorización de su titular, aquellos datos que son de carácter personalísimo, íntimos y privados. Además que se deja al arbitrio de un reglamento, no sabemos qué requisitos se exigirán.

El artículo 3, es otro elemento inconstitucional, ya que estipula que esta ley regirá para las instituciones del sector público y privado, que en el futuro administren bases o registros de datos públicos, un elemento absurdo ya que transgrede los principios mínimos y elementales de técnica legislativa, puesto que normar "hacia el futuro" sin sentar bases de una legislación, se presta para arbitrariedades.

El artículo 22, habla de la interconexión entre datos públicos y privados, rompe todo principio ético, ya que al hacer este tipo de cruzamiento, se atenta la privacidad y la intimidad de los datos de las

personas, puesto que puede ser mal empleado por los funcionarios públicos que manejen el sistema, los legisladores deben proteger los derechos de los ciudadanos, no dar herramientas para la persecución política o para el funcionamiento de la represión y la violación de los Derechos Humanos.

También la Disposición Segunda General, que considera como información pública, los nombres de propietarios, tenedores, beneficiarios o titulares de acciones y participaciones en sociedades, tanto comerciales, mercantiles y civiles, también atenta a los principios de protección de datos personales que se fundamentan en la privacidad e intimidad de los datos de las personas.

Los legisladores asambleístas deberían pensar en implementar una verdadera política de estado para garantizar los derechos fundamentales de los ciudadanos, se les ha solicitado por varias ocasiones que lo que se debe legislar es en una ley de protección de datos personales, acorde a los avances de la legislación internacional.

Acceso a la información mediante el uso de la tecnología

No nos olvidemos que la TECNOLOGÍA INFORMÁTICA está al alcance de todos, la actividad del ser humano se desarrolla y se desenvuelve por medios automáticos, por lo que se ha determinado una serie de ventajas y desventajas, que en lo principal pueden afectar a los derechos fundamentales de las personas, como por ejemplo lesionar la "intimidad" y la "privacidad" de los "datos" que se procesan electrónicamente.

Por ello la necesidad de precautelar, "regular", proteger, controlar y sancionar los actos y hechos que afecten negativamente a los sujetos sin que estos hayan tenido conocimiento de lo que ha sucedido con los datos y mensajes proporcionados electrónicamente.

Esta tarea le compete al Derecho Informático como una nueva rama del derecho de las nuevas tecnologías de la información.

Protección de datos

La doctrina utiliza la expresión "protección de datos" en lo referente a la protección jurídica de la persona frente a la tecnología que automatiza sus datos.

Pero que es lo que se protege, al respecto la mayoría de autores coinciden en los siguientes aspectos:

a) Proteger al individuo ante el "manejo o manipulación, no autorizada, de sus datos personales" que se encuentren en medios o formas electrónicas.
b) Los resultados de procesamientos informáticos, "deben ser identificable con el titular de los mismos" puesto que es muy fácil conocer características de la personalidad y de la intimidad de las personas.
c) Y, por último, el consentimiento no autorizado del uso de los datos, para fines en los que el titular no autorizo o fue obligado a darlos.

A continuación mapa mental de protección de datos en España. Fuente:

http://abesdih.wordpress.com/2011/10/06/tema-2-proteccion-de-datos-mapa-conceptual/

(Ver Anexo 14)

TERCERA PARTE
TÉCNICA DIGITAL FORENSE

CONCEPTUALIZACIÓN.

La técnica digital forense se denomina también: Informática Forense, es interdisciplinar, vinculada científicamente a la criminalística y a la ciencia forense.

La ciencia forense es el método científico que da la pauta de la recopilación y el examen de evidencias de la información sobre hechos acontecidos, que luego se utilizan en un tribunal de justicia como prueba.

La palabra forense viene del latín "forensis", que significa, "perteneciente o relativo al foro". "de o ante el foro". Fórum: El foro. En el Derecho Romano, una infracción penal significaba presentar el caso ante un grupo de personas públicas en el foro. Tanto la persona que se la acusaba por haber cometido el crimen como el denunciante tenían que explicar su versión de los hechos. La argumentación, las pruebas y el comportamiento de cada persona determinaban el veredicto del caso. "forumagere": Administrar justicia.

FORENSE.

Forense1. (Del lat. forensis). 1. adj. Perteneciente o relativo al foro. 2. adj. ant. Público y manifiesto. 3. com. Médico forense.(Fuente: http://lema.rae.es/drae/?val=forense)

Forense2. Adj. 1.- Relativo a los tribunales de justicia. Adj./s.com. 2.- Se aplica al médico que está encargado por un juez de señalar el origen de las lesiones sufridas por una herida, o, especialmente, de determinar las causas que han provocado la muerte de una persona. (Fuente: Diccionario Manual de la Lengua Española Vox. © 2007 Larousse Editorial, S.L.).

Este es el origen de los dos usos modernos de la palabra forense, como una forma de evidencia legal y como una categoría de presentación pública.

Se denominan ciencias forenses, al conjunto de disciplinas auxiliares que la componen, la criminalística es una disciplina que usa un conjunto de técnicas y procedimientos de investigación cuyo objetivo es el descubrimiento, explicación y prueba de los delitos, así como la verificación de sus autores y víctimas. La criminalística se vale de los conocimientos científicos para reconstruir los hechos.

"Mientras el Derecho penal determina lo que se considera delito y la criminología se ocupa de estudiar la causación del delito, la criminalística tiene como finalidad el descubrimiento del delito. Ese descubrimiento se refiere al cómo, dónde, cuándo y quién del delito, aspectos que dan lugar a una serie de actividades, todas las cuales constituyen la criminalística. La importancia de esta disciplina se acredita si tenemos en cuenta que en la práctica policial y judicial, donde se enfrentan las garantías constitucionales y la responsabilidad jurídico-social, no basta sólo saber que un hecho punible se ha cometido, sino que, además, se necesita probar cómo, dónde, cuándo y quién realizó el mismo para imponer una sanción. Recordamos, entre otros supuestos de importancia penal, el delito imposible, la prescripción, ejercicio de las acciones penales, autoría, etc." (Por el Dr. MANUEL LOPEZ-REY. En: "Enciclopedia Jurídica Omeba". Versión virtual-PDF.2012. Licencia de uso libre).

En la actualidad la criminalística está relacionada a la ciencia forense por lo que su denominación es correcta, y el término "forense" es sinónimo de "legal" y referente a "prueba" en los tribunales de justicia. Por lo que el término está estrechamente asociado con el campo científico que muchos diccionarios incluyen el significado que equipara el término "forense" con "ciencia forense".

"La criminalística, llamada con justicia "la enciclopedia del peritaje", es la que busca y proporciona las pruebas en la primera etapa. La que establece el proceso fáctico en relación con la existencia del hecho,

las circunstancias que lo rodearon y la identificación de las personas responsables; por ello repetimos que para afrontar la primera tarea, la del conocimiento material del hecho, en todas sus circunstancias y accidentes, tanto el abogado como el juez deben dominar el campo de la Criminalística". (pág. 44. Duran A. Jaime, Prof. "Criminalística utilización científica de la prueba material en la práctica forense. Tomo 1. Ediciones de la Universidad Católica. Quito 1977).

La técnica digital forense, es: "la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal". (Luis Ángel Gómez R, en:"La informática forense, una herramienta para combatir la Ciber-delincuencia." Argentina).

El mismo autor, continua: "Ampliaría diciendo que es: Una ciencia que busca reproducir científicamente con una metodología estricta de los hechos acontecidos y su correlación para determinar el grado de impacto, y posteriormente establecer en coordinación con otros entes intervinientes, mecanismos tendientes a evitar nuevamente su ocurrencia, que van desde el marco normativo hasta la utilización de mecanismos técnicos". (Ibídem).

Por lo tanto la técnica digital forense, es un método científico porque supone la adquisición de nuevos conocimientos, mediante el estudio de la evidencia observable y medible, aplicando un razonamiento lógico, elaborando modelos e hipótesis y corrigiendo o mejorando estas últimas según se obtenga de la "evidencia".

La característica principal de este método científico es que los resultados deben ser objetivos e imparciales, lo que implica un alto grado de profesionalidad y responsabilidad ética en el análisis técnico digital forense.

La metodología que se aplique debe ser estandarizada, conocida, inteligenciada y practicada, de forma que otros técnicos investigadores, utilizando los mismos métodos, lleguen a las mismas conclusiones.

Si esto no se logra, no existe la posibilidad de garantizar que "la evidencia" tenga valor probatorio en un proceso legal.

Otro concepto profundiza diciendo: "La Informática Forense es la ciencia que estudia la identificación, el almacenamiento, la protección, la recuperación, la documentación, y cualquier otra forma de tratamiento de datos informáticos para ser evaluados en un proceso legal y estudios, con fines probatorios, las técnicas y herramientas para el examen de los sistemas de información metodológicas". (Fuente: www.wikipedia.org)

Desarrollando este último concepto tenemos:

Identificación: El primer y más importante paso que un forense digital debe hacer antes de iniciar su investigación, es identificar el equipo de prueba y su posible ubicación. Una prueba digital puede de hecho estar contenida en diferentes tipos de medios, tales como discos duros, medios extraíbles, o en un archivo de registro en el servidor (o en la actualidad en la "nube").

Encontrar la información "vulnerada" es una condición necesaria para el forense digital.

Almacenamiento: El forense digital debe garantizar el máximo cuidado para preservar la integridad del equipo de prueba. Los datos originales no se deben cambiar ni corromperlos, luego proceder a respaldar una copia "bit" a "bit"* (Llevar a cabo una operación lógica AND bit a bit entre dos valores enteros. El operador & bit a bit realiza una operación lógica AND bit a bit entre las dos expresiones, y, para ello, utiliza el bit correspondiente de ambas. Los bits del resultado se establecen en 1 si y solo si los dos bits (para el bit actual que se resuelve) de las expresiones de entrada tienen el valor 1; de otro modo, el bit del resultado se establece en 0. Si las expresiones de la izquierda y de la derecha tienen tipos de datos de entero diferentes (por ejemplo, expression de la izquierda es de tipo smallint y expression de la derecha es de tipo int), el argumento del tipo de datos más pequeño se convierte al tipo de datos mayor. En este caso, el valor smallint en expression se convierte

en int. Termino informático. (en: http://technet.microsoft.com/es-es/library/ms174965(v=sql.110).aspx)

En este proceso el forense digital lleva a cabo el análisis. Después de hacer una copia de lo que necesita para verificar la coherencia con respecto a los datos originales, por lo que los datos se firman digitalmente tanto el original y la copia, los cuales deben coincidir.

Protección: Los datos originales se deben proteger de la manera más apropiada en función de los medios o equipos en los que se encuentre. Las causas de la alteración de medios magnéticos o medios ópticos, por ejemplo, son muy diferentes. También debe velar por una "cadena de custodia", que es un documento que abaliza lo que se ha realizado y el permiso para que el forense digital, tenga acceso a datos originales y realice las copias pertinentes.

La extracción es el proceso por el cual el forense digital, utiliza diferentes técnicas y por su experiencia, ubica los datos informáticos y los extrae.

Documentación: todo el trabajo dela actividad forense digital, debe estar constantemente documentado, desde el inicio de la investigación hasta el final del proceso. La documentación incluye, además de la "cadena de custodia", el análisis de los datos que se encontró y el proceso seguido. La documentación debe ser minuciosa y fundamental para minimizar las objeciones y explicar cómo se realizó la extracción, y se fortalece realizando un proceso similar en la copia.

También dentro del término forense encontramos varias definiciones como estas:

Computación forense (computerforensics).- Que entendemos por disciplina de las ciencias forenses, que considerando las tareas propias asociadas con la evidencia, procura descubrir e interpretar la información en los medios informáticos para establecer los hechos y formular las hipótesis relacionadas con el caso; o como la disciplina científica y especializada que entendiendo los elementos propios de

las tecnologías de los equipos de computación ofrece un análisis de la información residente en dichos equipos.

Forensia en redes (networkforensics).- Es un escenario aún más complejo, pues es necesario comprender la manera como los protocolos, configuraciones e infraestructuras de comunicaciones se conjugan para dar como resultado un momento específico en el tiempo y un comportamiento particular.

Esta conjunción de palabras establece un profesional que entendiendo las operaciones de las redes de computadores, es capaz, siguiendo los protocolos y formación criminalística, de establecer los rastros, los movimientos y acciones que un intruso ha desarrollado para concluir su acción. A diferencia de la definición de computación forense, este contexto exige capacidad de correlación de evento, muchas veces disyuntos y aleatorios, que en equipos particulares, es poco frecuente.

Es la captura, almacenamiento y análisis de los eventos de una red, para descubrir el origen de un ataque o un posible incidente. (Fuente: NFTA (Network Forensic Analysis Tool)

Forensia digital (digital forensics).-

Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática.

Importancia de la técnica digital forense.

"High-tech crime is one of the most important priorities of the Department of Justice". Con esta frase podemos ver cómo poco a

poco los crímenes informáticos, su prevención, y procesamiento se vuelven cada vez más importantes. Esto es respaldado por estudios sobre el número de incidentes reportados por las empresas debido a crímenes relacionados con la informática.

Objetivos de la técnica digital forense.

1. La compensación de los daños causados por los criminales o intrusos.

2. La persecución y procesamiento judicial de los criminales.

3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia, tema que lo profundizaremos en el acápite correspondiente.

Usos de la técnica digital forense.

Existen varios, muchos de estos usos provienen de la vida diaria, y no tienen que estar directamente relacionados con investigación científica, o la informática forense, entre estas tenemos:

1. Prosecución Criminal: Evidencia incriminatoria puede ser usada para procesar una variedad de crímenes, incluyendo homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.

2. Litigación Civil: Casos que tratan con fraude, discriminación, acoso, divorcio, pueden ser ayudados por la informática forense.

3. Investigación de Seguros: La evidencia encontrada en computadores, puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.

4. Temas corporativos: Puede ser recolectada información en casos que tratan sobre acoso sexual, robo, mal uso o apropiación de información confidencial o propietaria, o aún de espionaje industrial.

5. Mantenimiento de la ley: La técnica digital forense puede ser usada en la búsqueda inicial de órdenes judiciales, así como en la búsqueda de información una vez se tiene la orden judicial para hacer la búsqueda exhaustiva.

Nuestro Código orgánico integral penal –COIP* (vigente desde el 10 de agosto del 2014), en su Art. 500, numeral 1, claramente tipifica que, en la investigación se seguirán las siguientes reglas:

"1. EI análisis, valoración, recuperación y presentación del **contenido digital** almacenado en dispositivos o sistemas informáticos se realizará, a través de **técnicas digitales forenses**".

Es decir el análisis investigativo utiliza como método el científico y aplica la criminalística, la informática forense, o lo que es lo mismo la pericia (técnica) digital forense, cuando la norma adjetiva penal refiere a todo "contenido digital", que es: "Todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí" (Art 500. COIP).

Nacen de esta forma nuevas instituciones jurídicas en el derecho procesal penal, que deben ser analizadas y estudiadas a profundidad, entre estas tenemos la "prueba penal digital" que lo establece el COIP, art. 499 en la regla 6. "Podrá admitirse como medio de prueba todo **contenido digital** conforme con las normas de este Código".

En concordancia con la ley de Comercio electrónico, firmas electrónicas y mensajes de datos, vigente desde el año 2002, que norma la validez jurídica de los mensajes de datos y la evacuación de la prueba electrónica en los tribunales de justicia.

Tema que lo desarrollaremos a profundidad en el acápite correspondiente.

MODELOS Y METODOLOGÍAS PARA EL ANÁLISIS DE LA TÉCNICA DIGITAL FORENSE.

El aspecto más importante para un análisis forense digital es seguir la metodología estándar de investigación, y definir bien el problema forense al que ha sido sometido.

El análisis forense digital ha experimentado avances científicos, con el objetivo de ayudar al investigador en el manejo del proceso de investigación digital, con el propósito de informar, formar y estandarizar las investigaciones digitales que permitan obtener una conclusión al término de su investigación, la investigación forense está compuesta de múltiples facetas, que incluyen aspectos tecnológicos, procedimientos y aspectos legales, por lo que se vislumbra la necesidad de un modelo de Análisis Forense Integral, varios modelos de análisis forense han sido desarrollados pero hasta ahora ninguno ha sido aceptado universalmente.

Parte de la razón para esto puede ser debido al hecho de que muchos de los modelos de procesos fueron diseñados para un entorno específico, como el cumplimiento de la ley, y que por lo tanto no podrían aplicarse fácilmente en otros entornos, como respuesta a incidentes.

Esta es una lista de los principales modelos desde 2001 en orden cronológico:

El Modelo Forense Digital Abstract	Reith, et al.,	2002
El proceso de investigación digital integrado	Carrier y Spafford	2003
Un modelo ampliado de la ciberdelincuencia Investigaciones	Ciardhuain,	2004
El Proceso de Mejora de Investigación Digital Modelo,	Baryamureeba y Tushabe	2004

La escena del crimen Modelo de Análisis Digital	Rogers	2004
Un marco jerárquico y basado en objetivos para el Proceso de Investigaciones Digitales	Beebe & Clark,	2004
Marco para una Investigación Digital	Kohn, et al	2006
El Cuatro Pasos del Proceso Legal	Kent, et al	2006
FORZA - Digital marco de investigación forense	Ieong,	2006
Flujos de proceso para Cyber Forensics de Entrenamiento y Operaciones	Venter,	2006
El Modelo de Proceso Común	Freiling y Schwittay	2007
El bidimensional Evidencia Confiabilidad Amplificación Modelo de Procesos	Khatir, et al	2008
El Marco de Investigación Forense Digital	Selamat, et al	2008
El modelo de investigación sistemática Forense Digital	Agarwal, SRD-FIM, et al	2011

Realización: Juan José Páez Rivadeneira.

Expliquemos algunos de estos:

El modelo DFRWS.

El Taller de Investigación Forense Digital (DFRWS) se inició en agosto de 2001 para que los investigadores académicos y forenses

digitales investigadores y profesionales juntos para la discusión activa que aborda tres objetivos principales:

Definir la necesidad y crear los procesos para la incorporación de un método científico riguroso como inquilino fundamental de la disciplina en evolución de la ciencia forense digital.

Desarrollar una agenda de investigación que tenga en cuenta los requisitos de practicante, múltiples entornos de investigación y hace hincapié en la facilidad de uso de bienes del mundo.

El descubrimiento, explicación y presentación de pruebas concluyentes, persuasivo que se reunirá con el escrutinio de los tribunales y otros tomadores de decisiones en entornos militares y civiles.

El modelo DFRWS (Digital Forensic Research Workshop), el cual fue desarrollado como un sistema entre los años 2.001 y 2.003 en el Digital Forensic Research Workshop, introduce clases de acción en la investigación digital, las cuales sirven para clasificar las actividades de una investigación en grupos, este modelo no dicta que acciones en particular deben ser perseguidas, puesto que proporciona una lista de técnicas, lo específico del sistema debe ser claramente redefinido para cada investigador particular.

Ver: **¡Error! Referencia de hipervínculo no válida.**

Modelo de Reith, Carr y Gunsch.

El modelo presentado por Reith, Carr y Gunsch es muy similar al sistema DFRWS, este modelo incluye preservación, recolección, análisis y presentación, clases definidas en formas similares a las de DFRWS, este modelo también agrega soporte para la preparación de herramientas y la formulación dinámica de acercamientos de investigación, y soporta iteraciones libres de clases de actividad individuales.

El modelo de Ciardhuain.

El modelo propuesto por Ciardhuain, está basado en modelos previos, pero expone una arquitectura de cascada aumentada, las clases de actividad del modelo están doblemente ligadas, de manera que la búsqueda de trabajo en una clase de actividad puede causar una iteración de algunos o todos los trabajos en las clases de actividad anteriores, puesto que la inclusión de estructuras conocidas como flujo de información permite una comprensión más profunda de la fuente de evidencias y otros datos, este flujo debe estar definido sobre una base organizacional, pero puede aplicarse a diferentes investigaciones dentro de la misma organización.

El modelo Beebe y Clark.

El modelo propuesto por Beebe y Clark, proporciona la estructura para las actividades mediante fases que consisten de múltiples sub fases, que van más allá que el agrupamiento por actividades, en este modelo las sub fases están basadas en objetivos, más que estrictamente en actividades, las sub fases basadas en objetivos caen en una fase particular y consisten en una jerarquía de actividades que están subordinadas al objetivo particular, este modelo incluye los principios de la investigación digital sobre todas las fases y sub fases, lo cual afecta la forma en que están representadas como objetivos, más que como tareas específicas.

Metodología Forense del Departamento de Justicia de los Estados Unidos de Norte América (DOJ).

El tema de los Delitos Informáticos y Propiedad Intelectual (CCIPS) es el tema responsable de la implementación de estrategias nacionales del Departamento en la lucha contra los delitos informáticos y de propiedad intelectual en todo el mundo. CCIPS previene, investiga y enjuicia los delitos informáticos mediante la colaboración con otras agencias gubernamentales, el sector privado, instituciones académicas, y sus homólogos extranjeros. Sección abogados trabajan para mejorar

los delincuentes de la red interna y la infraestructura legal, tecnológica internacional, y operativa a perseguir con mayor eficacia.

Responsabilidades de ejecución de la Sección contra delitos contra la propiedad intelectual son igualmente múltiples facetas. Propiedad Intelectual (IP) se ha convertido en uno de los motores económicos principales de los Estados Unidos, y la nación es un objetivo de elección para los ladrones de material protegido por derechos de autor, marca registrada, o la designación de secreto comercial. En la consecución de todos estos objetivos, CCIPS abogados salen regularmente investigaciones complejas, resolver problemas legales y de investigación únicas planteadas por las tecnologías informáticas y de telecomunicaciones emergentes; litigar casos; proporcionar apoyo en litigios a otros fiscales; entrenar federales, estatales, y las fuerzas del orden locales; comentar y proponer legislación; e iniciar y participar en los esfuerzos internacionales para luchar contra la delincuencia informática y la propiedad intelectual.

El laboratorio de Cibercrimen: Computer Crime and Intellectually Property Section, de los Estados Unidos, desarrolló un diagrama de flujo en el cual se describe la metodología de análisis forense de varias agencias federales, los elementos claves del Cómputo Forense se listan a continuación:

· Empleo de métodos científicos.
· Recolección y Preservación.
· Validación.
· Identificación.
· Análisis e Interpretación.
· Documentación y Presentación.

Tres fases: Preparación-Extracción, Identificación y Análisis, conforman el núcleo principal del análisis forense.

(Ver Anexo 15)

Las fases se explican partiendo de que los analistas han obtenido de manera previa la imagen forense de los datos, así como los recursos

necesarios para el análisis, hasta que se elabore el reporte y el análisis del nivel del caso.

Primera fase es la "Validación", del hardware y software a emplear "Preparación y Extracción", los analistas deben realizar un duplicado de los datos forenses recopilados, sin contaminar ni alterar la integridad de los datos. No se trabaja sobre la "evidencia original" la cual debe ser protegida por el empleo de la "cadena de custodia".

Segunda fase es la "Identificación", en la cual los analistas repiten el proceso de identificación por cada elemento compilado, si el elemento no es "relevante" para la investigación es marcado como procesado y movido; si un elemento es "relevante" para la investigación el analista lo documenta como elemento "relevante" para la investigación.

Tercera fase de "Análisis", los investigadores relacionan todos los datos encontrados y bosquejan una imagen completa del caso, para cada elemento relevante, respondiendo a las preguntas ¿Quién?, ¿Cuándo?, ¿Dónde? Y ¿Cómo?, explicando lo que han encontrado y justificando el porqué es importante el análisis de toda la información relacionada con el caso.

El proceso puede ser analizado varias veces, para responder a la solicitud de investigación y se procede a elaborar el reporte de resultados, documentando y detallando los hallazgos forenses.

Metodología Forense del Instituto Nacional de Estándares de Tecnología (NIST).

El Instituto Nacional de Estándares de Tecnología (NIST), es una Agencia Federal no regulatoria dentro del Departamento de Comercio de los Estados Unidos y que tiene como misión promover la innovación y competitividad industrial mediante estándares y tecnología de forma que se mejore la seguridad económica y la calidad de vida.

El análisis forense es necesario en diferentes situaciones, tales como la recopilación de evidencia para los procedimientos judiciales y medidas

disciplinarias internas, manejo de incidentes relacionados con código malicioso y problemas operativos, entre otros, este proceso de análisis forense de esta metodología es descrito en la Figura 2.11 mostrada a continuación.

(Ver Anexo 16)

La metodología de prueba desarrollado por NIST es impulsado por sus funcionalidad. Las actividades de las investigaciones forenses se dividen en funciones o categorías discretas, como la protección de escritura del disco duro, imágenes de disco, la búsqueda de cadena, etc. Una metodología de la prueba se desarrolla a continuación, para cada categoría.

El proceso de prueba CFTT está dirigido por un comité directivo compuesto por representantes de la comunidad de las fuerzas del orden. Actualmente el comité directivo selecciona categorías de herramientas para la investigación y herramientas dentro de una categoría para la prueba real por el personal CFTT. Un proveedor puede solicitar la prueba de una herramienta, sin embargo, el comité de dirección hace que la decisión acerca de qué herramientas para poner a prueba.

1. Proceso de desarrollo de la especificación

Después de una categoría de la herramienta y al menos una herramienta es seleccionada por el comité de dirección del proceso de desarrollo es el siguiente:

Personal del NIST y aplicación de la ley desarrolla un documento de requisitos, las afirmaciones y los casos de prueba (llamada la especificación categoría de herramientas).

La especificación de la categoría de herramientas se contabiliza en la web para su revisión por los miembros de la comunidad forense y para el comentario público por otras partes interesadas.

Observaciones pertinentes y la retroalimentación se incorporan en la especificación.

Un entorno de prueba está diseñado para la categoría de herramienta.

2. Proceso de prueba de la herramienta

Después de una especificación de categoría ha sido desarrollada y una herramienta seleccionada, el proceso de prueba es el siguiente:

NIST adquiere la herramienta para ser probada. NIST revisa la documentación de la herramienta. NIST selecciona casos de prueba pertinentes en función de las características soportadas por la herramienta. NIST desarrolla estrategia de prueba. NIST ejecuta pruebas. NIST produce informe de la prueba. Comité Directivo revisa informe de la prueba. Opiniones Veedora prueban informe. Mensajes NIST soporte de software para web. DHS [cyberfetch.org] puestos a prueba informe a la web.

Fuente: http://www.cftt.nist.gov/Methodology_Overview.htm

Metodología de Análisis Forense de la Red Europea de Institutos Forenses (ENFSI).

La Tecnología de la Información Forense (FIT) de interés Grupo de trabajo, "todas las ciencias y disciplinas técnicas combinan para permitir el examen del material que contiene la información (ordenadores, redes, dispositivos electrónicos, etc....) para ayudar a una investigación y, finalmente, presentar evidencia para un juicio."

Las principales actividades refieren a análisis de datos informáticos y sus aspectos técnicos de las investigaciones de Internet así como examen de dispositivos electrónicos.

Objetivos y Misión:

Para mantener un FIT-WG que cumple con los objetivos globales de la ENFSI. Para desarrollar y promover en los laboratorios miembros de la ENFSI una disciplina de la informática forense. Cultivar la cooperación con otros grupos de trabajo y comités que se ocupan de

la evidencia digital. Para establecer la calidad en todos los aspectos de la tecnología de la información forense. Para cultivar las relaciones con las organizaciones técnicas significativas

Con el fin de lograr estos objetivos:

Se organizan reuniones FIT GT cada año, existen comités para seguridad y calidad de la investigación y desarrollo.

En la ENFSI, se desarrollan "Estándares Basados en Desempeño para los Profesionales de las Ciencias Forenses" (Performance Based Standars for Forensic Science Practicioners), los cuales son aplicados por todos los profesionales forenses adscritos a la ENFSI, estos estándares pueden ser aplicables en todos los Sistemas de Justicia Penal, puesto que cubren todo el proceso forense desde la primera acción que el oficial realiza en la escena del incidente, pasando por la inspección de la escena, el análisis en un laboratorio, hasta la interpretación y presentación del informe de resultados para ser mostrado ante una corte; las acciones no son prescriptivas y reconocen que existe más de una forma para llevar a cabo una tarea.

(Ver Anexo 17)

Metodología de Análisis Forense del EC-COUNCIL.

El EC-COUNCIL es una organización dedicada al desarrollo de cursos y al otorgamiento de certificaciones en el área de Seguridad Informática y Comercio Electrónico, en dicho modelo se realiza la preparación de un caso para solución de un problema forense, estas etapas se muestran en el siguiente diagrama:

(Ver Anexo 18)

Estas metodologías contienen las medidas estándar que se realizan durante el curso de un l evento:

Evaluación inicial: en esta fase el forense digitales se hace cargo del caso y tratar de determinar las características principales (análisis de

la escena del crimen, las personas involucradas y las herramientas tecnológicas que serán estudiados).

Preparación de un perfil de investigación: determinación de los pasos de operación necesarios para el desempeño del caso, tomando en consideración el tiempo requerido para cada caso.

La determinación de los recursos necesarios (hardware, software y personal profesional).

Encontrar evidencia.

Copia de la prueba (en el nivel más bajo posible, dependiendo de la ayuda específica).

Evaluación de riesgos.

La minimización de riesgos y el establecimiento de una cadena de custodia.

Análisis y recuperación de evidencia digital.

Análisis de los datos recuperados.

Redacción del informe final.

La evidencia es la etapa más importante en el trabajo de un forense digital.

ESTÁNDARES INTERNACIONALES

CASO.

Grupos de interés de Canadá, Estados Unidos, Reino Unido, Francia, Nueva Zelanda y otros países (Comisión Treadway) realizaron muchos esfuerzos para definir formalmente el Modelo de Control Interno COSO, que contiene objetivos y elementos del control interno, así

mismo establecieron los roles de todos los interesados incluyendo la Junta Directiva, los directivos, los jefes de mandos medios, los supervisores y empleados.

Definición:

La Comisión Treadway estableció la siguiente definición de control interno la cual ha sido adoptada ampliamente a nivel internacional.

"El control interno es un proceso llevado a cabo por la junta directiva de la entidad, los directivos y otro personal designado para proveer garantía razonable en cuanto al logro de objetivos en las tres siguientes categorías:

• Eficiencia y eficacia de las operaciones
• Razonabilidad de los estados financieros
• Cumplimiento con las políticas y procedimientos internos y con las leyes y regulaciones aplicables".

Componentes

El marco integrado de control consta de cinco componentes interrelacionados:

• Ambiente de control
• Evaluación de riesgos
• Actividades de control
• Información y comunicación
• Supervisión

(Ver Anexo 19)

Ambiente de control

El ambiente de control refleja el espíritu ético vigente en una entidad respecto del comportamiento de los agentes, la responsabilidad con

que encaran sus actividades, y la importancia que le asignan al control interno.

Los principales factores del ambiente de control son:

• La filosofía y estilo de la dirección y la gerencia.
• La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento.
• La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.
• Las formas de asignación de responsabilidades y de administración y desarrollo del personal.
• El grado de documentación de políticas y decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

Evaluación de riesgos

Se define como riesgo la probabilidad de que un suceso ocurra y provoque pérdidas. El control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las organizaciones.

Cada entidad enfrenta una variedad de riesgos de fuentes internas y externas que deben ser evaluadas. La evaluación de riesgos comprende su identificación y análisis, conformando una base para determinar cómo los riesgos deben ser manejados. Es necesario entonces, que la organización posea mecanismos para identificar y manejar riesgos nuevos debido a las condiciones cambiantes de la economía, industria, condiciones reglamentarias y operacionales.

Actividades de control

Están constituidas por los procedimientos específicos establecidos como un reaseguro para el cumplimiento de los objetivos, orientados primordialmente hacia la prevención y neutralización de los riesgos.

Las actividades de control se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos según lo expresado en el punto anterior: conociendo los riesgos, se disponen los controles destinados a evitarlos o minimizarlos.

A continuación se lista una gama de actividades de control, sin ser la totalidad de las mismas:

• Análisis efectuados por la dirección.
• Seguimiento y revisión por parte de los responsables de las diversas funciones o actividades.
• Comprobación de las transacciones en cuanto a su exactitud, totalidad, y autorización pertinente: aprobaciones, revisiones, cotejos, re cálculos, análisis de consistencia, pre numeraciones.
• Controles físicos patrimoniales: arqueos, conciliaciones, recuentos.
• Dispositivos de seguridad para restringir el acceso a los activos y registros.
• Segregación de funciones.
• Aplicación de indicadores de rendimiento.

Información y comunicación

En este elemento del sistema de control interno se diferencian la información de la comunicación; la primera son los datos necesarios para cumplir con las funciones, y la comunicación es la manera como la información fluye.

La información relevante debe ser captada, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores permitiendo asumir las responsabilidades individuales.

La comunicación es inherente a los sistemas de información. Las personas deben conocer a tiempo las cuestiones relativas a sus responsabilidades de gestión y control. Cada función ha de especificarse con claridad, entendiendo en ello los aspectos relativos

a la responsabilidad de los individuos dentro del sistema de control interno.

La existencia de líneas abiertas de comunicación y una clara voluntad de escuchar por parte de los directivos resultan vitales.

Supervisión

Los sistemas de control interno necesitan ser monitoreados. El monitoreo es un proceso que evalúa la calidad del comportamiento de los sistemas a través del tiempo.

Incumbe a la dirección la existencia de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica para mantenerla en un nivel adecuado.

Modalidades de supervisión

El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales.
Actividades continuas

Las primeras son aquellas incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real y arraigadas a la gestión, generan respuestas dinámicas a las circunstancias que pueden surgir.

Evaluaciones puntuales

En cuanto a las evaluaciones puntuales, corresponden las siguientes consideraciones:

a) Su alcance y frecuencia están determinados por la naturaleza e importancia de los cambios y riesgos que éstos conllevan, la competencia y experiencia de quienes aplican los controles, y los resultados de la supervisión continuada.

b) Son ejecutados por los propios responsables de las áreas de gestión, la auditoria interna y los auditores externos.
c) Constituyen en sí todo un proceso dentro del cual, aunque los enfoques y técnicas varíen, priman una disciplina apropiada y principios ineludibles.
d) Responden a una determinada metodología, con técnicas y herramientas para medir la eficacia directamente o a través de la comparación con otros sistemas de control probadamente buenos.
e) El nivel de documentación de los controles varía según la dimensión y complejidad de la entidad.
f) Debe confeccionarse un plan de acción que contemple:

- El alcance de la evaluación
- Las actividades de supervisión continuadas existentes.
- La tarea de los auditores internos y externos.
- Áreas o asuntos de mayor riesgo.
- Programa de evaluaciones.
- Evaluadores, metodología y herramientas de control.
- Presentación de conclusiones y documentación de soporte
- Seguimiento para que se adopten las correcciones pertinentes.
- Mediante un esquema de controles incorporados como el descrito:
- Se fomentan la calidad, las iniciativas y la delegación de poderes.
- Se evitan gastos innecesarios.
- Se generan respuestas ágiles ante circunstancias cambiantes.

COBIT.

COBIT es una herramienta para la administración y operación a un nivel superior a los estándares de tecnología para la administración de sistemas de información.

El objetivo principal de COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

El concepto fundamental del Marco Referencial de COBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.

Dominios de COBIT

Dentro de los niveles de actividades de TI de COBIT (2002) distinguimos los siguientes dominios: planeación y organización, adquisición e implementación, entrega y soporte y monitoreo.

Procesos y Objetivos de Control aplicables

A continuación se detallan los procesos y actividades que aplican para este estudio.

PLANEACIÓN Y ORGANIZACIÓN

En el caso de estudio, se aplica para lograr un balance entre las oportunidades de tecnología de información y los requerimientos del negocio, aprovechar la tecnología disponible para posibilitar la estrategia del negocio, mantener tareas y responsabilidades definidas bajo una dirección efectiva, asegurar el financiamiento y el control de los recursos, aplicar técnicas de administración de proyectos y planificar e implementar estándares de calidad en los sistemas.

Definición de un Plan Estratégico de Tecnología de Información

Tecnología de información como parte del Plan de la Organización a corto y a largo plazo1
Plan a largo plazo de Tecnología de Información.
Evaluación de los sistemas existentes.
Determinación de la Dirección Tecnológica.

Planes de Adquisición de Hardware y Software.
Definición de la Organización y de las Relaciones de TI.
Responsabilidad del aseguramiento de la calidad.
Responsabilidad por la seguridad lógica y física.
Propiedad de datos y sistemas.
Personal clave de TI.
Procedimientos y políticas para el personal contratado.
Manejo / Administración de la Inversión en Tecnología de Información.
Presupuesto Operativo anual para la función de Servicios de Información.
Monitoreo de Costo - Beneficios.
Justificación de Costo - Beneficios .
Administración de Proyectos.
Plan de Aseguramiento de Calidad de Sistemas.
Administración de Calidad.
Marco Referencial para la adquisición y mantenimiento de la Infraestructura de Tecnología.
Relaciones con terceras partes en su rol de implementadores.
Estándares para la documentación de programas.
Estándares para Pruebas de Sistemas.
Documentación de las Pruebas del Sistema.

ADQUISICIÓN E IMPLEMENTACIÓN

Nos asegura un efectivo y eficiente enfoque para satisfacer los requerimientos del usuario, proporciona plataformas apropiadas para soportar las aplicaciones, verifica y confirma que la solución (nuevo sistema) sea adecuada para el propósito deseado.
- Identificación de soluciones
- Requerimientos de servicios de terceros
- Adquisición de Productos de Software
- Contratos para la Programación de Aplicaciones
- Adquisición y mantenimiento de la Arquitectura Tecnológica
- Evaluación de nuevo hardware y software

- Instalación y Acreditación de Sistemas

ENTREGA DE SERVICIOS Y SOPORTE.

Provee controles para asegurar que los roles de terceras partes (proveedores de software) estén claramente definidos y que satisfagan los requerimientos, además sirve para garantizar la seguridad de los sistemas contra uso no autorizado, daño o pérdida.
- Administrar servicios de terceros
- Contratos con terceros
- Calificaciones de terceros
- Contratos de outsourcing
- Monitoreo
- Garantizar la seguridad de sistemas
- Manejo de incidentes

MONITOREO

Aplicable para asegurar el logro de los objetivos establecidos, incrementar los niveles de confianza entre la organización, clientes y proveedores externos a través de evaluaciones de cumplimiento de compromisos contractuales o revisiones de auditoría.

Monitoreo del Proceso.
Obtención de aseguramiento independiente.
Evaluación independiente de la efectividad de los proveedores externos de servicios.

Aseguramiento independiente del cumplimiento de leyes y requerimientos regulatorios y compromisos contractuales con proveedores externos de servicios.

Proveer Auditoría Independiente.

(Ver Anexo 20)

IEEE 730.

"IEEE corresponde a las siglas de The Institute of Electrical and Electronics Engineers, el Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Es la mayor asociación internacional sin fines de lucro formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, ingenieros en electrónica, científicos de la computación, ingenieros en informática e ingenieros en telecomunicación."

Logo de IEEE

Su trabajo es promover la creatividad, el desarrollo y la integración, compartir y aplicar los avances en las tecnologías de la información, electrónica y ciencias en general para beneficio de la humanidad y de los mismos profesionales. Uno, entre los más de 900 estándares publicados es el IEEE 730.

Definición, el estándar IEEE 730 - Plan de aseguramiento de la calidad del software, establece el puente entre la gestión de la calidad y la ingeniería del software; comprende requerimientos para llevar a cabo un Plan de Garantía de Calidad asociado a un proyecto de software. Cabe señalar, que mientras que la aplicación del ISO 9000-3 está dirigida a toda la organización, el IEEE 730 es para aplicación en un único proyecto dentro de esa organización.

El IEEE 730 describe el conjunto de actividades sistemáticas necesarias para aportar la confianza en que el software satisfará los requisitos dados de calidad. Esta norma aplica para el desarrollo y

mantenimiento de software crítico; la norma nos ayuda a evaluar el proceso mediante el cual se desarrolla el software.

A su vez el IEEE 730 tiene relación con otros estándares como el IEEE 828 y el 1219, que son de utilidad para aplicar las necesidades expuestas en el 730.

Recomendaciones más aplicables siguiendo el estándar IEEE, al iniciar un proyecto software hay que:

• Seleccionar uno o varios modelos del ciclo de vida, y concretarlo luego en uno determinado para dicho proyecto.
• Definir los aspectos relacionados con la financiación y viabilidad del proyecto.
• Definir las metodologías, técnicas y herramientas a utilizar.
• Planificar la gestión del proyecto software. Esta planificación debe incluir y describir:

1. El día a día del proyecto, con los correspondientes controles de auditorias y revisiones
2. La planificación del aseguramiento de la calidad del software (SQA)
3. La planificación de la documentación del proyecto

ISO 9000-3.

Esta parte de la ISO 9001:2000 tiene vinculación con situaciones donde se desarrolla software específico como parte de un contrato, siguiendo las especificaciones del comprador; sin embargo, puede ser de valor en otras situaciones.

Logo de la ISO

Fuente: www.iso.org/

La ISO 9000-3 intenta proporcionar directrices aplicables cuando un contrato entre dos partes requiere la demostración de la capacidad de un proveedor para desarrollar, suministrar y mantener productos de software, en otras palabras proporciona una guía para asegurar la calidad del software.

En la naturaleza del desarrollo del software algunas actividades están relacionadas a fases particulares del proceso de desarrollo, mientras que otras pueden aplicarse a través de todo el proceso.
Cláusulas

Se presenta en tabla adjunta el índice de cláusulas que comprenden la norma. Cada cláusula está identificada con un número.

Índice de cláusulas de la ISO 9000-3

NÚMERO	CLÁUSULA
4	Sistema de calidad-modelo
4.1	Administración de la Responsabilidad
4.2	Sistema de Calidad
4.3	Auditorias Internas del Sistema de Calidad
4.4	Acción Correctora
5	Sistema de calidad -actividades de ciclo de vida
5.1	General
5.2	Revisión del Contrato
5.3	Especificación de los requerimientos de la Organización
5.4	Planificación del desarrollo
5.5	Planificación de la Calidad
5.6	Diseño e Implementación
5.7	Testeo y Validación
5.8	Aceptación

5.9	Generación, Entrega e Instalación
5.10	Mantenimiento
6	Sistema de calidad - actividades de apoyo
6.1	Administración de la Configuración
6.2	Documentos de Control
6.3	Calidad de los Archivos
6.4	Medidas
6.5	Reglas y Convenciones
6.6	Herramientas y Técnicas
6.7	Compra
6.8	Productos de software incluidos
6.9	Formación

Descripción de cláusulas aplicables
Se hará una descripción breve de las cláusulas más relacionadas con el tema, siguiendo la numeración que se mostró en la tabla anterior.
Administración de la Responsabilidad
Responsabilidad gerencial del proveedor
Organización
Autoridad y responsabilidad
Debe definirse la responsabilidad, la autoridad y las relaciones entre todo el personal que dirige, realiza y verifica cualquier trabajo relacionado con la calidad, particularmente aquel personal que precisa independencia y autoridad para:

1. Iniciar, acciones para prevenir la ocurrencia de productos no conformes.
2. Identificar y registrar cualquier problema relacionado con la calidad del producto.
3. Iniciar, recomendar o aportar soluciones a través de los canales establecidos.
4. Comprobar que se ponen en práctica las soluciones adoptadas.

5. Controlar el procesamiento posterior, el envío y la entrega o la instalación del producto no conforme, hasta que la deficiencia o la condición insatisfactoria haya sido corregida.

Responsabilidad gerencial del comprador.
"El comprador deberá colaborar con el proveedor para proporcionar a tiempo toda la información necesaria y resolver las situaciones pendientes de arreglo".
El comprador designará un representante con la responsabilidad de tratar con el proveedor sobre asuntos contractuales. Este representante tendrá la autoridad necesaria que le permita tratar cualquier asunto contractual que incluya, pero no esté limitado, a los siguientes aspectos:

1. Definir los requerimientos del comprador hacia el proveedor;
2. Responder a preguntas del proveedor;
3. Aprobar las propuestas del proveedor;
4. Finalizar acuerdos con el proveedor;
5. Asegurar que la organización del comprador cumpla con los acuerdos hechos con el proveedor;
6. Definir los criterios y los procedimientos de aceptación;
7. Resolver acerca de los componentes de software que se considere son inadecuados para ser usados, siguiendo los criterios comprador – proveedor". [12]

Revisiones conjuntas

Se debe establecer revisiones conjuntas periódicas que involucran al proveedor y al comprador, de modo de cubrir los siguientes aspectos, si ello es apropiado:

1. La conformidad del software con los requisitos de la especificación del comprador acordada;
2. Los resultados de la verificación;
3. Los resultados de los ensayos de aceptación.

Los resultados de tales revisiones deben ser acordados y estar documentados.

Acciones Correctivas

El proveedor debe establecer, documentar y mantener procedimientos para:

1. Investigar las causas de los productos no conformes y la acción correctivo que debe aplicarse para evitar su repetición;
2. Analizar todos los procesos, operaciones, autorizaciones, registros de calidad, informes de servicio y quejas de clientes para detectar y eliminar las causas potenciales que generan productos no conformes;
3. Iniciar acciones preventivas para tratar los problemas a un nivel que corresponda a los riesgos encontrados;
4. Realizar controles para asegurar que se tomen las acciones correctivas y que éstas sean efectivas,
5. Aplicar y registrar las modificaciones a los procedimientos que resulten de las acciones correctivas.

Revisión de Contratos

"El proveedor establecerá y mantendrá procedimientos para la revisión de contratos y para la coordinación de estas actividades.

Cada contrato será revisado por el proveedor para asegurar que:

1. El objeto y los requisitos del contrato están definidos y documentados;
2. Se ha identificado posibles riesgos o contingencias;
3. La propiedad de la información está adecuadamente protegida;
4. Se ha resuelto cualesquiera requisitos que difieren de aquellos que están en la propuesta;
5. El proveedor tiene la capacidad para cumplir los requisitos contractuales;
6. Se ha definido la responsabilidad del proveedor con respecto al trabajo subcontratado;
7. La terminología está acordada por ambas partes;
8. El comprador tiene la capacidad para cumplir las obligaciones contractuales.

Se debe mantener registros de tales revisiones de contrato."

Detalles del contrato sobre calidad

Se encuentra, frecuentemente, que es pertinente que los siguientes detalles, entre otros, figuren en el contrato:

1. Criterios de aceptación;
2. Manejo de los cambios en los requisitos del proveedor durante el desarrollo;
3. Manejo de los problemas detectados después de la aceptación, incluyendo las reclamaciones y las quejas del comprador relacionadas con calidad;
4. Actividades llevadas a cabo por el comprador, especialmente la función del comprador en la especificación de los requisitos, en la instalación y en la aceptación;
5. Instalaciones, herramientas y componentes de software a ser suministrados por el comprador;
6. Normas y procedimientos a ser usados;
7. Requisitos de reproducción.

Especificación de los Requisitos del Comprador

Con la finalidad de llevar a cabo el desarrollo de software el proveedor dispondrá de un conjunto completo y no ambiguo de requisitos funcionales. Además, estos requisitos incluirán todos los aspectos necesarios para satisfacer las necesidades del comprador. Éstos pueden incluir, pero no están limitados, a los siguientes: comportamiento, seguridad, confiabilidad, protección y privacidad. Estos requisitos serán establecidos en forma suficientemente precisa, de modo de permitir la validación durante la aceptación del producto.

La especificación de los deseos y las necesidades del comprador es el documento que registra estos requisitos. En algunos casos, este documento es proporcionado por el comprador. En caso contrario, el proveedor deberá desarrollar estos requisitos en estrecha colaboración con el comprador, para lo cual el proveedor deberá obtener la aprobación del comprador antes de iniciar la etapa de desarrollo. Como parte de la documentación de desarrollo, la especificación de los

requisitos del comprador estará sometida a control de documentación y a gestión de configuración.

En la especificación de los requisitos del comprador, deberán establecerse totalmente todas las interfaces entre el producto de software y otros productos de software y de hardware, ya sea directamente o mediante referencia.

Colaboración mutua

Se recomienda que durante el desarrollo de la especificación de los requisitos del comprador, se preste atención a los siguientes puntos:

1. La designación de personas (de ambas partes) que tengan responsabilidad para establecer la especificación de los requisitos del comprador;
2. Los métodos para acordar los requisitos y aprobar los cambios;
3. Las acciones para prevenir malas interpretaciones, tales como definiciones de términos, explicación de fundamentos de los requisitos;
4. Los resultados de la discusión deben ser registrados y revisados por ambas partes.

Planificación del Desarrollo

El plan de desarrollo deberá cubrir lo siguiente:

1. La definición del proyecto, incluyendo una declaración de sus objetivos y la referencia a los proyectos conjuntos entre comprador y proveedor;
2. La organización de los recursos del proyecto, incluyendo la estructura del grupo humano, las responsabilidades, el uso de subcontratistas y los recursos materiales a ser usados;
3. Las fases de desarrollo;
4. El calendario del proyecto, identificando las tareas que se deben realizar, los recursos y el tiempo necesario para cada una de ellas y cualesquiera interrelaciones entre las tareas;

5. La identificación de los planes relacionados, tales como:

- Plan de calidad,
- Plan de gestión de configuración,
- Plan de integración,
- Plan de ensayo.

El plan de desarrollo debe irse adecuando a medida que el desarrollo progresa y cada fase debe ser definida antes de comenzar las actividades en esa fase. Dicho plan debe ser revisado y aprobado antes de su ejecución.

Plan de desarrollo

Fases

El plan de desarrollo definirá un proceso o una metodología para transformar la especificación de los requisitos del comprador en un producto de software. Esto puede involucrar la segmentación del trabajo en fases y la identificación de:

1. Las fases de desarrollo a llevar a cabo;
2. Los elementos de entrada requeridos a cada fase;
3. Los elementos de salida requeridos de cada fase;
4. Los procedimientos de verificación a llevar a cabo en cada fase;
5. El análisis de los problemas potenciales asociados con las fases de desarrollo y con el logro de los requisitos especificados.

Gestión

El plan de desarrollo definirá la forma en que se gestionará el proyecto, incluyendo la identificación de:

1. Calendario de desarrollo, de aplicación y de distribuciones asociadas;
2. Control del progreso del trabajo;
3. Responsabilidades organizativas, recursos y asignación de trabajo;

4. Interfaces organizativas y técnicas entre los diferentes grupos de trabajo.

Control de progreso

Las revisiones de progreso deben ser planificadas, mantenidas y documentadas para asegurar que los temas vinculados con recursos pendientes, son resueltos y para asegurar la ejecución efectiva de los planes de desarrollo.

Aceptación
Generalidades

Cuando el proveedor está en condiciones de despachar el producto validado, el comprador debe juzgar si el mismo es o no aceptable, según los criterios previamente acordados y de la manera especificada en el contrato.

El método de manejo de los problemas detectados durante el procedimiento de aceptación y su destino, deberán ser acordados entre el comprador y el proveedor, debiendo ser esto documentado.

Reproducción, Despacho e Instalación

Instalación

Las funciones, las responsabilidades y las obligaciones del proveedor y del comprador deberán ser establecidas claramente, tomando en cuenta lo siguiente:

1. El calendario, incluyendo horarios de trabajo extra y fines de semana;
2. El acceso a los locales del comprador (distintivos de seguridad, claves, escoltas);
3. La disponibilidad de personal calificado;
4. La disponibilidad y el acceso a los sistemas y al equipamiento del comprador;
5. La necesidad de realizar validación formal, como parte de cada instalación, deberá ser determinada en forma contractual;

6. Un procedimiento formal para la aprobación final de cada instalación.

(Ver Anexo 21)

ISO 17799

La ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de seguridad de la información; está dirigida a los responsables de iniciar, implantar o mantener la seguridad de una organización.

La seguridad de la información se define como la preservación de:

• Confidencialidad.- Asegura que la información sea accesible sólo para aquellos autorizados a tener acceso.
• Integridad.- Garantiza la exactitud y completitud de la información y de los métodos de su procesamiento.
• Disponibilidad.- Asegura que los usuarios autorizados tengan acceso cuando lo requieran a la información y sus activos asociados.

El objetivo principal de la ISO 17799 es proporcionar un conjunto de normas comunes de seguridad de información reconocidas globalmente, y ser una práctica eficaz de la gestión de la seguridad capaz de someterse a auditorías independientes.

Estructura

La norma ISO 17799:2002 establece diez dominios de control que cubren todos los aspectos fundamentales aplicables a la seguridad en el manejo de la información:

• Política de seguridad
• Aspectos organizativos para la seguridad
• Clasificación y control de activos
• Seguridad ligada al personal
• Seguridad física y del entorno
• Gestión de comunicaciones y operaciones

- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Administración de la continuidad del negocio
- Conformidad con la legislación

De estos diez dominios se derivan 36 objetivos de control (resultados que se esperan alcanzar mediante la implementación de controles) y 127 controles (prácticas, procedimientos o mecanismos que reducen el nivel de riesgo).

Dominios de control ISO 17799

(Ver Anexo 22)

Descripción de los objetivos de control que guardan mayor relación
Aspectos organizativos para la seguridad.

Dentro de los aspectos organizativos podemos encontrar aspectos referentes a la infraestructura de seguridad de la información, seguridad frente al acceso de terceros y la tercerización. Se profundizará en el segundo punto, cuyo objetivo es mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

Identificación de riesgos del acceso de terceras partes

Tipos de acceso

El tipo de acceso otorgado a terceras partes es de especial importancia. Por ejemplo, los riesgos de acceso a través de una conexión de red son diferentes de los riesgos relativos al acceso físico. Los tipos de acceso que deben tenerse en cuenta son:

a) Acceso físico, por ejemplo, a oficinas, salas de cómputos, armarios;
b) Acceso lógico, por ejemplo, a las bases de datos y sistemas de información de la organización.

Razones para el acceso

Puede otorgarse acceso a terceros por diversas razones. Por ejemplo, existen terceros que proveen servicios a una organización y no están ubicados dentro de la misma pero se les puede otorgar acceso físico y lógico, tales como:

a) Personal de soporte de hardware y software, quienes necesitan acceso a nivel de sistema o a funciones de las aplicaciones;
b) Socios comerciales o socios con riesgos compartidos, quienes pueden intercambiar información, acceder a sistemas de información o compartir bases de datos.

La información puede ponerse en riesgo si el acceso de terceros se produce en el marco de una inadecuada administración de la seguridad. Cuando existe una necesidad de negocios que involucran una conexión con un sitio externo, debe llevarse a cabo una evaluación de riesgos para identificar los requerimientos de controles específicos. Ésta debe tener en cuenta el tipo de acceso requerido, el valor de la información, los controles empleados por la tercera parte y la incidencia de este acceso en la seguridad de la información de la organización.

Contratistas in situ

Las terceras partes que sean ubicadas in situ por un período de tiempo determinado según contrato, también pueden originar debilidades en materia de seguridad. Entre los ejemplos de terceras partes in situ se enumeran los siguientes:

a) Personal de mantenimiento y soporte de hardware y software;
b) Limpieza, catering, guardia de seguridad y otros servicios de soporte tercerizados;
c) Pasantías de estudiantes y otras designaciones contingentes de corto plazo;
d) Consultores.

Es esencial determinar qué controles son necesarios para administrar el acceso de terceras partes a las instalaciones de procesamiento de

información. En general, todos los requerimientos de seguridad que resultan de los controles internos o del acceso de terceros, deben estar reflejados en los contratos celebrados con los mismos. Por ejemplo, si existe una necesidad específica de confidencialidad de la información, podrían implementarse acuerdos de no-divulgación.

No se debe otorgar a terceros acceso a la información ni a las instalaciones de procesamiento de la misma hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato que defina las condiciones para la conexión o el acceso.

Requerimientos de seguridad en contratos con terceros

Las disposiciones que contemplan el acceso de terceros a las instalaciones de procesamiento de información de la organización deben estar basadas en un contrato formal que contenga todos los requerimientos de seguridad, o haga referencia a los mismos, a fin de asegurar el cumplimiento de las políticas y estándares (normas) de seguridad de la organización. El contrato debe garantizar que no surjan malentendidos entre la organización y el proveedor. Las organizaciones deben estar satisfechas con las garantías de su proveedor. Se deben considerar las siguientes cláusulas para su inclusión en el contrato:

a) La política general de seguridad de la información;
b) La protección de activos, con inclusión de:

1) Procedimientos de protección de los activos de la organización, incluyendo información y software;
2) Procedimientos para determinar si se han comprometido los activos, por ej., debido a pérdida o modificación de datos;
3) Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato, o en un momento convenido durante la vigencia del mismo;
4) Integridad y disponibilidad;
5) Restricciones a la copia y divulgación de información;

c) Una descripción de cada servicio del que podrá disponerse;

d) El nivel de servicio al que se aspira y los niveles de servicio que se consideran inaceptables;
e) Disposición que contemple la transferencia de personal cuando corresponda;
f) Las respectivas obligaciones de las partes con relación al acuerdo;
g) Responsabilidades con respecto a asuntos legales, por ej., legislación referida a protección de datos, especialmente teniendo en cuenta diferentes sistemas legales nacionales si el contrato contempla la cooperación con organizaciones de otros países;
h) Derechos de propiedad intelectual y asignación de derecho de propiedad intelectual, y protección de trabajos realizados en colaboración;
i) Acuerdos de control de accesos que contemplen:

1) Los métodos de acceso permitidos, y el control y uso de identificadores únicos como IDs y contraseñas de usuarios;
2) Un proceso de autorización de acceso y privilegios de usuarios;
3) Un requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso;

j) La definición de criterios de desempeño comprobables, y el monitoreo y presentación de informes respecto de los mismos;
k) el derecho a monitorear, y revocar (impedir), la actividad del usuario;
l) el derecho a auditar responsabilidades contractuales o a contratar a un tercero para la realización de dichas auditorías;
m) el establecimiento de un proceso gradual para la resolución de problemas; también deben considerarse, si corresponde, disposiciones con relación a situaciones de contingencia;
n)responsabilidades relativas a la instalación y el mantenimiento de hardware y software;
o)una clara estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos;
p) un proceso claro y detallado de administración de cambios;
q) los controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos;

r) los métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad;
s) los controles que garanticen la protección contra software malicioso;
t) las disposiciones con respecto a elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad; la relación entre proveedores y subcontratistas.

Seguridad del personal

La norma considera dentro de la seguridad del personal, la respuesta a incidentes y anomalías, en este caso se ampliará el tema sobre la comunicación de anomalías del software.

Comunicación de anomalías del software

Se deben considerar las siguientes acciones:

a) Deben advertirse y registrarse los síntomas del problema y los mensajes que aparecen en pantalla.
b) La computadora debe ser aislada, si es posible, y debe detenerse el uso de la misma. Se debe alertar de inmediato a la persona pertinente (contacto). Si se ha de examinar el equipo, éste debe ser desconectado de las redes de la organización antes de ser activado nuevamente. Los disquetes no deben transferirse a otras computadoras.
c) El asunto debe ser comunicado inmediatamente al gerente de seguridad de la información.

Los usuarios no deben quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados a hacerlo. La recuperación debe ser realizada por personal adecuadamente capacitado y experimentado.

Seguridad física y ambiental

Se tratará únicamente sobre los controles de acceso físico.

Controles de acceso físico

Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Deben tenerse en cuenta los siguientes controles:

a) Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
b) El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ej. Tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.
c) Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.
d) Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

Gestión de comunicaciones y operaciones

Tiene como objetivo garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información. Para el caso de estudio, se explicará sobre la planificación y aprobación del sistema.

Aprobación del sistema

Se deben establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, y se deben llevar a cabo adecuadas pruebas de los sistemas antes de su aprobación.

Los gerentes deben garantizar que los requerimientos y criterios de aprobación de nuevos sistemas sean claramente definidos, acordados, documentados y probados. Se deben considerar los siguientes puntos:

a) Desempeño y requerimientos de capacidad de las computadoras;
b) Recuperación ante errores y procedimientos de reinicio, y planes de contingencia;
c) Preparación y prueba de procedimientos operativos de rutina según estándares definidos
d) Conjunto acordado de controles de seguridad implementados
e) Procedimientos manuales eficaces;
f) Disposiciones relativas a la continuidad de los negocios,
g) Evidencia que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento, como durante los últimos días del mes
h) Evidencia de que se ha tomado en cuenta el efecto que tiene el nuevo sistema en la seguridad global de la organización
i) Entrenamiento en la operación o uso de nuevos sistemas.

Para los principales nuevos desarrollos, las funciones y usuarios de operaciones deben ser consultados en todas las etapas del proceso de desarrollo para garantizar la eficiencia operativa del diseño propuesto del sistema. Deben llevarse a cabo pruebas apropiadas para constatar el cumplimiento cabal de todos los criterios de aprobación.

Desarrollo y mantenimiento de sistemas

Se indica consideraciones para el desarrollo de software por parte de terceros.

Desarrollo externo de software

Cuando se terceriza el desarrollo de software, se deben considerar los siguientes puntos:

a) Acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual;
b) Certificación de la calidad y precisión del trabajo llevado a cabo;
c) Acuerdos de custodia en caso de quiebra de la tercera parte;
d) Derechos de acceso a una auditoria de la calidad y precisión del trabajo realizado;

e) Requerimientos contractuales con respecto a la calidad del código; realización de pruebas previas a la instalación para detectar códigos troyanos.

ISO/IEC 27001.

Es un estándar diseñado para la gestión de la seguridad de la Información. Proporciona un marco de gestión de seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Aplica a:

Organizaciones que procesen o manejen información y que requieran protegerla:

- Impresa o escrita en papel
- Almacenada electrónicamente
- Enviada por correo o algún otro medio electrónico
- Mostrada en videos corporativos
- Verbal (expresada en conversaciones)

Aspectos Importantes a Considerar

El lograr y mantener una certificación es consecuencia de varios factores, entre los más importantes se encuentran una buena planeación, comunicación, preparación y esfuerzo. Sin embargo, a veces por desconocimiento de las organizaciones no toman en cuenta aspectos claves para una adecuada implementación como:

- Consultores Certificados: Un consultor certificado cuenta con la competencia y experiencia para brindar consultoría formal, específica

y puntual, lo que genera confianza y la mayoría de las veces reduce tiempos y costos.
• Capacitación: Prepara al capital humano involucrado en los procesos de Gestión de TI, ayuda a reducir la curva de aprendizaje, aumentando su productividad y mayor entendimiento sobre los beneficios de los procesos y actividades a implementar.
• Herramientas de Gestión: Apoyarse con una herramienta de gestión durante la implementación y mantenimiento del sistema de gestión reduce tiempos y ayuda a tener un mayor control de las tareas periódicas.

Fuente: http://www.nyce.org.mx/index.php/sistemas/iso-27001

ISO / IEC 27037: 2012

Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital.

Esta norma proporciona orientación sobre la identificación, recopilación / recepción / adquisición, manejo y protección / preservación de pruebas forenses digitales es decir, "los datos digitales que pueden ser de valor probatorio" para su uso en los tribunales.

El propósito fundamental de los estándares forenses digitales ISO / IEC 27037, 27041, 27042 y 27043 y 27050 es promover métodos de buenas prácticas y procesos para la captura y la investigación de la evidencia digital forense. Mientras que los investigadores individuales,

organizaciones y jurisdicciones pueden así retener ciertos métodos, procesos y controles, se espera que la normalización (eventualmente) llevar a la adopción de enfoques similares, si no idénticas a nivel internacional, por lo que es fácil comparar, combinar y contrastar los resultados de tales investigaciones incluso cuando es realizada por distintas personas u organizaciones y, potencialmente, a través de diferentes jurisdicciones.

Uno de los problemas más críticos en las investigaciones forenses es la adquisición y preservación de las pruebas de tal manera que se garantice su integridad. Al igual que con la evidencia física convencional, es crucial para la primera y subsiguientes respondedores (definidos como "Evidencia Digital equipos de respuesta" y "Especialistas evidencia digital") para mantener la cadena de custodia de todas las pruebas forenses digitales, asegurando que se recopila y protegida a través de procesos estructurados que sean aceptables para los tribunales. Más que simplemente proporcionar integridad, los procesos deben dar garantías de que nada malo puede haber ocurrido. Esto requiere que un nivel de referencia definido de controles de seguridad de la información se alcanza o se supera.

Evidencia forense digital puede venir de cualquier medios de almacenamiento electrónico o de comunicaciones, tales como teléfonos celulares, computadoras, consolas de videojuegos, de iPod, etc. Por su naturaleza, la evidencia forense digital es frágil - que puede ser fácilmente dañado o alterado debido a una manipulación incorrecta, ya sea por accidente oa propósito.

Antes de la publicación de la norma ISO / IEC 27037, había normas aceptadas a nivel mundial-no en la adquisición de la evidencia digital, el primer paso en el proceso. La policía ha desarrollado sus propias directrices y procedimientos nacionales para la adquisición y protección de pruebas electrónicas. Sin embargo, esto crea problemas cuando los crímenes transfronterizos se han comprometido ya puede necesitar pruebas forenses digitales adquiridos en un país que se presentará en los tribunales de otro. Pruebas viciadas que pueden haber sido

adquiridos o protegida sin el nivel necesario de seguridad puede ser legalmente inadmisible.

Ámbito de aplicación y objetivo

La norma proporciona orientación detallada sobre la identificación, recolección y / o adquisición, marcado, almacenamiento, transporte y preservación de pruebas electrónicas, particularmente para mantener su integridad. Se define y describe los procesos mediante los cuales se reconoce la evidencia y ha identificado, de documentación de la escena del crimen, recolección y preservación de las pruebas, y el embalaje y transporte de evidencia.

El ámbito de aplicación abarca "tradicional" los sistemas de TI y medios de comunicación en lugar de los sistemas del vehículo, la computación en nube, etc.. La guía está dirigida principalmente a los primeros en responder.

Cada país tiene su propio sistema legislativo único. Un crimen cometido en una jurisdicción no puede incluso ser considerado como un crimen en otro. El reto es armonizar los procesos a través de fronteras de forma que los cibercriminales pueden ser procesados en consecuencia. Por lo tanto, un medio para permitir y facilitar el intercambio y el uso de pruebas fiables (es decir, una norma internacional sobre la adquisición de evidencia digital) se requiere.

"Evidencia digital", es decir, la información de los dispositivos digitales que se presentará ante el tribunal, se interpreta de manera diferente en las distintas jurisdicciones. Para la aplicabilidad más amplia, el estándar será evitar el uso de terminología jurisdicción específica. No va a cubrir el análisis de la evidencia digital, ni su admisibilidad, el peso, la pertinencia, etc. También no exigen el uso de herramientas o métodos particulares.

Estructura y contenido

1 Ámbito de aplicación.

2 Referencias normativas.
3 Términos y definiciones.
4 términos abreviados.
5 Información general.
6 Los componentes clave de identificación, recolección, consolidación y preservación de evidencia digital.
7 casos de identificación, recolección, adquisición y preservación.

Anexo Evidencia A Digital First Responder habilidades básicas y descripción de competencias

Requisitos mínimos del Anexo B de la documentación para la transferencia de la evidencia

La norma se publicó en octubre de 2012.

La norma ISO, se reproduce en la norma británica BS 10008: 2008 " Especificación,fuerza probatoria y admisibilidad legal de la información electrónica.".

Cuando se publique, la norma ISO / IEC 27042 se cubrirán todas las actividades que se derivan de la recolección de evidencia digital.

ISO, está desarrollando varias normas forenses distintas, que cubren diferentes aspectos de la ciencia forense, cuando son en realidad partes complementarias de un mismo proceso. Un estándar de varias partes tendría más sentido, con un resumen explicando cómo si fuera las piezas de un rompecabezas que encajan en la investigación forense. (Ver Anexo 23)

En el caso de Ecuador, esta norma técnica no está replicada.

El INEC, establece que las normas Técnicas NTE INEN-ISO/ IEC 27000, son una traducción idéntica de la Norma Internacional ISO/IEC 27000:2011 TECNOLOGÍA DE LA INFORMACIÓN - TÉCNICAS DE SEGURIDAD - SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI), El Ministerio

de Telecomunicaciones, MINTEL, es el responsable de la traducción de esta Norma Técnica Ecuatoriana, y de su adopción es el Comité Técnico de Normalización del INEN.

Para el propósito de esta Norma Técnica Ecuatoriana se han hecho los siguientes cambios editoriales:

a) Las palabras "esta Norma Internacional" han sido reemplazadas por "esta norma nacional".

Para el propósito de esta Norma Técnica Ecuatoriana se enlistan los documentos normativos internacionales que se referencian en la Norma Internacional ISO/IEC 27000 y los documentos normativos nacionales correspondientes:

(Ver Anexo 24)

NEA No. 11

La NEA No. 11 -Sirve para aplicar auditorías financieras, en ambientes de información por computadora, se enfocan principios básicos y procedimientos esenciales para desempeñar el trabajo del auditor en un ambiente de sistemas de información; estos guardan similitud con los lineamientos que el forense digital debe seguir durante su ejercicio.

Esta NEA abarca contenidos sobre la habilidad y competencia del auditor forense, la planificación, la evaluación del riesgo y los procedimientos de auditoría; de los cuales citaremos las partes más importantes con el fin de dar una idea de lo que la norma ecuatoriana indica, y que está relacionado con el tema en análisis.

Habilidad y competencia

El auditor debería tener suficiente conocimiento del SIC (sistema de información computarizada) para planificar, dirigir, supervisar y revisar el trabajo desarrollado. El auditor debería considerar si se necesitan habilidades especializadas en SIC en una auditoría".

Planificación

De acuerdo con la NEA "Evaluaciones del Riesgo y Control Interno" el auditor debería obtener una suficiente comprensión de los sistemas de contabilidad y de control interno, para planificar la auditoría y desarrollar un enfoque de auditoría efectivo.

Al planificar las porciones de la auditoría que pueden verse afectadas por el ambiente SIC del cliente, el auditor debería obtener una comprensión de la importancia y complejidad de las actividades del SIC y la disponibilidad de datos para el uso en la auditoría. Esta comprensión incluiría asuntos como:

• La importancia y complejidad del procesamiento por computadora en cada operación importante de contabilidad.
• La estructura organizacional de las actividades SIC del cliente y el grado de concentración o distribución del procesamiento por computadora en toda la entidad, particularmente en cuanto puedan afectar la segregación de deberes.
• La disponibilidad de datos. Los documentos fuente, ciertos archivos de computadora, y otro material de evidencia que puede ser requerido por el auditor, pueden existir por un corto periodo de tiempo o solo en forma legible por computadora. El SIC del cliente puede generar reportes internos que pueden ser útiles para llevar a cabo ciertas pruebas sustantivas (particularmente procedimientos analíticos).

Evaluación del riesgo

De acuerdo con la NEA "Evaluación del riesgo y control interno", el auditor forense debería hacer una evaluación de los riesgos inherente y de control para las aseveraciones importantes de los estados financieros.

Los riesgos inherentes y de control en un ambiente de SIC pueden tener tanto efectos generales como específicos:

• Los riesgos pueden resultar de deficiencias en actividades generales de SIC como desarrollo y mantenimiento de programas, respaldo de

software de sistemas, operaciones, seguridad física de SIC y control sobre el acceso a programas de privilegio especial.
• Los riesgos pueden incrementar el potencial de errores y actividades fraudulentas en aplicaciones, bases de datos o archivos maestros. Los sistemas que controlan desembolsos de efectivo u activos líquidos son susceptibles a acciones fraudulentas por los usuarios o por el personal del SIC.

Procedimientos de auditoría

De acuerdo con la NEA "Evaluaciones del riesgo y control interno" el auditor forense debería considerar el ambiente al diseñar los procedimientos de auditoría para reducir el riesgo a un nivel aceptablemente bajo.

PRUEBA PENAL.

NOTA EXPLICATIVA: Todo el desarrollo de esta parte se basa en material manuscrito preparado para clase de formación profesional a Peritos Digitales Forenses y a Notarios Digitales Forenses, que lo imparto en curso organizado por del Instituto de Capacitación Jurídica –CETID, Notaria Digital, y por la Asociación ecuatoriana de peritos forenses, filial de la Federación de Peritos del Ecuador. He dictado cursos en Quito, Guayaquil, Tulcán, Cuenca, Loja, Portoviejo, Machala, Ibarra, Milagro, Chone, Santo Domingo,Puyo, Esmeraldas, Ambato. A nivel internacional en Lima, Bogotá, Madrid.

En el Nuevo COIP del Ecuador, la norma positiva describe la Prueba Digital Penal, en el TÍTULO IV. PRUEBA. CAPÍTULO PRIMERO.

La prueba penal tiene por finalidad llevar a la o al juzgador al convencimiento de los hechos y circunstancias materia de la infracción y la responsabilidad de la persona procesada. (Art.453 COIP)

Principios.-

El anuncio y práctica de la prueba se regirá por los siguientes principios:

1.- Oportunidad.-
Es anunciada en la etapa de evaluación y preparatoria de juicio y se practica únicamente en la audiencia de juicio.

Los elementos de convicción deben ser presentados en la etapa de evaluación y preparatoria de juicio. Las investigaciones y pericias practicadas durante la investigación alcanzarán el valor de prueba, una vez que sean presentadas, incorporadas y valoradas en la audiencia oral de juicio.

Sin embargo, en los casos excepcionales previstos en este Código, podrá ser prueba el testimonio producido de forma anticipada.

2.- Inmediación.-
Las o los juzgadores y las partes procesales deberán estar presentes en la práctica de la prueba.

3. Contradicción.- Las partes tienen derecho a conocer oportunamente y controvertir las pruebas, tanto las que son producidas en la audiencia de juicio como las testimoniales que se practiquen en forma anticipada.

4.-Libertad probatoria.-
Todos los hechos y circunstancias pertinentes al caso, se podrán probar por cualquier medio que no sea contrario a la Constitución,los instrumentos internacionales de derechos humanos,los instrumentos internacionales ratificados por el Estado y demás normas jurídicas.

5. Pertinencia.-
Las pruebas deberán referirse, directa o indirectamente a los hechos o circunstancias relativos ala comisión de la infracción y sus consecuencias, así como a la responsabilidad penal de la persona procesada.

6. Exclusión.-

Toda prueba o elemento de convicción obtenidos con violación a los derechos establecidos en la Constitución, en los instrumentos internacionales de derechos humanos o en la Ley, carecerán de eficacia probatoria, por lo que deberán excluirse de la actuación procesal.

Se inadmitirán aquellos medios de prueba que se refieran a las conversaciones que haya tenido la o el fiscal con la persona procesada o su defensa en desarrollo de manifestaciones preacordadas.

Los partes informativos, noticias del delito, versiones de los testigos, informes periciales y cualquier otra declaración previa, se podrán utilizar en el juicio con la única finalidad de recordar y destacar contradicciones,siempre bajo la prevención de que no sustituyan al testimonio. En ningún caso serán admitidos como prueba.

7. Principio de igualdad de oportunidades para la prueba.-
Se deberá garantizar la efectiva igualdad material y formal de los intervinientes en el desarrollo de la actuación procesal. (Art. 454).

Nexo causal.-

La prueba y los elementos de prueba deberán tener un nexo causal entre la infracción y la persona procesada, el fundamento tendrá que basarse en hechos reales introducidos o que puedan ser introducidos a través de un medio de prueba y nunca, en presunciones. Artículo 455.-

Cadena de custodia.-

Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su autenticidad,acreditando su identidad y estado original; las condiciones,las personas que intervienen en la recolección, envío,manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio.

La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación,el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación. (Artículo 456)

Criterios de valoración.-

La valoración dela prueba se hará teniendo en cuenta su legalidad,autenticidad, sometimiento a cadena de custodia y grado actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales.

La demostración de la autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, estará a cargo de la parte que los presente.(Artículo 457)

Preservación de la escena del hecho o indicios.-

La o el servidor público que intervenga o tome contacto con la escena del hecho e indicios será la responsable de su preservación, hasta contar con la presencia del personal especializado.

Igual obligación tienen los particulares que por razón de su trabajo o función entren en contacto con indicios relacionados con un hecho presuntamente delictivo. (Artículo 458)

ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN.

Capítulo II. Art. 459. COIP.

Artículo 459.- Actuaciones.- Las actuaciones de investigación se sujetarán a las siguientes reglas:

1. Para la obtención de muestras, exámenes médicos o corporales, se precisa el consentimiento expreso de la persona o la autorización de la o el juzgador, sin que la persona pueda ser físicamente constreñida. Excepcionalmente por las circunstancias del caso,cuando la persona no pueda dar su consentimiento, lo podrá otorgar un familiar hasta el segundo grado de consanguinidad.
2. Las diligencias de reconocimiento constarán en actas e informes periciales.
3. Las diligencias de investigación deberán ser registradas en medios tecnológicos y documentales más adecuados para preservar la realización de la misma y formarán parte del expediente fiscal.
4. El registro que conste en el expediente fiscal deberá ser suficiente para determinar todos los elementos de convicción que puedan fundamentar la formulación de cargos o la acusación.
5. En caso de no existir una institución pública acreditada, las autopsias, exámenes médicos, de laboratorio o pruebas biológicas, podrán ser realizados en una institución de salud privada acreditada y los costos serán asumidos por el Consejo de la Judicatura.

Los mismos tendrán valor pericial.

LUGAR DE LOS HECHOS EN TERRITORIO DIGITAL (ESCENA DEL CRIMEN)

Reconocimiento del lugar de los hechos.-

La o el fiscal con el apoyo del personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, o el personal competente en materia de tránsito, cuando sea relevante para la investigación,reconocerá el lugar de los hechos de conformidad con las siguientes disposiciones:
8. Se realizarán diligencias de reconocimiento del lugar de los hechos en territorio digital, servicios digitales,medios o equipos tecnológicos. (Artículo 460)

El primer y más importante paso es analizar la escena del crimen y encontrar los medios en los que se registró la prueba.

Por la naturaleza intangible de los datos digitales, puede ser en cualquier medio de comunicación, capaces de contenerlo, desde un disco duro a una tarjeta de memoria de una cámara digital, un teléfono celular en un CD, un reproductor portátil de MP3 a un archivo de registro en un servidor.

Para cada uno de los medios de comunicación identificados debe preparar una Orden de Volatilidad (Orden de volatilidad), o entender los datos que debe ser adquirido antes de los demás con el fin de evitar el borrado o sobrescribir otros datos. Esta orden se dará por la mayor volatilidad que las más persistentes.

Por ejemplo, el orden de la volatilidad para un ordenador personal podría ser la siguiente:

Registros del sistema	Memoria física y memoria virtual	tabla de enrutamiento
caché de Arp	Tabla de procesos en ejecución	Sistema de archivos temporales
unidad de disco duro	Configuración física y topología de la red	Almacenamiento y copia de seguridad de los medios de comunicación (CD, DVD, NAS, etc.).

Una vez que haya localizado el orden de la volatilidad, se procede a la obtención de pruebas a través de copia forense.

Una vez que la copia, se procede a la primera compilación de la cadena de custodia.

CADENA DE CUSTODIA.

El Artículo 456,del COIP, se define a la cadena de custodia, en los siguientes términos: "Se aplicará cadena de custodia a los elementos físicos o contenido digital materia de prueba, para garantizar su

autenticidad, acreditando su identidad y estado original; las condiciones, las personas que intervienen en la recolección, envío, manejo, análisis y conservación de estos elementos y se incluirán los cambios hechos en ellos por cada custodio".

En el segundo párrafo de este artículo, se norma el procedimiento:

"La cadena inicia en el lugar donde se obtiene, encuentra o recauda el elemento de prueba y finaliza por orden de la autoridad competente. Son responsables de su aplicación, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el personal competente en materia de tránsito y todos los servidores públicos y particulares que tengan relación con estos elementos, incluyendo el personal de servicios de salud que tengan contacto con elementos físicos que puedan ser de utilidad en la investigación".

La cadena de custodia es un documento que contiene la información relevante de lo que se hizo con la prueba original y las copias forenses realizadas, a partir de su adquisición hasta la presentación en el proceso legal.

El manual de cadena de Custodia de la Policía Nacional del Ecuador, expedido por Resolución 1 Registro Oficial 156 de 27-ago-2007, define a la Cadena de Custodia: "Es el conjunto de procedimientos tendientes a garantizar la correcta preservación de los indicios encontrados en el lugar de los hechos; durante todo el proceso investigativo, desde que se produce la colección hasta su valoración por parte de la autoridad competente".

El manual cumple con el objetivo principal de establecer:"un procedimiento adecuado y estandarizado en el manejo de la Cadena de Custodia, en cuanto a la identificación, organización y administración de los indicios y/o evidencias, por parte delos organismos de socorro, bomberos, paramédicos, profesionales de las casas de salud, Ministerio Público y personal policial, para asegurar una mejor calidad del servicio en la administración de justicia". (Ibídem)

El Manual compila objetivos específicos, relación de responsabilidad y elementos que constituyen la cadena de custodia, entre los objetivos específicos están: "1. Orientar al personal de la Policía Nacional del Ecuador, Ministerio Público y organismos de socorro en la ejecución secuencial y ordenada de las actividades que implican el manejo de una cadena de custodia.2. Normar el procedimiento de registro y administración de indicios y/o evidencias en centros de acopio y bodegas de evidencias de Criminalística, Policía Judicial y Antinarcóticos.3. Mejorar el desempeño y confiabilidad de los servicios policiales en cuanto tiene que ver con la administración y conservación de indicios y/o evidencias de diferente naturaleza". (Ibídem)

En relación a la responsabilidad el manual dispones que "es responsabilidad de toda persona, organismos de socorro, bomberos, paramédicos, profesionales de las casas de salud, Policía Nacional y funcionarios del Ministerio Público ejecutar todas aquellas acciones y procedimientos que permitan llevar una correcta cadena de custodia". Y sobre los elementos que constituyen la cadena de custodia, el manual compila tres en importancia: "1. El control, nos permitirá identificar e individualizar los indicios y/o evidencias, de esta forma asegurar un seguimiento y registro de los procesos de entrega y recepción de estos elementos.2. La seguridad, nos permitirá establecer las medidas físicas y administrativas necesarias para el resguardo de indicios y/o evidencias en lugares que reúnan las condiciones necesarias, con el propósito de evitar extravíos, hurtos, cambios, deterioros, entre otros. 3. Medidas de preservación, nos facultará a través de procedimientos idóneos, garantizar la inalterabilidad de muestras, esto es: Degradación, contaminación o destrucción, a causa de un inadecuado tratamiento de éstas, o por un incorrecto almacenamiento". (Ibídem).

La información mínima que debe contener este documento es:

INSTITUCIÓN	
Número del caso.	
Encargado de la investigación	

Investigador asignado al caso.	
Naturaleza y breve descripción del caso	
Investigador a cargo de la duplicación de datos	
Fecha y hora de la custodia.	
Lugar donde fue encontrado el apoyo	
Apoyo del fabricante	
Modelo de Apoyo	
Número de serie del soporte.	

Cada vez que los medios digitales que se investigan son asignados a un nuevo investigador, en la cadena de custodia se debe añadir la siguiente información:

Nombre de la persona que integra análisis.	
Fecha y hora de la toma de carga del soporte.	
Fecha y hora de la devolución del apoyo	

FASES DE LA CADENA DE CUSTODIA

Extracción adecuada de la prueba. El procedimiento e instrumentos por utilizar deben ser los idóneos, válidos y recomendados. Preservación. El medio en que es colocado debe asegurar que sus propiedades no se alteren, ya sea por circunstancias naturales o artificiales. Individualización: Debe garantizarse que el indicio este individualizado y registrado debidamente, de manera que no se produzca su combinación o confusión con otros del mismo u otro caso. Si es factible marcarla para su identificación, deberá hacerse constar la señal o marca que puso. Transporte apropiado: La calidad del transporte debe salvaguardar su integridad de manera que no sufra

daños o alteraciones, ya sea por el movimiento o cambios en el medio ambiente. Entrega controlada: Debe hacerse constar quién la encontró, quién la recolectó, dónde y que circunstancias. La posesión del indicio debe estar a cargo de personas autorizadas y con capacidad técnica para manipularla sin causar alteración o destrucción.

(Ver Anexo 25)

EVIDENCIA DIGITAL

La evidencia digital, es un tipo de evidencia física, menos tangible que otras formas de evidencia (DNA, huellas digitales, componentes de computadores)

Características:

- Puede ser duplicada de manera exacta y copiada tal como si fuese el original.
- Con herramientas adecuadas es relativamente fácil identificar si la evidencia ha sido alterada, comparada con la original.
- Aún si es borrada, es posible, en la mayoría de los casos, recuperar la información.
- Cuando los criminales o sospechosos tratan de destruir la evidencia,existen copias que permanecen en otros sitios del sistema.

El autor Casey, define a la evidencia digital como "cualquier dato que puede establecer que un crimen se ha ejecutado (commit) o puede proporcionar una enlace (link) entre un crimen y su víctima o un crimen y su autor".

"Evidencia Digital Es un tipo de evidencia física que está construida de campos magnéticos y pulsos electrónicos que pueden ser recolectados y analizados con herramientas y técnicas especiales". (Casey 2000, pág.4). Eoghan Casey, MA. JCM-04 All Rights Reserved.

"Cualquier información, que sujeta a una intervención humana u otra semejante, ha sido extraída de un medio informático" Fuente: Acuerdo HB:171 2003 Guidelines for the Managment of IT Evidence.

A diferencia de la documentación en papel, la evidencia computacional es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia computacional es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías, como por ejemplo checksums o hash MD5.

Cuando ha sucedido un incidente, generalmente, las personas involucradas en el crimen intentan manipular y alterar la evidencia digital, tratando de borrar cualquier rastro que pueda dar muestras del daño. Sin embargo, este problema es mitigado con algunas características que posee la evidencia digital.

• La evidencia de Digital puede ser duplicada de forma exacta y se puede sacar una copia para ser examinada como si fuera la original. Esto se hace comúnmente para no manejar los originales y evitar el riesgo de dañarlos.
• Actualmente, con las herramientas existentes, se muy fácil comparar la evidencia digital con su original, y determinar si la evidencia digital ha sido alterada.
• La evidencia de Digital es muy difícil de eliminar. Aún cuando un registro es borrado del disco duro del computador, y éste ha sido formateado, es posible recuperarlo.
• Cuando los individuos involucrados en un crimen tratan de destruir la evidencia, existen copias que permanecen en otros sitios.

Clasificación de la evidencia digital

El Autor colombiano Cano, clasifica la evidencia digital en 3 categorías:

Registros generados por computador: Estos registros son aquellos, que como dice su nombre, son generados como efecto de la programación de un computador. Los registros generados por computador son inalterables por una persona. Estos registros son llamados registros de eventos de seguridad (logs) y sirven como prueba tras demostrar el correcto y adecuado funcionamiento del sistema o computador que generó el registro.

Registros no generados sino simplemente almacenados por o en computadores: Estos registros son aquellos generados por una persona, y que son almacenados en el computador, por ejemplo, un documento realizado con un procesador de palabras. En estos registros es importante lograr demostrar la identidad del generador, y probar hechos o afirmaciones contenidas en la evidencia misma. Para lo anterior se debe demostrar sucesos que muestren que las afirmaciones humanas contenidas en la evidencia son reales.

Registros híbridos que incluyen tanto registros generados por computador como almacenados en los mismos: Los registros híbridos son aquellos que combinan afirmaciones humanas y logs. Para que estos registros sirvan como prueba deben cumplir los dos requisitos anteriores. (Fuente: Evidencia Digital Reflexiones Técnicas, Administrativas y Legales Jeimy J. Cano, M.Sc., Ph.D GECTI – Facultad de Derecho Universidad de los Andes Colombia).

Criterios de admisibilidad

En legislaciones modernas existen cuatro criterios que se deben tener en cuenta para analizar al momento de decidir sobre la admisibilidad de la evidencia: la autenticidad, la confiabilidad, la completitud o suficiencia, y el apego y respeto por las leyes y reglas del poder judicial.

Autenticidad: Una evidencia digital será autentica siempre y cuando se cumplan dos elementos:

• El primero, demostrar que dicha evidencia ha sido generada y registrada en el lugar de los hehos

• La segunda, la evidencia digital debe mostrar que los medios originales no han sido modificados, es decir, que la los registros corresponden efectivamente a la realidad y que son un fiel reflejo de la misma.

A diferencia de los medios no digitales, en los digitales se presenta gran volatilidad y alta capacidad de manipulación. Por esta razón es importante aclarar que es indispensable verificar la autenticidad de las pruebas presentadas en medios digitales contrario a los no digitales, en las que aplica que la autenticidad de las pruebas aportadas no será refutada, de acuerdo por lo dispuesto por el artículo 11 de la ley 446 de 1998:

"Autenticidad de documentos. En todos los procesos, los documentos privados presentados por las partes para ser incorporados a un expediente judicial con fines probatorios, se reputarán auténticos, sin necesidad de presentación personal ni autenticación. Todo ello sin perjuicio de lo dispuesto en relación con los documentos emanados de terceros".

Para asegurar el cumplimiento de la autenticidad se requiere que una arquitectura exhiba mecanismos que certifiquen la integridad de los archivos y el control de cambios de los mismos.
Confiabilidad: Se dice que los registros de eventos de seguridad son confiables si provienen de fuentes que son "creíbles y verificable". Para probar esto, se debe contar con una arquitectura de computación en correcto funcionamiento, la cual demuestre que los logs que genera tiene una forma confiable de ser identificados, recolectados, almacenados y verificados.

Una prueba digital es confiable si el "sistema que lo produjo no ha sido violado y estaba en correcto funcionamiento al momento de recibir, almacenar o generar la prueba" [EviDig05]. La arquitectura de computación del sistema logrará tener un funcionamiento correcto siempre que tenga algún mecanismo de sincronización del registro de las acciones de los usurarios del sistema y que a posea con un registro centralizado e íntegro de los mismos registros.

Suficiencia o completitud de las pruebas: Para que una prueba esté considerada dentro del criterio de la suficiencia debe estar completa. Para asegurar esto es necesario "contar con mecanismos que proporcionen integridad, sincronización y centralización" para lograr tener una vista completa de la situación. Para lograr lo anterior es necesario hacer una verdadera correlación de eventos, la cual puede ser manual o sistematizada.

Apogeo y respeto por las leyes y reglas del poder judicial: Este criterio se refiere a que la evidencia digital debe cumplir con los códigos de procedimientos y disposiciones legales del ordenamiento del país. Es decir, debe respetar y cumplir las normas legales vigentes en el sistema jurídico.

Manipulación de la evidencia digital

Es importante tener presente los siguientes requisitos que se deben cumplir en cuanto a la manipulación de la evidencia digital.

• Hacer uso de medios forenses estériles (para copias de información)
• Mantener y controlar la integridad del medio original. Esto significa, que a la hora de recolectar la evidencia digital, las acciones realizadas no deben cambiar nunca esta evidencia.
• Cuando sea necesario que una persona tenga acceso a evidencia digital forense, esa persona debe ser un profesional forense.
• Las copias de los datos obtenidas, deben estar correctamente marcadas, controladas y preservadas. Y al igual que los resultados de la investigación, deben estar disponibles para su revisión.
• Siempre que la evidencia digital este en poder de algún individuo, éste será responsable de todas la acciones tomadas con respecto a ella, mientras esté en su poder.
• Las agencias responsables de llevar el proceso de recolección y análisis de la evidencia digital, serán quienes deben garantizar el cumplimiento de los principios anteriores.

Gestión de la Evidencia digital

Existen gran cantidad de guías y buenas prácticas que nos muestran como llevar acabo la gestión de la evidencia digital

Las guías que se utilizan tienen como objetivo identificar evidencia digital con el fin de que pueda ser usada dentro de una investigación. Estas guías se basan en el método científico para concluir o deducir algo acerca de la información. Presentan una serie de etapas para recuperar la mayor cantidad de fuentes digitales con el fin de asistir en la reconstrucción posterior de eventos. Existen diferentes tipos de planteamientos, estos varían dependiendo del criterio de la institución y/o personas que definen la guía, como se define a continuación.

(Ver Anexo 26)

Según el FBI, la técnica digital o informática (computación) forense es la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados electrónicamente y guardados en un medio computacional. La informática forense hace entonces su aparición como una disciplina auxiliar de la justicia moderna, para enfrentar los desafíos y técnicas de los intrusos informáticos, así como garante de la verdad alrededor de la evidencia digital que se pudiese aportar en un proceso.

Desde 1984, el Laboratorio del FBI y otras agencias que persiguen el cumplimiento de la ley empezaron a desarrollar programas para examinar evidencia computacional.

Ciencia Forense

La ciencia forense nos proporciona los principios y técnicas que facilitan la investigación del delito criminal, en otras palabras: cualquier principio o técnica que puede ser aplicada para identificar, recuperar, reconstruir o analizar la evidencia durante una investigación criminal forma parte de la ciencia forense.

Los principios científicos que hay detrás del procesamiento de una evidencia son reconocidos y usados en procedimientos como:

- Recoger y examinar huellas dactilares y ADN.
- Recuperar documentos de un dispositivo dañado.
- Hacer una copia exacta de una evidencia digital.
- Generar una huella digital con un algoritmo hash MD5 o SHA1 de un texto para asegurar que este no se ha modificado.

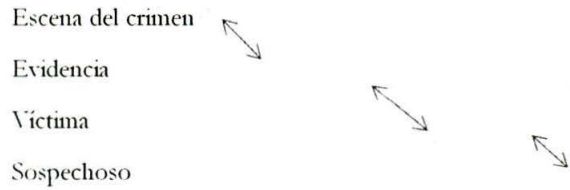
• Firmar digitalmente un documento para poder afirmar que es auténtico y preservar la cadena de evidencias.

Un forense digital aporta su entrenamiento para ayudar a los investigadores a reconstruir el crimen y encontrar pistas. Aplica un método científico analiza las evidencias disponibles, crea hipótesis sobre lo ocurrido para crear la evidencia y realiza pruebas, controles para confirmar o contradecir esas hipótesis. Esto puede llevar a una gran cantidad de posibilidades sobre lo que pudo ocurrir, esto es debido a que un forense no puede conocer el pasado, no puede saber qué ocurrió ya que sólo dispone de una información limitada. Por esto, sólo puede presentar posibilidades basadas en la información limitada que posee.

Un principio fundamental en la ciencia forense, que usaremos continuamente para relacionar a un individuo con el crimen que ha cometido, es el Principio de Intercambio o transferencia de Locard, (Edmond Locard, francés fundador del instituto de criminalística de la universidad de Lion).

(Ver Anexo 27)

Este principio fundamental viene a decir que cualquiera o cualquier objeto que entra en la escena del crimen deja un rastro en la escena o en la víctima y vice-versa (se lleva consigo), en otras palabras: "cada contacto deja un rastro". En el mundo real significa que si piso la escena del crimen con toda seguridad dejaré algo mío ahí, pelo, sudor, huellas, etc. Pero también me llevaré algo conmigo cuando abandone la escena del crimen, ya sea barro, olor, una fibra, etc. Con algunas de estas evidencias, los forenses podrán demostrar que hay una posibilidad muy alta de que el criminal estuviera en la escena del crimen.



En este ejemplo hemos hablado de evidencias físicas, en la ciencia forense tradicional hay varios tipos de evidencias físicas:

• Evidencia transitoria: como su nombre indica es temporal por naturaleza, por ejemplo un olor, la temperatura, o unas letras sobre la arena o nieve (un objeto blando o cambiante).
• Evidencia curso o patrón: producidas por contacto, por ejemplo la trayectoria de una bala, un patrón de rotura de un cristal, patrones de posicionamiento de muebles, etc.
• Evidencia condicional: causadas por una acción o un evento en la escena del crimen, por ejemplo la localización de una evidencia en relación con el cuerpo, una ventana abierta o cerrada, una radio encendida o apagada, dirección del humo, etc.
• Evidencia transferida: generalmente producidas por contacto entre personas, entre objetos o entre personas y objetos. Aquí descubrimos el concepto de relación.

En la práctica las evidencias transferidas se dividen en dos tipos, conocidas como:

• Transferencia por rastro: aquí entra la sangre, semen, pelo, etc.
• Transferencia por huella: huellas de zapato, dactilares, etc.
Aunque en la realidad, estas últimas suelen mezclarse, por ejemplo una huella de zapato sobre un charco de sangre.

El principio de intercambio de Locard se puede resumir así:

1. El sospechoso se llevará lejos algún rastro de la escena y de la víctima.
2. La víctima retendrá restos del sospechoso y puede dejar rastros de si mismo en el sospechoso.
3. El sospechoso dejará algún rastro en la escena.

El objetivo es establecer una relación entre los diferentes componentes:

• La escena del crimen
• La víctima
• La evidencia física
• El sospechoso

Para la correcta resolución del caso, todos estos componentes deben estar relacionados. Esto se conoce como el concepto de relación, que es lo que nos faltaba para completar el principio de intercambio de Locard.

Las evidencias pueden, a su vez, ser transferidas de dos formas distintas:

1. Transferencia directa: cuando es transferida desde su origen a otra persona u objeto de forma directa.
2. Transferencia indirecta: cuando es transferida directamente a una localización y, de nuevo, es transferida a otro lugar.

Importante resaltar que cualquier cosa y todo puede ser una evidencia.

Brevemente, la ciencia forense facilita las herramientas, técnicas y métodos sistemáticos (pero científicos) que pueden ser usados para analizar una evidencia digital y usar dicha evidencia para reconstruir qué ocurrió durante la realización del crimen con el último propósito de relacionar al autor, a la víctima y la escena del crimen.

Guías Mejores Prácticas.

A continuación se enuncian siete guías existentes a nivel mundial de mejores prácticas en computación forense

RFC 3227.

Directrices para la recolección de evidencia y archivo. Esta RFC se publicó en 2002.

Este documento especifica un Internet Mejores Prácticas Actuales de la Comunidad de Internet, y solicita debate y sugerencias para mejoras. La distribución de este memo es ilimitada.

Un "incidente de seguridad" como se define en el "Glosario de seguridad de Internet", RFC 2828, es un evento del sistema relevante para la seguridad en el que el sistema de la política de seguridad se desobedeció o incumplió lo contrario. El propósito de este documento

es proporcionar a los administradores de sistemas con directrices sobre la recopilación y el archivo de las pruebas pertinentes a una seguridad, incidente.

Si la recolección de evidencia se hace correctamente, es mucho más útil en aprehender el atacante, y se encuentra una probabilidad mucho mayor de ser admisible en el caso de un proceso judicial.

Principios Rectores durante la recolección de evidencia. (Fuente: http://www.rfc-base.org/txt/rfc-3227.txt&usg=ALkJrhiMESzDBaHa8-x6E2y5QEVHes73Ag

"- Adherirse a la política de seguridad de su sitio y comprometer el Manejo de Incidentes apropiado y personal aplicación de la ley.
- Capture como una imagen precisa del sistema como sea posible.
- Mantener notas detalladas. Estos deben incluir las fechas y horas. Si posible generar una transcripción automática. (Por ejemplo, en Unix sistemas del programa 'script' puede ser utilizado, sin embargo la salida el archivo que genera no debe ser a medios de comunicación que es parte de la pruebas). Notas e impresiones deben ser firmados y fechados.
- Tenga en cuenta la diferencia entre el reloj del sistema y UTC. Para cada indicación de la hora prevista, indicar si se utiliza UTC o local tiempo.
- Esté preparado para testificar (quizás años más tarde), que expondrá todo acciones que tomaron y en qué momento. Notas detalladas serán vital.
- Minimizar los cambios en los datos a medida que se está recogiendo. Es no se limita a cambios de contenido; usted debe evitar el archivo de actualización o los tiempos de acceso de directorio.
- Retire avenidas externas para el cambio.
- Cuando nos enfrentamos a una elección entre la recolección y el análisis que debe hacer en primer lugar la colección y el análisis posterior.
- A pesar de que casi no necesita afirmar, sus procedimientos deben ser implementable. Al igual que con cualquier aspecto de una respuesta a incidentes la política, los procedimientos debe ser probado para

asegurar la viabilidad,particularmente en una crisis. Si es posible, los procedimientos deben ser automatizado por razones de velocidad y precisión. Sea metódico.
- Para cada dispositivo, un enfoque metódico que debe adoptar se sigue las directrices establecidas en el procedimiento de recogida. Velocidad a menudo será crítico así que donde hay una serie de dispositivos que requieren examen puede ser apropiado para difundir el trabajo entre su equipo para recoger las pruebas en paralelo. Sin embargo en una sola colección sistema dado debe hacerse paso a paso.
- Proceder de la volátil al menos volátil (véase la Orden Volatilidad de abajo).
- Usted debe hacer una copia a nivel de bit de los medios de comunicación del sistema. Si usted desean hacer análisis forense, debe realizar una copia a nivel de bit de su evidencia copiar para tal fin, ya que su análisis casi seguro que alterar los tiempos de acceso de archivo. Evite hacer medicina forense en la copia pruebas."

El "RFC 3227: Guía Para Recolectar y Archivar Evidencia" (Guide lines for Evidence Collection and Archiving) [GuEvCo02], escrito en febrero de 2002 por Dominique Brezinski y Tom Killalea, ingenieros del Network Working Group. Es un documento que provee una guía de alto nivel para recolectar y archivar datos relacionados con intrusiones. Muestra las mejores prácticas para determinar la volatilidad de los datos, decidir que recolectar, desarrollar la recolección y determinar cómo almacenar y documentar los datos. También explica algunos conceptos relacionados a la parte legal. Su estructura es:

a) Principios durante la recolección de evidencia: orden de volatilidad de los datos, cosas para evitar, consideraciones de privacidad y legales.
b) El proceso de recolección: transparencia y pasos de recolección.
c) El proceso de archivo: la cadena de custodia y donde y como archivar.

Guía de la IOCE

La IOCE [IOCE06], publico "Guía para las mejores prácticas en el examen forense de tecnología digital" (Guidelines for the best practices in theforensicexamination of digital technology) [IOCE02].

El documento provee una serie de estándares, principios de calidad y aproximaciones para la detección prevención, recuperación, examinación y uso de la evidencia digital para fines forenses.

Cubre los sistemas, procedimientos, personal, equipo y requerimientos de comodidad que se necesitan para todo el proceso forense de evidencia digital, desde examinar la escena del crimen hasta la presentación en la corte.

Su estructura es:

a) Garantía de calidad (enunciados generales de roles, requisitos y pruebas de aptitud del personal, documentación, herramientas y validación de las mismas y espacio de trabajo).
b) Determinación de los requisitos de examen del caso.
c) Principios generales que se aplican a la recuperación de la evidencia digital (recomendaciones generales, documentación y responsabilidad).
d) Prácticas aplicables al examen de la evidencia de digital.
e) Localización y recuperación de la evidencia de digital en la escena: precauciones, búsqueda en la escena, recolección de la evidencia y empaquetado, etiquetando y documentación.
f) Priorización de la evidencia.
g) Examinar la evidencia: protocolos de análisis y expedientes de caso.
h) Evaluación e interpretación de la evidencia
i) Presentación de resultados (informe escrito).
j) Revisión del archivo del caso: Revisión técnica y revisión administrativa.
k) Presentación oral de la evidencia.
l) Procedimientos de seguridad y quejas.

Investigación en la Escena del Crimen Electrónico (Guía DoJ 1)

El Departamento de Justicia de los Estados Unidos de América (DoJ EEUU), publico "Investigación En La Escena Del Crimen Electrónico" (Electronic Crime Scene Investigation: A Guide for First Responders) [ElCr01]. Esta guía se enfoca más que todo en identificación y recolección de evidencia. Su estructura es:

a) Dispositivos electrónicos (tipos de dispositivos se pueden encontrar y cual puede ser la posible evidencia).
b) Herramientas para investigar y equipo.
c) Asegurar y evaluar la escena.
d) Documentar la escena.
e) Recolección de evidencia.
f) Empaque, transporte y almacenamiento de la evidencia.
g) Examen forense y clasificación de delitos.
h) Anexos (glosario, listas de recursos legales, listas de recursos técnicos y listas de recursos de entrenamiento).

Examen Forense de Evidencia Digital (Guía DoJ 2)

Otra guía del DoJ EEUU, es "Examen Forense de Evidencia Digital" (Forensic Examination of Digital Evidence: A Guide for Law Enforcement) [FoEx04].

Esta guía esta pensada para ser usada en el momento de examinar la evidencia digital. Su estructura es:

a) Desarrollar políticas y procedimientos con el fin de darle un buen trato a la evidencia.
b) Determinar el curso de la evidencia a partir del alcance del caso.
c) Adquirir la evidencia.
d) Examinar la evidencia.
e) Documentación y reportes.
f) Anexos (casos de estudio, glosario, formatos, listas de recursos técnicos y listas de recursos de entrenamiento).

Guía Hong Kong

El ISFS, Information Security and Forensic Society (Sociedad de Seguridad Informática y Forense) creada en Hong Kong, publico "Computación Forense - Parte 2: Mejores Practicas" (Computer Forensics - Part 2: Best Practices) [CoFor04]. Esta guía cubre los procedimientos y otros requerimientos necesarios involucrados en el proceso forense de evidencia digital, desde el examen de la escena del

crimen hasta la presentación de los reportes en la corte. Su estructura es:

a) Introducción a la computación forense.
b) Calidad en la computación forense.
c) Evidencia digital.
d) Recolección de Evidencia.
e) Consideraciones legales (orientado a la legislación de Hong Kong).
f) Anexos.

Guía De Buenas Prácticas Para Evidencia Basada En Computadores (Guía Reino Unido)

La ACPO, Association of Chief Police Officers (Asociación de Jefes de Policía), del Reino Unido mediante su departamento de crimen por computador, publico "Guía de Buenas Practicas para Evidencia basada en Computadores" (Good Practice Guide For Computer Based Evidence) [GoPra99]. La policía creó este documento con el fin de ser usado por sus miembros como una guía de buenas prácticas para ocuparse de computadores y de otros dispositivos electrónicos que puedan ser evidencia. Su estructura es:

a) Los principios de la evidencia basada en computadores.
b) Oficiales atendiendo a la escena.
c) Oficiales investigadores.
d) Personal para la recuperación de evidencia basada en computadores.
e) Testigos de consulta externos.
f) Anexos (legislación relevante, glosario y formatos)

Guía Para El Manejo De Evidencia En IT (Guía Australia)

Standards Australia (Estándares de Australia) publico "Guía Para El Manejo De Evidencia En IT" (HB171:2003 Hand book Guidelines for the management of IT evidence) [HBIT03]. Esta guía no esta disponible para su libre distribución, por esto para su investigación se consultó los artículos "Buenas Prácticas En La Administración De La Evidencia Digital"

[BueAdm06] y "New Guidelines to Combat ECrime" [NeGu03].

Es una guía creada con el fin de asistir a las organizaciones para combatir el crimen electrónico. Establece puntos de referencia para la preservación y recolección de la evidencia digital.

Detalla el ciclo de administración de evidencia de la siguiente forma:

a) Diseño de la evidencia.
b) Producción de la evidencia.
c) Recolección de la evidencia.
d) Análisis de la evidencia.
e) Reporte y presentación.
f) Determinación de la relevancia de la evidencia.

PROCEDIMIENTO DE INVESTIGACIÓN TÉCNICA DIGITAL FORENSE.

La adquisición de datos de un ordenador personal se puede realizar de diferentes modos, en relación con metodología operativa, sistema operativo, adquisición de software, procedimientos para la validación de la copia, metodología operativa.

La primera recomendación u opción que debe hacer un forense digital es retirar el dispositivo de almacenamiento del dispositivo que está conectado a una máquina y conectarla al dispositivo forense.

Luego hay que capturar la imagen del disco utilizando el equipo que analizó la fuente y guardar el resultado en un medio externo o extraíble en una máquina de análisis forense.

(Ver Anexo 28)

Sistema operativo para aplicar técnica digital forense.

Los principales sistemas operativos que ofrecen soluciones de aplicaciones nativas (o adicionales) para la copia forense de los datos son Linux y Windows.

Por su naturaleza, el sistema operativo Linux parece ser el más adecuado para la adquisición de datos en óptico forense, ya que es capaz de hacer que un disco duro accesible sólo en lectura, lo que garantiza un nivel de integridad del software y un no-escritura en los medios originales. Sin embargo, para reducir al mínimo el riesgo de deterioro, debe utilizar dispositivos de bloqueo de escritura, lo que impide a nivel de hardware de escritura en el soporte original.

Adquisición de software.

En Linux, la adquisición de datos se puede lograr mediante el uso de la dd nativa o una variante con un mayor rendimiento, o DCFLDD.

Estos comandos se pueden conseguir una copia bit a bit de un disco duro completo a un archivo de imagen, desde cualquier disco que el sistema operativo es capaz de interpretar.

En particular, las particiones son compatibles EXT2FS, Ext3, FAT12, FAT16, FAT32, NTFS, HFS y HPFS.

La ventaja de esta solución es que es totalmente gratuita, siempre y cuando tenga un buen conocimiento y comprensión de los comandos de la "Shell" a un sistema operativo Linux.

Para satisfacer las necesidades de velocidad y facilidad de uso se han desarrollado algunas distribuciones de Linux Live, que permite que el ordenador arranque desde un CD o memoria USB externa.

Estas distribuciones tienen la ventaja de que se pueden iniciar en la máquina que se está analizando (asegurándose de que, por supuesto, la secuencia de inicio de la PC) y permiten que el forense digital para localizar cualquier medio de almacenamiento en el ordenador personal y acceso en sólo lectura.

Una vez que haya identificado las fuentes de datos que desea duplicar, sólo tiene que conectar un dispositivo externo o una conexión de red en la que desea guardar la imagen en su disco duro.

Para escribir en un medio externo que tendrá que montar el dispositivo en lectura y escritura, con el comando nativo de montaje.

Las principales distribuciones de Linux en vivo que están disponibles actualmente en la web son:

Hélice 3 Enterprise	desarrollado por e-Fense, ex proyecto gratuito ahora ofrece una suscripción mensual.
DEFT (Digital Evidencia y ForensicToolkit) de Linux	desarrollado por Stephen Fratepietro.
CAINE (ComputerAided Medio Ambiente de Investigación)	desarrollado por NanniBassetti.
INTELIGENTE Linux	desarrollado por ASR datos
Forlex	desarrollado por Luca Guerrieri
Proyecto IRItaly (Proyecto de Respuesta a Incidentes Italia)	desarrollado por Darío Forte (este proyecto es final de la vida y no ser nuevas versiones disponibles.
El Kit de pingüino Sleuth	desarrollado por Ernest Baca.
Backtrack 4	desarrollado como una distribución de pruebas de penetración tiene algunas herramientas Informática Forense

Elaboración Cuadro: Dr. Juan José Páez Rivadeneira.

En el entorno Windows, hay sin embargo,, diversos programas de aplicación que permiten la copia forense de los datos. Como se mencionó anteriormente, para la adquisición en Windows no están disponibles actualmente Live CD con el que iniciar el equipo. Por tanto, es necesario desmontar el disco duro físico del equipo analizado y un acceso directo a una máquina dedicada forense. Dado que el disco

está conectado a un sistema operativo de Windows es necesaria para garantizar el acceso del bloque de escritura, utilice un bloqueador de escritura (hardware o software).

Las principales herramientas de adquisición disponibles en el entorno de Windows son:

AccessData FTK (Forensic Toolkit) Imager freeware	que le permite capturar imágenes de un dispositivos físicos completos o particiones lógicas (FAT, NTFS, ext2, ext3, HFS y HFS +) como soporte de ForensicToolkit
DIM-AM (Gerente de Investigación Digital - Módulo de Adquisición)	Software gratuito desarrollado por DFLabs como herramienta de apoyo a la DIM (Gerente de Investigación Digital.
Herramienta Encase	Producido por Guidance Software comercial.
Drive Snapshot	desarrollado por Tom Ehlert
SafeBack	herramienta comercial desarrollada por NTI
Monte Imagen Pro	desarrollado por Encase y SMART.l Obtener datos, lo que le permite montar en "sólo lectura" imágenes de formato dd.

Elaboración Cuadro: Dr. Juan José Páez Rivadeneira.

Dos herramientas de software para aplicación forense y muy especializadas son ENCASE, de Guidance Software, y FORENSIC TOOL KIT (FTK), de Access Data.

ENCASE es una herramienta informática forense que permite asistir al investigador durante todo el proceso de investigación digital, este

software permite el copiado comprimido de discos fuente empleando un estándar sin pérdida conocido como "loss-less", para crear copias comprimidas de los discos origen, los archivos comprimidos resultantes pueden ser analizados, buscados y verificados de manera semejante a los originales, esta característica ahorra cantidades importantes de espacio en disco del computador en el cual se realiza la investigación forense permitiendo de este modo trabajar al mismo tiempo con una gran diversidad de casos buscando la evidencia y realizando búsquedas en paralelo Access Data Forensic Tool Kit con su herramienta FTK ofrece un análisis forense completo proporcionando búsquedas y filtrados de ficheros que permiten encontrar de manera más ágil una evidencia, es una herramienta fácil de usar y contiene 270 formatos de ficheros diferentes los cuales pueden ser navegados a través de un explorador, genera logs e informes y es compatible con otras herramientas de software forense, permite efectuar búsquedas avanzadas para imágenes (jpg) y textos de Internet,recupera automáticamente ficheros y particiones borradas de un disco, y realiza el análisis de emails y ficheros (zip).

(Ver Anexo 29)

El hallazgo de una prueba específica depende, en gran parte, de la exactitud e integridad con la que el soporte original ha sido copiado: por esta razón se debe hacer una copia al nivel más bajo posible, o una copia del soporte-bit a bit almacenamiento original (copia forense).

A diferencia de una copia de seguridad de datos simple, que se encarga de salvar a un medio diferente una copia de los datos en el disco original, una copia bit a bit es un duplicado exacto de la totalidad de los medios originales. Un flujo de bits de imagen es, por lo tanto, un archivo que contiene una réplica de todos los datos en un disco o en una partición de un disco.

Los expertos recomiendan que antes de proceder con la copia de los datos forenses, debe asegurarse de:

- Que los medios de comunicación de destino en el que está copiando datos es forense estéril;
- Que los medios de comunicación fuente no se modificará durante la fase de adquisición de datos, o que, si se tratara de ser así, es posible dar la documentación completa en su informe

El primer requisito se consigue mediante el uso de las técnicas de eliminación segura de datos en el software.

El segundo punto se puede realizar de diferentes maneras, dependiendo del sistema de adquisición utilizado, tanto en hardware como en software.

El corazón de la información almacenada en un ordenador personal se encuentra dentro de la unidad de disco duro en ella.

(Ver Anexo 30)

Una unidad de disco duro es un dispositivo de almacenamiento permanente (debido a que conserva la información aun cuando no se alimenta), sellado y contiene una serie de platos (platos) en una pila.

Por encima o por debajo de las placas son de las cabezas electromagnéticas (cabezas) de la lectura y la escritura. Los platos se hacen girar las cabezas y se pueden mover desde el centro hacia el exterior, lo que le permite llegar a toda la superficie de todos los platos del disco.

Cada unidad de disco duro, los datos se almacenan en rayas finas y concéntricas, llamadas pistas (pistas). Cada pista se divide en sectores (sectores a), que es la unidad más pequeña de almacenamiento de un disco duro. Un sector es generalmente 512 bytes grande.

La mayoría de los discos duros están diseñados para su instalación dentro de un ordenador, por lo que también se les llama disco duro (disco fijo).

Con los años las normas han sido definidas con base en el tamaño físico y la interfaz que se utiliza para conectar el disco duro a la computadora.

Los principales tipos de discos duros usados en equipos son:

Discos 5.25	Los primeros discos duros instalados en un ordenador personal en los ochenta.
Discos 3.5 pulgadas	De tamaño estándar para los discos duros instalados dentro de la PC moderna
Unidades de 2,5 pulgadas	De tamaño estándar para los discos duros montados en el interior del portátil moderno

Elaboración: Dr. Juan José Páez Rivadeneira.

En relación a software expliquemos con el siguiente diagrama:

(Ver Anexo 31)

Durante la adquisición de datos desde el disco duro, es necesario para garantizar un acceso de escritura de bloque para mantener la integridad de la prueba.

En la mayoría de los casos, de hecho, mediante la conexión de la unidad de disco duro a un ordenador, se hacen los cambios a los datos contenidos en el mismo (a causa de las operaciones de montaje).

Estos cambios pueden incluir, por ejemplo, la fecha del último acceso o modificación de un archivo (por ejemplo. Un archivo de registro), e invalidar la prueba.

Hay dos métodos diferentes para garantizar el bloqueo de escritura:

1.-Software bloqueador de escritura. 2.-Hardware del controlador de disco Forense

Bloqueador de Software.

El bloqueo de escritura en el nivel de software se puede conseguir actuando sobre la operación de montar el disco duro por el sistema operativo.

En general, cuando un disco duro se conecta a un ordenador, el sistema operativo ofrece al usuario realizar operaciones de lectura y escritura.

Dependiendo del sistema operativo en la máquina adquisición forense, podrá tomar las medidas apropiadas para prevenir el flujo bidireccional de la comunicación y permitir el acceso en modo de sólo lectura.

En Microsoft Windows (desde Windows XP SP2 en adelante), es posible actuar a nivel del registro de protección contra escritura dispositivos USB. Una vez activado, este bloque se utiliza para conectar la unidad de disco duro para la adquisición de la máquina forense, utilizando la interfaz apropiada conversión (USB / IDE, USB / SCSI, USB / S-ATA, etc.).

Unas herramientas gratuitas útiles para el puerto USB de bloqueo de escritura en un entorno de Windows son: Bytescout USB Lockery, y Document Solutions Escribir USB Blocker

En Linux estos volúmenes se pueden montar directamente en modo de sólo lectura. Las distribuciones de captura forense adoptan esta técnica.

La elección de un software de escritura de bloqueo es, sin duda, económica, ya que requiere la compra de dispositivos especiales. Obviamente la forense digital debe probar constantemente la validez de este método con el nacimiento y desarrollo del nuevo estándar de conectividad.

Hardware del controlador de disco Forense.

Un bloqueador de escritura de hardware es en cambio un dispositivo físico que se interpone entre el disco duro y la máquina captura forense

(que es por eso que también se llama "puentes forenses". Estos dispositivos, además de ser flexible, fácil de transportar y fácil de usar, sino que también son más fáciles de entender para los interesados no técnicos (por ejemplo,el juez). También hay modelos que se pueden instalar de forma permanente en una bahía de la estación de trabajo de adquisición.

El bloqueador de escritura suele integrar diferentes tipos de interfaz (IDE, SATA, SCSI, USB, Firewire, etc.) y están conectados a la adquisición de la máquina a través de USB o Firewire. Ellos requieren una fuente de energía y se suministran con cables de conexión y conversión.

Los principales productores de bloqueadores de escritura de hardware son los siguientes:

Cuadro; WiebeTech; Soluciones Inteligentes en Informática; Voom Tecnologías; MyKey Tecnología; Inteligencia digital; Logicube; DIBS EE.UU; Fernico.

Con el nombre en buscador de internet encuentra directamente acceso a contenidos.

También hay, otras herramientas de bloqueo para otros tipos de recursos, tales como lectores de tarjetas forenses, que proporcionan acceso de sólo lectura en el procesamiento de tarjetas de memoria (SD, COSUDE, xD, MMC, CF, etc.).

Algunos fabricantes ofrecen, además, los kits de escritura de bloqueo para hacer el informe forense digitales capaces de operar con el mayor número posible en diferentes dispositivos e interfaces. Por lo general, incluyen cables, adaptadores, instrumentos de la foto / grabación de vídeo y bolsas aisladas para el transporte de la unidad de disco duro.
La recuperación de datos, o la creación de una copia forense del original del disco duro, también se puede hacer mediante el uso de la duplicación de hardware.

Estos dispositivos integran la funcionalidad a continuación, escribir el bloqueo de los medios de comunicación original, la duplicación de datos en otros medios de comunicación, y la evaluación de la exactitud e integridad del proceso a través de las herramientas de validación apropiadas (en la mayoría de los casos utilizando un algoritmo de hash como MD5, SHA1 o ambos). Muchos dispositivos también incorporan capacidades de informes automáticos.

La ventaja de estos dispositivos es que permiten lograr una mayor velocidad de transferencia durante la copia, con respecto a una solución de software.

Algunos de los productos que se encuentran en el mercado, son: Logicube Super Sonix (6 GB por minuto, soporte para IDE, SATA, USB y Firewire); Logicube Forense Talon (alcanzando velocidades de hasta 4 GB por minuto, ofrece varios adaptadores y es capaz de generar un informe detallado); Computer Solutions Intelligent Image MASSter Solo-III (se puede escribir la salida simultáneamente en dos discos duros); Tableau TD1 duplicador forense; Voom Tecnologías Hardcopy III.

Algunos fabricantes presentan bloqueador y duplicadores conjuntamente, estos entornos integrados permiten no sólo la duplicación de la prueba, sino también su análisis completo.

Las máquinas de este tipo de análisis deben ser fácilmente transportables.

Es por esto que las computadoras portátiles son generalmente protegidas en dispositivos resistentes o estación de trabajo compacta con teclado, ratón y monitor. En ambos casos, la máquina debe estar equipada con un procesador rápido y una gran cantidad de memoria RAM y espacio en disco.

Algunos de los productos disponibles en el mercado son:Forense Aire Lite V MKIII (Informática Forense); "PFL" Los forenses portátiles Lab (Logicube); DIBS Mobile Workstation Forense (DIBS EE.UU.);

FRED-L (Inteligencia Digital); Informática Forense Forense Aire Lite IV MK II; Inteligencia Digital FREDDIE

Se puede abaratar costos adquiriendo equipos para el análisis forense.

El diseño de una máquina de este tipo es simple: elegir el procesador más rápido, la mayoría de la cantidad de memoria RAM puede ser (8.4 Gb) y un espacio de almacenamiento de alta capacidad.

Teniendo en cuenta que hoy en día los discos duros que van desde 250 GB a 1 TB doméstica, lo que se necesita para preparar un equipo es 6.4 TB de espacio en disco.

Otro aspecto que no debe pasarse por alto es la elección del monitor.

Dado que el trabajo de análisis puede requerir el análisis de muchos datos al mismo tiempo, se recomienda una gran pantalla (LCD de 22 a 30 pulgadas) o una tarjeta de video de doble cabezal para conectarse a múltiples monitores.

Es también necesario diseñar medidas apropiadas de copia de seguridad y redundancia de datos para la gestión de copias forenses.

A nivel de software, es aconsejable que la máquina utilice diferentes entornos operativos (DOS, Linux, Windows, Solaris, etc.) y versiones (Windows 2000, Windows XP, Windows Vista, etc.).

El paso final de la adquisición es verificar la adecuación de los datos copiados con los datos originales.

Un chequeo-bit-a-bit requiere tiempo de procesamiento muy alto. Por esta razón utilizamos funciones hash.

Una función hash, es una función unidireccional que, dada una entrada de longitud arbitraria, proporciona una salida (hash) de longitud fija. El hash no se puede remontar de nuevo a los datos originales y una pequeña variación en los resultados de los datos originales no es un gran cambio en el resultado.

Estas propiedades hacen que las funciones hash la herramienta ideal para la verificación de una copia forense.

Una vez que obtenga la copia bit a bit, calculamos el hash del original y de la copia. Si coinciden, entonces también el original y copia son la misma.

Dado que existe una remota posibilidad de "colisión" de la almohadilla (es decir, dado dos entradas diferentes, que generan el mismo hash), usted debe verificar los datos mediante dos funciones hash diferentes. Las principales funciones de hash utilizados son:

MD5 (Message Digest Algorithm)

SHA-0, SHA-1, SHA-2 (Secure Hash Algorithm)

La mayoría de los programas de adquisición, tanto en los equipos Linux y Windows, integran en ellos el cálculo y la comparación de la función.

Una fuente abierta, programa multiplataforma utilizado para calcular el hash es md5deep.

Uno de los aspectos claves para un forense es asegurar la integridad de la prueba, a través de medidas adecuadas de conservación de los datos. Los principales problemas en un laboratorio forense están vinculados a:

Altas cantidades de datos.

La necesidad de la transferencia de datos.

La necesidad de conservar los datos intactos durante mucho tiempo. Necesidad de garantizar el acceso a datos confidenciales.

Para satisfacer estas necesidades, es necesario aplicar una política de gestión de datos de cuidado.

Una vez que los datos se han adquirido, el forense digital tiene que analizarlos científicamente, en busca de cualquier evidencia.

Dependiendo del caso se debe analizar: Los documentos (DOC, XLS, PDF, ...); imágenes; E-mail; navegación por Internet; Mensajería instantánea Chat; base de datos; archivos de registro; registros del sistema; flujo de datos activo; archivos borrados; archivos ocultos; espacio Slack; bloques Bad; archivos steganografati; archivos cifrados; particiones cifradas; particiones ocultas; Memoria Volátil (RAM)

El método de análisis varía considerablemente con la variación del sistema de archivos y el sistema operativo.

CUARTA PARTE
DELITO DIGITAL (INFORMÁTICO) COIP.

SISTEMA ADVERSARIAL

En los considerandos del Código integral penal COIP, en vigencia desde el 10 de agosto del 2014, en el parágrafo XII, se establecen los fundamentos del sistema adversarial, basado en el ejercicio de la acción penal, en lo procesal dentro de los principios y fundamentos del sistema acusatorio.

"Que el derecho penal adjetivo debe garantizar la existencia de un **sistema adversarial**, que cuente con **fiscales** que promuevan el ejercicio de la acción penal dentro de los principios y fundamentos del sistema acusatorio, con **defensoras y defensores públicos** que patrocinen técnicamente a las personas acusadas de cometer una infracción y a las personas que, por su estado de indefensión o condición económica, social o cultural, no puedan contratar los servicios de defensa legal para la protección de sus derechos, y con **juezas y jueces** que dirijan el proceso y sean garantes de los derechos de los participantes procesales;"

En el caso del Ecuador el sistema es ADVERSARIAL – ACUSATORIO, podemos resumir manifestando que en la parte sustantiva del concepto (Teoría Del Delito) es adversarial, y en la parte adjetiva (proceso penal), es acusatorio, es decir dos sistemas en uno.

(Ver Anexo 32)

El Art. 2 del COIP expone los Principios generales del sistema adversarial: "En materia penal se aplican todos los principios que emanan de la Constitución de la República, de los instrumentos internacionales de derechos humanos y los desarrollados en este Código". *Jurisprudencia: Gaceta Judicial, CUERPO DEL DELITO, 17-sep-1903; Gaceta Judicial, CAPELLANIAS, 23-sep-1904;Gaceta Judicial, FUERO PENAL, 04-jul-1949.

El Art. 3, norma el Principio de mínima intervención: "La intervención penal está legitimada siempre y cuando sea estrictamente necesaria para la protección de las personas. Constituye el último recurso, cuando no son suficientes los mecanismos extra penales. *Jurisprudencia: Gaceta Judicial, JUICIO DE COMPETENCIA, 21-jun-1973; Gaceta Judicial, COMPETENCIA EN MATERIA PENAL, 21-mar-1984; Gaceta Judicial, CRITERIO DE EQUIDAD, 29-ago-1996.

Y, los principios del modelo acusatorio, se encuentran en el CAPITULO SEGUNDO. GARANTÍAS Y PRINCIPIOS RECTORES DEL PROCESO PENAL.

Art. 4.- Dignidad humana y titularidad de derechos.- Las y los intervinientes en el proceso penal son titulares de los derechos humanos reconocidos por la Constitución de la República y los instrumentos internacionales. Las personas privadas de libertad conservan la titularidad de sus derechos humanos con las limitaciones propias de la privación de libertad y serán tratadas con respeto a su dignidad como seres humanos. Se prohíbe el hacinamiento.

Art. 5.- **Principios procesales**.- El derecho al debido proceso penal, sin perjuicio de otros establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, se regirá por los siguientes principios:

1. Legalidad: no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho. Este principio rige incluso cuando la ley penal se remita a otras normas o disposiciones legales para integrarla.
2. Favorabilidad: en caso de conflicto entre dos normas de la misma materia, que contemplen sanciones diferentes para un mismo hecho, se aplicará la menos rigurosa aun cuando su promulgación sea posterior a la infracción.
3. Duda a favor del reo: la o el juzgador, para dictar sentencia condenatoria, debe tener el convencimiento de la culpabilidad penal de la persona procesada, más allá de toda duda razonable.
4. Inocencia: toda persona mantiene su estatus jurídico de inocencia y debe ser tratada como tal,mientras no se ejecutoríe una sentencia que determine lo contrario.

5. Igualdad: es obligación de las y los servidores judiciales hacer efectiva la igualdad de los intervinientes en el desarrollo de la actuación procesal y proteger especialmente a aquellas personas que, por su condición económica, física o mental, se encuentren en circunstancias de vulnerabilidad.
6. Impugnación procesal: toda persona tiene derecho a recurrir del fallo, resolución o auto definitivo en todo proceso que se decida sobre sus derechos, de conformidad con lo establecido en la Constitución de la República, los instrumentos internacionales de derechos humanos y este Código.
7. Prohibición de empeorar la situación del procesado: al resolver la impugnación de una sanción, no se podrá empeorar la situación de la persona procesada cuando esta es la única recurrente.
8. Prohibición de autoincriminación: ninguna persona podrá ser obligada a declarar contra sí misma en asuntos que puedan ocasionar su responsabilidad penal.
9. Prohibición de doble juzgamiento: ninguna persona podrá ser juzgada ni penada más de una vez por los mismos hechos. Los casos resueltos por la jurisdicción indígena son considerados para este efecto. La aplicación de sanciones administrativas o civiles derivadas de los mismos hechos quesean objeto de juzgamiento y sanción penal no constituye vulneración a este principio.
10. Intimidad: toda persona tiene derecho a su intimidad personal y familiar. No podrán hacerse registros, allanamientos, incautaciones en su domicilio, residencia o lugar de trabajo, sino en virtud de orden de la o el juzgador competente, con arreglo a las formalidades y motivos previamente definidos, salvo los casos de excepción previstos en este Código.
11. Oralidad: el proceso se desarrollará mediante el sistema oral y las decisiones se tomarán en audiencia; se utilizarán los medios técnicos disponibles para dejar constancia y registrar las actuaciones procesales; y, los sujetos procesales recurrirán a medios escritos en los casos previstos en este Código.
12. Concentración: la o el juzgador concentrará y realizará la mayor cantidad de actos procesales en una sola audiencia; cada tema en discusión se resolverá de manera exclusiva con la información producida en la audiencia destinada para el efecto.

13. Contradicción: los sujetos procesales deben presentar, en forma verbal las razones o argumentos de los que se crean asistidos; replicar los argumentos de las otras partes procesales; presentar pruebas; y, contradecir las que se presenten en su contra.
14. Dirección judicial del proceso: la o el juzgador, de conformidad con la ley, ejercerá la dirección del proceso, controlará las actividades de las partes procesales y evitará dilaciones innecesarias. En función de este principio, la o el juzgador podrá interrumpir a las partes para solicitar aclaraciones, encauzar el debate y realizar las demás acciones correctivas.
15. Impulso procesal: corresponde a las partes procesales el impulso del proceso, conforme con el sistema dispositivo.
16. Publicidad: todo proceso penal es público salvo los casos de excepción previstos en este Código.
17. Inmediación: la o el juzgador celebrará las audiencias en conjunto con los sujetos procesales y deberá estar presente con las partes para la evacuación de los medios de prueba y demás actos procesales que estructuran de manera fundamental el proceso penal.
18. Motivación: la o el juzgador fundamentará sus decisiones, en particular, se pronunciará sobre los argumentos y razones relevantes expuestos por los sujetos procesales durante el proceso.
19. Imparcialidad: la o el juzgador, en todos los procesos a su cargo, se orientará por el imperativo de administrar justicia de conformidad con la Constitución de la República, los instrumentos internacionales de derechos humanos y este Código, respetando la igualdad ante la Ley.
20. Privacidad y confidencialidad: las víctimas de delitos contra la integridad sexual, así como toda niña, niño o adolescente que participe en un proceso penal, tienen derecho a que se respete su intimidad y la de su familia.
Se prohíbe divulgar fotografías o cualquier otro dato que posibilite su identificación en actuaciones judiciales, policiales o administrativas y referirse a documentación, nombres, sobrenombres, filiación,parentesco, residencia o antecedentes penales.
21. Objetividad: en el ejercicio de su función, la o el fiscal adecuará sus actos a un criterio objetivo, a la correcta aplicación de la ley y al respeto a los derechos de las personas. Investigará no solo los hechos y circunstancias que funden o agraven la responsabilidad de la persona procesada,

sino también los que la eximan, atenúen o extingan.*Jurisprudencia: Gaceta Judicial, TIPIFICACIÓN DE INFRACCIONES, 30-may-1891; Gaceta Judicial, TIPIFICACIÓN DE DELITOS, 07-jul-1911; Gaceta Judicial, TIPIFICACIÓN DE INFRACCIONES PENALES, 25-feb-1924; Gaceta Judicial, JUSTICIA POR PROPIA MANO, 19-oct-1950; Gaceta Judicial, PRINCIPIO REFORMATIO IN PEJUS, 17-dic-1980; Gaceta Judicial, DOCTRINA REFORMATIO IN PEJUS, 15-sep-1981;Gaceta Judicial, REFORMATIO IN PEJUS, 26-ene-1982; Gaceta Judicial, REFORMATIO IN PEJUS, 09-mar-1982;Gaceta Judicial, PRINCIPIO REFORMATIO IN PEJUS, 07-oct-1982; Gaceta Judicial, PRINCIPIO REFORMATIO IN PEJUS, 02-jun-1988; Gaceta Judicial, LEY APLICABLE A LA SANCIÓN DEL DELITO, 17-jun-1993; Gaceta Judicial, LA TIPIFICACIÓN DE UN HECHO LO HACE EL LEGISLADOR, NO EL JUEZ, 22-ago-1994.

El modelo adversarial fue extraído del procedimiento penal anglosajón. Es un procedimiento de partes (adversary system), en el que estas deciden sobre la forma de llevar a cabo la prueba, quedando la decisión de culpabilidad en manos del Tribunal Penal, en los países anglosajones es el Jurado (veredict), mientras que el Juez profesional (bench) se limita, en su caso, a la fijación de la pena (sentence). La confesión de culpabilidad (guiltyplea) permite pasar directamente a la individualización de la pena. Desde hace cien años, aproximadamente, los fiscales y las defensores se presten a negociar tal reconocimiento (pleabargaining). *Fuente: DERECHO PROCESAL PENAL. 2 PRIMERA SESIÓN NOCIONES GENERALES PRINCIPIOS PROCESALES. Publicada por Jaime Palencia.

En este sistema procesal, el juez, como sujeto procesal, está completamente separado de las partes, el proceso penal es una contienda entre iguales que inicia con la acusación, a quien compete la carga de la prueba, y confronta a la defensa, en un proceso o juicio contradictorio, oral y público, y el juez resuelve según su libre convicción.

El sistema acusatorio funciona haciendo una separación entre las funciones de investigación, acusación y sentencia, en este orden, quien

investiga es la policía, quien acusa es el fiscal, y quien sentencia es el juez tomando en cuenta la deliberación de un jurado especializado.

Se dan casos en algunos países, como Estados Unidos, donde el fiscal puede llegar a dirigir una investigación policial, pero la función de investigación la dirige, la maneja, en la mayoría de los sistemas, una policía independiente.

Esta independencia de la policía investigadora es una manera de garantizar que no serán influenciadas por algún poder público o político que recaiga en determinado funcionario del Estado.

El sistema acusatorio se rige por distintos principios que buscan garantizar la seguridad y los derechos del individuo imputado y de los ciudadanos en general, algunos de estos principios son los siguientes:

Oralidad: quiere decir que toda audiencia que se desarrolle durante el juicio se llevara a cabo de manera oral, a viva voz.

Publicidad: es la necesidad de dar a conocer a la sociedad, con toda transparencia, todo sobre el proceso, así como el resultado del juicio penal, esto constituye una garantía para todos los involucrados de que las decisiones que se hayan tomado, fueron en estricto derecho. Este es un modo de que la sociedad tenga un control sobre la actuación ministerial y judicial durante el proceso.

Contrariedad: este principio tiene como base la igualdad de las partes en orden a sus atribuciones procesales. "Garantiza que la producción de las pruebas se hará bajo el control de todos los sujetos procesales, con la finalidad de que ellos tengan la facultad de intervenir en dicha producción, formulando preguntas, objeciones, observaciones, aclaraciones y evaluaciones tanto sobre la prueba como sobre los otros. Este control se extiende a las argumentaciones de las partes, garantizándose que estas puedan en todo momento escuchar de viva voz los argumentos de la contraria apoyándolos o rebatiéndolos."

Inmediación: consiste en exigir al juez que pronuncia la sentencia, el asistir a la práctica de las pruebas de donde extrae su convencimiento,

que lo hicieren volverse de determinada postura, es decir que haya estado en relación directa con las partes, con los testigos, los peritos y los objetos de juicio, fundándose de este modo en la impresión inmediata que le hayan dado estas personas y no en referencias ajenas.

Concentración: gracias a este principio todas las pruebas deberán ser presentadas durante la misma audiencia de juicio, ofreciendo los medios al juez para que emita su resolución conforme a lo que fue materia durante la audiencia. Su evidente ventaja es la gran rapidez con la que se actúa, el proceso puede resolverse en poco tiempo.

Estos principios son los que rigenel proceso penal buscando eficacia, rapidez, mejores resultados y satisfacción ciudadana, pero sobre todo garantizar los derechos de las partes y el debido proceso.

El autor Richard Vogler* (El profesor Richard Vogler ha enseñado justicia penal comparado, derecho penal y criminología de la Universidad de Sussex desde 1988. En la actualidad es Director de Cursos de Postgrado en Derecho de la Facultad de Derecho, Política y Sociología) manifiesta que la adversarialidad como forma de juicio, no tiene nada que ver con la antigua tradición acusatoria y fue, en cambio, un procedimiento radicalmente nuevo desarrollado en Inglaterra en el siglo XVII.

La adversarialidad introdujo en la temprana Inglaterra industrial un juicio basado en un conjunto de derechos legales del debido proceso con los que el imputado estaba investido, como la presunción de inocencia, el derecho a guardar silencio, el derecho a examinar a los testigos, etc. Profundamente inspirado en el pensamiento de la Ilustración y en las obras de John Locke, esta nueva forma de juicio fue inventada por abogados litigantes en Inglaterra entre 1730 y 1770.

Es anterior a la obra de los "philosophes" franceses y conformó las bases prácticas sobre las que se erigieron las grandes declaraciones de derechos humanos, por ejemplo, la Carta de Derechos estadounidense y la Declaración de los Derechos del Hombre francesa. Por primera vez se trataba de una forma de juicio penal articulada en el lenguaje de

los derechos, en la cual el ciudadano acusado era puesto en un nivel de equidad con el poder soberano del estado (y no, como en el sistema "acusatorio", a nivel de la víctima acusadora.

Es decir que la adversarialidad debe ser considerada como un producto de la Ilustración Europea, con elementos poco comunes con el procedimiento acusatorio, y esencialmente es una aproximación del libre mercado al sistema penal, basado en la negociación individual, la libertad de contratar y el concepto de un individuo portador de derechos.

Adicionalmente encontramos varias características en la adversarialidad, así tenemos:

1. Es el producto de la tensión entre el ideal de equidad de la Ilustración y un sistema político fragmentado que no es lo suficientemente fuerte para producir un cambio social de tanta radicalidad.
2. Está marcado por la retórica antiautoritaria del protestantismo angloamericano.
3. Trajo consigo, por primera vez en la historia de la humanidad, un lenguaje de derechos humanos y de protección.
4. La metodología que emplea es el empírico tanto a nivel del derecho como de la ideología.
5. En sus propósitos prácticos presupone un espacio público en el cual el estado debe justificarse a sí mismo y ante los ciudadanos y es además el eje central de la organización del sistema penal.
6. La técnica que emplea es la declaración voluntaria de culpabilidad (guiltyplea) y la negociación de la pena (pleabargain) que representa la cualidad transaccional de su dinámica esencial. El descubrimiento de la verdad procesal depende del método relativista y comparativista.

*Fuente: Dr. M.Sc. Giovani Criollo Mayorga.

EXORDIO DE LOS DELITOS INFORMÁTICOS.

La tecnología y su desarrollo inciden en todas las actividades del ser humano, la dependencia tecnológica se concentra en el fenómeno de la

tecnología informática, la información y la comunicación. Asi mismo viene acompañado de riesgos en su uso cotidiano.

En 1980, la ArpaNet (Advanced Research Projects Agency Network) del Departamento de Defensa de Estados Unidos, creadora de la internet, documentó que en su red se emitieron extraños mensajes que aparecían y desaparecían en forma aleatoria, y que algunos códigos ejecutables de los programas usados sufrían una mutación; en ese momento, los hechos inesperados no pudieron comprenderse pero se les buscó solución. Los técnicos altamente calificados en seguridad informática del Pentágono desarrollaron un antivirus para contrarrestar el riesgo y atender la urgencia del caso, a los tres días de ocurrido el evento. * Fuente: (Trend Micro, 2008).

A medida que utilizamos el internet también aumenta el riesgo de su uso inadecuado. Aparecen los "delincuentes cibernéticos", denominados hackers, crackers, espias, etc, realizan incursiones fraudulentas cada vez más frecuentes y variadas, como por ejemplo: el acceso sin autorización a sistemas de información, piratería informática, fraude financiero, sabotaje informático, pornografía infantil, entre otros.

Sin embargo hay dificultad para descubrirlos, varios países han dispuesto un sistema judicial especializado que permite procesarlos y castigarlos, involucra reforma judicial, instituciones especializadas, aplicación de tecnología de punta, inversión permanente en capacitación e investigación.

En un comienzo, los ciberdelincuentes infectaban los equipos de sus víctimas al transportar mano a mano los virus desarrollados, en los medios de almacenamiento de información disponibles en ese momento: los disquetes.

Más tarde, utilizaron las redes de datos al aprovechar la internet, pero encontraron la barrera de las restricciones de acceso para evitar contagios. De nuevo, regresaron a la difusión contaminante mano a mano al emplear las memorias móviles con puerto USB y arreciaron los bombardeos de malware1 en la internet. De igual manera, los

ciberdelincuentes han utilizado el correo electrónico y los chat rooms o salas de conversación virtual de internet para buscar presas vulnerables.

Pero además de los delincuentes informáticos propiamente tales, otros tipos de delincuentes han encontrado espacios propicios en los distintos medios de comunicación electrónica, para desarrollar sus crímenes, como los pedófilos que buscan generar relaciones de confianza on line con niños inocentes*(Sweetie), para luego aprovecharse de ellos y hasta secuestrarlos o asesinarlos. Estafadores, falsificadores, defraudadores, secuestradores, proxenetas, traficantes de armas, de drogas, de personas, de pornografía, de información, sicarios y terroristas se agregan a esta tenebrosa lista que utiliza el ciberespacio y la red para multiplicar sus negocios, sus ilícitas ganancias y sus manifestaciones criminales.

• Por Redacción LAVOZ en: http://www.lavoz.com.ar/ciudadanos/sweetie-la-nina-virtual-que-consiguio-atrapar-y-condenar-un-pedofilo

Sweetie, una niña virtual filipina de 9 años, ha logrado atrapar y condenar al primer pedófilo. Se trata de un hombre australiano que se contactó con la intención de abusar de ella. El pedófilo nunca supo que era un personaje ficticio. Sweetie es un personaje generado por computadora, operado por los trabajadores de la organización holandesa a favor de los derechos humanos de los niños, Terre des Hommes (Tierra de Hombres). **La operación.-** Durante una operación en 2013, cuatro investigadores trabajaron durante 10 semanas haciéndose pasar por niñas filipinas en salas de chat. Se contactaron con 10 mil personas, de las cuales mil le pidieron a Sweetie que realizara actos sexuales ante una cámara web a cambio de dinero. Uno de ellos es Scott Robert Hansen (de Brisbane, Australia), quien se acaba de declarar culpable de tres cargos. Admitió haberle enviado fotos obscenas de sí mismo a Sweetie, poseer imágenes de abuso sexual infantil en su computadora

y de no cumplir con el mandato judicial para agresores sexuales. Fue sentenciado a dos años de prisión, aunque se cree que no ingresará en la cárcel porque ya lleva ocho meses detenido. Seguirá en cambio una orden correccional de 12 meses y se le obligará a participar en un programa de tratamiento para agresores sexuales. **El chat**.- La BBC pudo acceder al chat que mantuvo el agresor sexual con Sweetie. Hansen empezó preguntando: "Hola, ¿de verdad tienes 9 años?".
El operador que se hacía pasar por Sweetie contestó que sí, a lo que Hansen respondió: "Quieres chatear o poner la cámara con alguien mayor?". Después dijo: "Me gustan las niñas asiáticas, ¿quieres... acción?". Y sus comentarios se volvieron más explícitos: "Estoy desnudo, ¿has visto a un tipo desnudo?".Después encendió la cámara y realizó un acto sexual delante de Sweetie, que él creía era una niña de 9 años. **Los operadores.-** El canal de noticias británico también habló en exclusiva con uno de los operadores detrás de Sweetie, quien pidió mantenerse en el anonimato. En referencia a Hansen, indicó: "Fue muy directo, en un momento nos pidió que involucráramos a nuestra hermana ficticia de 8 años. Era muy difícil dormir por la noche después de interactuar con gente como Hansen". **Valor legal**.-Según dijo la jueza del caso, Judge Ryrie, durante la sentencia, Hansen tenía un extenso interés en aproximarse a los niños de diferentes maneras. Según Ryrie, el hecho de que Sweetie no fuera alguien real es irrelevante. "Si tú crees que esa es una niña de 9 años, para la ley eso es suficiente", dijo

Con ese antecedente, las entidades que desarrollaban o trabajaban en los escenarios informáticos del mundo, comenzaron a generar instrumentos de control y sanción a quienes en forma inescrupulosa utilizaban la informática para delinquir. Sin embargo, se encontró que los entes encargados de sancionar a quienes hacían uso ilegal y delictivo de las herramientas informáticas, no tenían cómo judicializar a los nuevos delincuentes. La ley inglesa sirvió para que otros países -en especial aquellos donde la internet tenía más desarrollo- se sumaran al

esfuerzo de discutir y promulgar leyes orientadas a proteger y sancionar la violación de la información.

En los países de la región la reacción fue lenta y tardía, de acuerdo con los estudios realizados por Cisco, según los cuales el país registraba una de las calificaciones más bajas en seguridad informática (62 puntos de 100 posibles), en comparación con otros seis países de Latinoamérica.

Esa situación, que obedece a distintos factores, según concepto de algunos ejecutivos de firmas relacionadas con la informática y la auditoría (Etek, Cisco, Trend Micro), se explica en factores como:

- Falta de información, falta de claridad o debilidad en la gestión gerencial, referidos particularmente a la implementación de la seguridad informática.
- Abuso en el empleo de los sistemas y sus aplicativos.
- Ausencia de políticas claras sobre seguridad informática.
- Falta de reconocimiento estratégico al área de Auditoría de Sistemas.
- Falta de conciencia en el desempeño de los sistemas de información.
- Baja gestión y poco uso de herramientas de análisis y control.
- Falta de evaluación con relaciones beneficio/costo y criterios de continuidad del negocio, sobre uso y seguridad de la información y los recursos informáticos.

Cisco presentó el reporte de seguridad 2014. En el informe se menciona que los vínculos débiles como software vencido, malos códigos, propiedades digitales abandonadas, o errores de usuarios contribuyen a aumentar las amenazas en la seguridad de las organizaciones.

Además, el informe de Cisco destaca que los métodos más utilizados para explotar vulnerabilidades son consultas de DNS, kits de explotación, ataques de amplificación, compromiso del sistema point-of-sale (POS), malvertising, ransomware, infiltración de protocolos de cifrado, ingeniería social y spam "lifeevent".

El reporte sustentado bajo una investigación a 16 organizaciones multinacionales evidenció cifras claves, así:

El 94 por ciento de las redes de clientes observadas en el año 2014 han sido identificadas con tráfico que se deriva hacia sitios web con malware y que son asociadas con la distribución de familias de malware como Palevo, SpyEye y Zeus

El 70 por ciento de las redes fueron identificadas con peticiones de emisión de DNS para Dynamic DNS Domains (Dominios DNS Dinámicos).

El 44 por ciento de las redes de los clientes observadas en el 2014 han emitido peticiones de DNS para sitios y dominios con dispositivos que entregan servicios de canal cifrados, utilizados por actores maliciosos para cubrir sus huellas exfiltrando los datos por medio de canales cifrados como VPN, SSH, SFTP, FTP y FTPS para evitar su detección

Los investigadores de seguridad de Cisco descubrieron que los ataques a Java subieron un 93 por ciento en todos los indicadores de compromiso (IOCs). Fuente: Informe CISCO 2014-Ecuador.

(Ver Anexo 33)

Según Manuel Bustos, director de la multinacional de seguridad de la información Etek: "La industria en general, el sector gobierno y las pyme son los menos preocupados por la seguridad de la información, porque requiere inversiones y normalmente no le dedican lo suficiente para lograr un nivel adecuado de seguridad" (Cisco).

Para José Battat, ejecutivo de Trend Micro: "En el país, las pyme viven un proceso más lento en cuanto a la implementación de estrategias de seguridad; sin embargo, poco a poco, tanto los proveedores como esas empresas han buscado los mecanismos para solventar esta falta" (Cisco).

De acuerdo con las conclusiones del mencionado estudio realizado por Cisco, líder mundial en redes, las tres principales formas de ataque informático a las organizaciones son, en su orden: virus informático

(45% del total), los abusos por parte de los empleados (42%) y luego la penetración a los sistemas por parte de fuentes externas (13%).

(Ver Anexo 34)

CONCEPTO DE DELITO INFORMÁTICO.

Es importante el concepto que dan los tratadistas y especialistas de esta materia, entre estos tenemos varias definiciones:

"Infracciones electrónicas son actitudes ilícitas en que se tienen a las computadoras (tecnologías) como instrumento (medio) o fin (concepto atípico) o las conductas típicas, antijurídicas y, culpables en que se tienen a las computadoras (tecnologías) como instrumento (medio) o fin (concepto típico)".(**Julio Téllez Valdez** –México). VER A: Einstein Alejandro Morales Galito (Venezuela) http://www.monografias.com/trabajos17/delitos-informaticos/delitos-informaticos.shtml

Para **Carlos Sarzana**, en su obra Criminalista Y 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".

Alberto Suárez-Sánchez (2009), por su parte, señala: "En conclusión, el delito informático está vinculado no sólo a la realización de una conducta delictiva a través de medios o elementos informáticos, o a los comportamientos ilícitos en los que aquellos sean su objeto, sino también a la afectación de la información per se como bien jurídico tutelado, diferente de los intereses jurídicos tradicionales".

Luis Camacho-Losa (1987), de otro lado, había dicho: "Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor, o que, por el contrario, produce un beneficio ilícito a su autor aun cuando no perjudique de forma directa o inmediata a la víctima, y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas".2

Otras concepciones sobre delito informático, complementarias todas, referidas por **Suárez-Sánchez** (2009), señalan un foco común con elementos distintos en su formalidad, más no en su esencia:

La especificidad del delito informático le viene dada por dos factores fundamentales: las acciones se vinculan al funcionamiento de una máquina y, en buena parte de los supuestos, recae sobre un objeto intangible o inmaterial (**Choclán-Montalvo**, 1997).

La realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnere los derechos del titular de un elemento informático, ya sea hardware o software (**Davara-Rodríguez**, 2007).

Podría ser delito informático todo comportamiento criminal en el que aparezca involucrado un ordenador; de este modo, casi cualquier delito con esta peculiaridad podría ser, eventualmente delito informático (**Aldama-Baquedano**, 1993).

Conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos (**Gómez-Perals**, 1994).

Mario Gerardo Piattini-Velthuis y Emilio del Peso-Navarro (2001) recuerdan el elemento sancionatorio: "Se podría definir el delito informático como toda acción (acción u omisión) culpable realizada por un ser humano, que cause perjuicio a persona sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor, aunque no perjudique de forma directa o indirecta a la víctima, tipificado por la Ley, que se realiza en el entorno informático y está sancionado con una pena".

La **Constitución de España** define el 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".

Guillermo Beltramone, Rodolfo Herrera-Bravo y Ezequiel Zabale (1998) añaden el concepto de soporte: "Toda conducta que revista características delictivas, es decir, sea típica, antijurídica y culpable y atente contra el soporte lógico de un sistema de procesamiento de información, y la cual se distingue de los delitos computacionales o tradicionales informatizados".

Henry William Torres-Torres, amplía el concepto a lo internacional en su definición de delito informático: "Toda conducta punible en la que el sujeto activo utilice método o técnica de carácter informático en su ejecución que tenga como medio o instrumento elementos integrantes de un sistema informático o telemático o intereses jurídicos tutelados por el derecho a la intimidad, a la propiedad intelectual y el software a que sin estar reconocida por nuestro legislador es aceptada por tratadistas internacionales como Infracción Informática".

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", "delito digital", "infracción informática", "cibercrímen".

Analizando estas determinaciones conceptuales estamos en condiciones de dar una definición de delito informático:

Son todas aquellas actitudes y conductas ilícitas sancionadas por el derecho penal, a quienes hacen uso indebido de cualquier medio tecnológico, de las nuevas tecnologías de la información, comunicación, e Informática, implicando actividades delictivas.

Entre las anteriores concepciones, hay dos enfoques complementarios, para entender el fenómeno informático: por una parte, la identificación de **conductas que utilizan** las herramientas informáticas en la acción delictiva y por la otra, las **conductas que atacan** o vulneran los bienes informáticos y sus componentes, ya cobijados por la protección jurídica del país.

También se advierte que, en el esfuerzo de llegar a una definición comprensiva pero simple, como lo hace la mayoría de tratadistas, se procura sintetizar las conductas tipificables como delito, lo cual conlleva el riesgo de confundir, eventualmente, la definición de delito informático, como género, con el objeto del delito mismo. A esto se agrega otra circunstancia que incide claramente en la definición de delito informático, como es la efectiva falta de 'madurez' en el tratamiento normativo penal de aquellas conductas que, no obstante ser antijurídicas y culpables, no han tenido la debida tipificación en algunos países, lo cual mantiene el riesgo en el sentido de la globalidad de las relaciones, de las comunicaciones, de los negocios.

El delito informático también se conoce con la denominación anglosajona de computercrime y se sabe que quienes cometen estos delitos son expertos conocedores de la tecnología, con

fundamento científico e investigativo de los sistemas y también del comportamiento humano y organizacional. Otra característica importante es que el atractivo del delito no siempre es el botín económico, sino que puede obedecer a intereses de diverso orden, como los personales, psicológicos, sociales, laborales, políticos o de simple curiosidad tecnológica. Paradójicamente, sus acechanzas están cubiertas o protegidas por la misma seguridad que ofrece la tecnología informática.

Clasificación

Según Oliver Hance en su libro "Leyes y Negocios en Internet", existen tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos:

Acceso no autorizado, actos dañinos o circulación de material dañino e intercepción no autorizada.

Otros autores han abordado el tema de los delitos informáticos sobre la base de dos criterios: como instrumento o medio, o como fin u objetivo.

Como instrumento o medio:	Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito
Como fin u objetivo:	En ésta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física

Otros sin embargo advierten una clasificación sui géneris, "delitos electrónicos" diciendo que existen tres categorías, a saber:

Los que utilizan la tecnología electrónica como método:	(Conductas criminógenas en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito).
Los que utilizan la tecnología electrónica como medio:	(Conductas criminógenas en donde para realizar un delito utilizan una computadora como medio o símbolo)
Los que utilizan la tecnología electrónica como fin:	(conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla

Ahora bien realicemos un análisis objetivo de estas clasificaciones a los delitos informáticos: como instrumento o medio, como fin u objetivo:

1. Como instrumento o medio	Se tienen a las conductas criminógenas que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.
2. Como fin u objetivo	En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

La jurisprudencia del Ecuador, muy claramente expone que los actos y conductas para que sean consideradas delito, deben cumplir con varios elementos: "Para que cualquier acto sea considerado como delito, se exige la concurrencia de los siguientes elementos integrados: a) Un sujeto activo, esto es, un individuo que quebrante la norma jurídica y que siendo imputable incurre por ello en la condicional punitiva determinada por el Legislador. b) Un objeto que se determina por el derecho violado, bien sea que éste pertenezca a personas naturales

o jurídicas; c) Un sujeto pasivo, esto es, la víctima, en otras palabras la persona que sufre el agravio; d) Un fin, esto es, la perturbación del orden jurídico. La noción de delito, por su parte, está compuesta también por tres elementos básicos: 1) El elemento material; 2) El elemento moral; y 3) El elemento jurídico. El elemento material, lo conforma a su vez la acción que desarrolla el autor; es el resultado de la acción, y la relación de casualidad que debe haber entre la acción del autor y el resultado. El elemento moral lo constituyen la imputabilidad y la culpabilidad. El elemento jurídico, a su vez, está conformado por la antijuricidad y la tipicidad". *(Gaceta Judicial N' 9, Serie XV,1990, págs. 2732.2733)

Sujeto activo en el delito Informático.

Las personas que cometen los "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes. 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, aun 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 "ingresa" 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 algún 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", aun 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 es 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 status socioeconómico, su comisión no se explica por pobreza, carencia de recreación, baja educación, ni por poca inteligencia, ni por inestabilidad emocional. Es difícil elaborar estadísticas sobre ambos tipos de delitos.

Las estadísticas son muy altas; no es fácil descubrirlo y sancionarlo, en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad, otra coincidencia que tienen estos tipos de delitos es que, generalmente, son difíciles en su comprobación por lo que el objeto de medidas o sanciones de carácter administrativo y privativo de la libertad, puede quedar en la impunidad.

El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador

de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sujeto pasivo en el delito informático.

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

El sujeto pasivo del delito ,es importante para el estudio de los "delitos informáticos", puesto que podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, para prever las acciones de los delincuentes.

La mayoría de los "delitos informáticos", no son descubiertos o no son denunciados a las autoridades responsables , a esto se suma la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; puede influenciar el temor por parte de las victimas en denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas.

Para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro.

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

En el mismo sentido, podemos decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, protegiendo los intereses de las víctimas y preparación por parte del personal encargado de la administración de justicia para atender e investigar estas conductas ilícitas.

En la legislación del Ecuador define a la infracción penal como: "Es la conducta típica, antijurídica y culpable cuya sanción se encuentra revista en este Código". Art.18.COIP.

Las infracciones se clasifican en delitos y contravenciones.

Delito es la infracción penal sancionada con pena privativa de libertad mayor a treinta días.

Contravención es la infracción penal sancionada con pena no privativa de libertad o privativa de libertad de hasta treinta días. Arts. 18 y 19.

En el capítulo segundo tenemos la CLASIFICACIÓN DE LA PENA:

"Las penas que se imponen en virtud de sentencia firme, con carácter principal o accesorio, son **privativas, no privativas de libertad y restrictivas de los derechos de propiedad,** de conformidad con este Código". Art. 58.

Penas privativas de libertad: Art. 59.	Las penas privativas de libertad tienen una duración de hasta cuarenta años. La duración de la pena empieza a computarse desde que se materializa la aprehensión.
Son penas no privativas de libertad: Art. 60.	1. Tratamiento médico, psicológico, capacitación, programa o curso educativo.

	2. Obligación de prestar un servicio comunitario. 3. Comparecencia periódica y personal ante la autoridad, en la frecuencia y en los plazos fijados ensentencia 4. Suspensión de la autorización o licencia para conducir cualquier tipo de vehículo. 5. Prohibición de ejercer la patria potestad o guardas en general. 6. Inhabilitación para el ejercicio de profesión, empleo u oficio. 7. Prohibición de salir del domicilio o del lugar determinado en la sentencia. 8. Pérdida de puntos en la licencia de conducir en las infracciones de tránsito. 9. Restricción del derecho al porte o tenencia de armas. 10. Prohibición de aproximación o comunicación directa con la víctima, sus familiares u otras personas dispuestas en sentencia, en cualquier lugar donde se encuentren o por cualquier medio verbal, audiovisual, escrito, informático, telemático o soporte físico o virtual. 11. Prohibición de residir, concurrir o transitar en determinados lugares. 12. Expulsión y prohibición de retorno al territorio ecuatoriano para personas extranjeras. 13. Pérdida de los derechos de participación. La o el juzgador podrá imponer una o más de estas sanciones, sin perjuicio de las penas previstas en cada tipo penal

Son penas restrictivas de los derechos de propiedad: Art.69.	1. **Multa**, cuyo valor se determina en salarios básicos unificados del trabajador en general. La multa debe pagarse de manera íntegra e inmediata una vez que la respectiva sentencia se ejecutoríe. No obstante, cuando la persona sentenciada demuestre su incapacidad material para cancelarla en las condiciones antes previstas, la o el juzgador podrá autorizar que su cumplimiento se realice de la siguiente manera:
	a) Pago a plazos o por cuotas durante el mismo tiempo de la condena.
	b) Condonación de una parte de la multa si, además, se demuestra extrema pobreza.
	c) Servicio comunitario equivalente, únicamente en las infracciones sancionadas con penas privativas de libertad de un día a seis meses.
	2. Comiso penal, procede en todos los casos de delitos dolosos y recae sobre los bienes, cuando estos son instrumentos, productos o réditos en la comisión del delito. No habrá comiso en los tipos penales culposos. En la sentencia condenatoria, la o el juzgador competente dispondrá el comiso de:
	a) Los bienes, fondos o activos, o instrumentos equipos y dispositivos informáticos utilizados para financiar o cometer la infracción penal o la actividad preparatoria punible.
	b) Los bienes, fondos o activos, contenido digital y productos que procedan de la infracción penal.
	c) Los bienes, fondos o activos y productos en los que se transforman o convierten los bienes provenientes de la infracción penal.

	d) El producto del delito que se mezcle con bienes adquiridos de fuentes lícitas; puede ser objeto de comiso hasta el valor estimado del producto entremezclado. e) Los ingresos u otros beneficios derivados de los bienes y productos provenientes de la infracción penal. Cuando tales bienes, fondos o activos, productos e instrumentos no pueden ser comisados, la o el juzgador dispondrá el pago de una multa de idéntico valor, adicional a la prevista para cada infracción penal. En caso de sentencia condenatoria ejecutoriada, dentro de procesos penales por lavado de activos, terrorismo y su financiamiento, y delitos relacionados con sustancias catalogadas sujetas a fiscalización, si tales bienes, fondos o activos, productos e instrumentos no pueden ser comisados, la el juzgador dispondrá el comiso de cualquier otro bien de propiedad del condenado, por un valor equivalente, aun cuando este bien no se encuentre vinculado al delito.

INFRACCIONES INFORMÁTICAS.

Expongo un cuadro de estudio general sobre los principales delitos informáticos y su incidencia, para tener una idea de la magnitud del problema que afronta la sociedad con este tipo de delitos:

CÓDIGO ORGÁNICO INTEGRAL PENAL. (CUADRO INFRACCIONES INFORMÁTICAS) **ELABORACIÓN:** Dr. Juan José Páez Rivadeneira.	
TÍTULO IV. INFRACCIONES EN PARTICULAR	**DESCRIPCIÓN**

CAPÍTULO PRIMERO. GRAVES VIOLACIONES A LOS DERECHOS HUMANOS Y DELITOS CONTRA EL DERECHO INTERNACIONAL HUMANITARIO **SECCIÓN TERCERA.** **Diversas formas de explotación.**	Artículo 96.- **Tráfico de órganos**.- La persona que, fuera de los casos permitidos por la ley, realice actos que tengan por objeto la intermediación onerosa o negocie por cualquier medio* o traslade órganos, tejidos, fluidos, células, componentes anatómicos o sustancias corporales, será sancionada con pena privativa de libertad de **trece a dieciséis años.** Artículo 97.- **Publicidad de tráfico de órganos**.- La persona que promueva, favorezca, facilite o publicite* la oferta, la obtención o el tráfico ilegal de órganos y tejidos humanos o el trasplante de los mismos será sancionada con pena privativa de libertad **de siete a diez años** Artículo 99.- **Turismo para la extracción, tratamiento ilegal o comercio de órganos.-** La persona que organice, **promueva***, ofrezca, brinde, adquiera o contrate actividades turísticas para realizar o favorecer las actividades de tráfico, extracción o tratamiento ilegal de órganos y tejidos, será sancionada con pena privativa de libertad de **siete a diez años.**
	Artículo 102.- **Turismo sexual**.- La persona que organice, **promueva**, ofrezca, brinde, traslade, reclute, adquiera o contrate actividades turísticas que impliquen servicios de naturaleza sexual, será sancionada con pena privativa de libertad de **siete a diez años**. Si las víctimas se encuentran en alguno de los siguientes casos, la pena privativa de libertad será de **diez a trece años:** 1. Si son niñas, niños o adolescentes o personas en situación

	de vulnerabilidad, aun cuando hayan prestado su consentimiento. 2. Cuando se utilice violencia, amenaza o intimidación. 3. La persona no tenga capacidad para comprender el significado del hecho. Artículo 103.- **Pornografía con utilización de niñas, niños o adolescentes**.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de **trece a dieciséis años**. Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de **dieciséis a diecinueve años.** **veintiséis años.** Artículo 104.- **Comercialización de pornografía con utilización de niñas, niños o adolescentes.**- La persona que publicite, compre, posea, porte, transmita*, descargue*, almacene*, importe, exporte o venda, por cualquier medio, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años. Artículo 110.- **Disposiciones comunes**.- Para los delitos previstos en las Secciones segunda y tercera de este capítulo se observarán las

	siguientes disposiciones comunes: 1. En estos delitos, la o el juzgador, adicional a la pena privativa de libertad podrá imponer una o varias penas no privativas de libertad. 2. En los casos en los que la o el presunto agresor sea ascendiente o descendiente, colateral hasta el cuarto grado de consanguinidad o segundo de afinidad, cónyuge, excónyuge, conviviente, exconviviente, pareja o expareja en unión de hecho, tutora o tutor, representante legal, curadora o curador o cualquier persona a cargo del cuidado o custodia de la víctima, la o el juez de Garantías Penales como medida cautelar **suspenderá** la patria potestad, tutoría, curatela y cualquier otra modalidad de cuidado sobre la víctima a fin de proteger sus derechos. 3. Para estos delitos no cabe la atenuante prevista en el número 2 del artículo 45* de este Código. 4. El comportamiento público o privado de la víctima, anterior a la comisión de la infracción, no es considerado dentro del proceso. 5. En estos delitos el consentimiento dado por la víctima no excluye la responsabilidad penal ni disminuye la pena correspondiente. 6. Las víctimas en estos delitos podrán ingresar al programa de víctimas y testigos.
***Medio.-**Definición Real Academia de la Lengua Española: (Del lat. medĭus). 11. m. Cosa que puede servir para un determinado fin. Medios de transporte, de comunicación. Medio de comunicación. - 1. m. Órgano destinado a la información pública. U. m. en pl. -	***Descargue**: no está en el diccionario de la RAE, pero en términos de tecnología refiere a bajar archivos de bases de datos o de la web. *Almacene: La palabra almacene no está registrada en el Diccionario. La que se muestra a continuación tiene

14. m. Diligencia o acción conveniente para conseguir algo. ***Promueva.** Definición Real Academia de la Lengua Española: Promover. (Del lat. promovēre). 1. tr. Iniciar o impulsar una cosa o un proceso, procurando su logro. 2. tr. Levantar o elevar a alguien a una dignidad o empleo superior al que tenía. 3. tr. Tomar la iniciativa para la realización o el logro de algo. ***Publicite**: RAE: publicitar. 1. tr. Promocionar algo mediante publicidad. PUBLICIDAD: 3. f. Divulgación de noticias o anuncios de carácter comercial para atraer a posibles compradores, espectadores, usuarios, etc. ***Transmita**: transmitir. (Del lat. transmittĕre). 1. tr. Trasladar, transferir. 2. tr. Dicho de una emisora de radio o de televisión: Difundir noticias, programas de música, espectáculos, etc. U. t. c. intr. 3. tr. Hacer llegar a alguien mensajes o noticias. 4. tr. Comunicar a otras personas enfermedades o estados de ánimo. 5. tr. Conducir o ser el medio a través del cual se pasan las vibraciones o radiaciones. 6. tr. En una máquina, comunicar el movimiento de una pieza a otra. U. t. c. prnl. 7. tr. Der. Enajenar, ceder o dejar a alguien un derecho u otra cosa.	formas con una escritura cercana. Almacenar: 3. tr. Inform. Registrar información en la memoria de un ordenador. *Artículo 45.- **Circunstancias atenuantes de la infracción.**- Son circunstancias atenuantes de la infracción penal: 1. Cometer infracciones penales contra la propiedad sin violencia, bajo la influencia de circunstancias económicas apremiantes. 2. Actuar la persona infractora por temor intenso o bajo violencia. 3. Intentar, en forma voluntaria anular o disminuir las consecuencias de la infracción o brindar auxilio y ayuda inmediatos a la víctima por parte de la persona infractora. 4. Reparar de forma voluntaria el daño o indemnizar integralmente a la víctima. 5. Presentarse en forma voluntaria a las autoridades de justicia, pudiendo haber eludido su acción por fuga u ocultamiento. 6. Colaborar eficazmente con las autoridades en la investigación de la infracción.
SECCIÓN CUARTA **Delitos contra la integridad sexual y reproductiva**	Artículo 168.- **Distribución de material pornográfico a niñas, niños y adolescentes.**- La persona que difunda, venda o entregue a niñas, niños o adolescentes, **material pornográfico**, será sancionada con pena privativa de libertad de uno a

	tres años. Artículo 173.- **Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos**.- La persona que a través de un medio electrónico o telemático proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años. Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años. La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor dedieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años. Artículo 174.- **Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos**.- La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexualescon menores de dieciocho años de edad, será sancionada con pena privativa de libertad de siete a diez años. Artículo 175.- Disposiciones comunes a los delitos contra la integridad sexual y reproductiva.-

	Para los delitos previstos en esta Sección se observarán las siguientes **disposiciones comunes**: 1. En estos delitos, la o el juzgador, adicional a la pena privativa de libertad puede imponer una o varias penas no privativas de libertad. 2. En los casos en los que la o el presunto agresor sea ascendiente o descendiente o colateral hasta el cuarto grado de consanguinidad o segundo de afinidad, cónyuge, excónyuge, conviviente, ex conviviente, pareja o ex pareja en unión de hecho, tutora o tutor, representante legal, curadora o curador o cualquier persona a cargo del cuidado o custodia de la víctima, el juez de Garantías Penales como medida cautelar suspenderá la patria potestad, tutoría, curatela y cualquier otra modalidad de cuidado sobre la víctima a fin de proteger sus derechos. Esta medida también la podrá solicitar la o el fiscal, de oficio o petición de parte la o el juez competente. 3. Para estos delitos no será aplicable la atenuante prevista en el número 2 del artículo 45 de este Código. 4. El comportamiento público o privado de la víctima, anterior a la comisión de la infracción sexual, no es considerado dentro del proceso. 5. En los delitos sexuales, el consentimiento dado por la víctima menor de dieciocho años de edad es irrelevante. 6. Las víctimas en estos delitos pueden ingresar al programa de víctimas y testigos.

SECCIÓN QUINTA **Delitos contra el derecho a la igualdad** PARÁGRAFO PRIMERO **Delito de discriminación**	Artículo 176.- **Discriminación**.- La persona que salvo los casos previstos como políticas de acción afirmativa propague* practique o incite* **a toda distinción, restricción, exclusión o preferencia** en razón de nacionalidad, etnia, lugar de nacimiento, edad, sexo, identidad de género u orientación sexual, identidad cultural, estado civil, idioma, religión, ideología, condición socioeconómica, condición migratoria, discapacidad o estado de salud con el objetivo de anular o menoscabar el reconocimiento, goce o ejercicio de derechos en condiciones de igualdad, será sancionada con pena privativa de libertad de uno a tres años. Si la infracción puntualizada en este artículo es ordenada o ejecutada por las o los servidores públicos, será sancionada con pena privativa de libertad de tres a cinco años.
***PROPAGUE**. RAE: propagar. (Del lat. propagāre). 1. tr. Multiplicar por generación u otra vía de reproducción. U. t. c. prnl. 2. tr. Hacer que algo se extienda o llegue a sitios distintos de aquel en que se produce. 3. tr. Extender, dilatar o aumentar algo. U. t. c. prnl. 4. tr. Extender el conocimiento de algo o la afición a ello. U. t. c. prnl. En tecnología: fig. Difundir o extender [una cosa] los efectos de ella. Puede ser un virus informático, o información protegida.	***INCITE.** RAE: incitar. (Del lat. incitāre). 1. tr. Mover o estimular a alguien para que ejecute algo.
SECCIÓN SEXTA **Delitos contra el derecho a la intimidad personal y familiar**	Artículo 178.- **Violación a la intimidad**.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte,

	examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de **información pública*** de acuerdo con lo previsto en la ley. Artículo 179.- **Revelación de secreto***.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año. Artículo 180.- **Difusión de información de circulación restringida**.- La persona que difunda información de circulación restringida* será sancionada con pena privativa de libertad de uno a tres años. **Es información de circulación restringida:** 1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley. 2. La información producida por la Fiscalía en el marco de una investigación previa. 3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia.

*INFORMACIÓN PÚBLICA: Es la información que toda persona tiene derecho a manifestar por medio de la libertad de expresión y difusión de pensamiento oral o escrito, por cualquier medio de comunicación, sin previa autorización, sin censura o impedimento, siguiendo los reglamentos de la ley. También es la información que todo el mundo tiene derecho a solicitar y a recibir de parte de cualquier entidad pública, así sea que tenga un costo o un plazo para ser entregada. Un ejemplo de esto son los informes del estado que deben estar a disposición de cualquiera que lo exija. FUENTE: http://www.tiposde.com/escritos/informacion/tipos-de-informacion.html	*REVELACIÓN DE SECRETO: El delito de descubrimiento de secretos es un atentado contra la intimidad de la persona que puede realizarse de dos maneras distintas: por medio del apoderamiento de documentos o efectos personales, o mediante la intromisión en ámbitos reservados de la víctima. En el primer caso, el supuesto típico consiste en apoderarse de papeles, cartas, mensajes de correo electrónico o cualesquiera documentos o efectos personales de otra persona, siendo suficiente el apoderamiento y no necesario desposeer al afectado de papeles, cartas o mensajes, ni tampoco que se descubre de entre ellos algún secreto. Por otro lado, en el segundo caso, se castiga a aquellos que intercepten las telecomunicaciones o utilicen artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación. Asimismo, la conducta interna del sujeto que comete el delito será castigada siempre que tenga intención de apoderarse o entrometerse en asuntos protegidos por la intimidad de la persona y se realicen estos actos sin el consentimiento de su titular. Fuente: http://www.delitosinformaticos.com/10/2012//revelacion-de-secretos/de-los-delitos-de-descubrimiento-revelacion-de-secretos *INFORMACION DE CIRCULACION RESTRINGIDA: concepto ligado al contenido del articulo.

SECCIÓN SÉPTIMA **Delito contra el derecho al honor y buen nombre**	Artículo 182.- **Calumnia.-** La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años. No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa. No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo. No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación. La retractación no constituye una forma de aceptación de culpabilidad.
SECCIÓN NOVENA **Delitos contra el derecho a la propiedad**	Artículo 185.- **Extorsión.-** La persona que, con el propósito de obtener provecho personal o para un tercero, obligue a otro, con violencia o intimidación, a realizar u omitir un acto o negocio jurídico en perjuicio de su patrimonio o el de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. La sanción será de cinco a siete años si se verifican alguna de las siguientes circunstancias:

	1. Si la víctima es una persona menor a dieciocho años, mayor a sesenta y cinco años, mujer embarazada o persona con discapacidad, o una persona que padezca enfermedades que comprometan su vida. 2. Si se ejecuta con la intervención de una persona con quien la víctima mantenga relación laboral, comercio u otra similar o con una persona de confianza o pariente dentro del cuarto grado de consanguinidad y segundo de afinidad. 3. Si el constreñimiento se ejecuta con amenaza de muerte, lesión, secuestro o acto del cual pueda derivarse calamidad, infortunio o peligro común. 4. Si se comete total o parcialmente desde un lugar de privación de libertad. 5. Si se comete total o parcialmente desde el extranjero*. Artículo 186.- **Estafa*.**- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que: 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.

	2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares. 3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica. 4. Induzca a la compra o venta pública de valores por medio de cualquieracto, práctica, mecanismo o artificio engañoso o fraudulento. 5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. La persona que perjudique a más de dos personas o el monto de su perjuicio sea igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de siete a diez años. La estafa cometida a través de una institución del Sistema Financiero Nacional, de la economía popular y solidaria que realicen intermediación financiera mediante el empleo de fondos públicos o de la Seguridad Social, será sancionada con pena privativa de libertad de siete a diez años. La persona que emita boletos o entradas para eventos en escenarios públicos o de concentración masiva por sobre el número del aforo autorizado por la autoridad pública competente, será sancionada con pena privativa de libertad de treinta a noventa días. para aprovecharse de los servicios públicos de energía eléctrica, agua, derivados de hidrocarburos, gas

	natural, gas licuado de petróleo o de telecomunicaciones, en beneficio propio o de terceros, o efectúen conexiones directas, destruyan, perforen o manipulen las instalaciones de transporte, comunicación o acceso a los mencionados servicios, será sancionada con pena privativa de libertad de seis meses a dos años. La pena máxima prevista se impondrá a la o al servidor público que permita o facilite la comisión de la infracción u omita efectuar la denuncia de la comisión de la infracción. La persona que ofrezca, preste o comercialice servicios públicos de luz eléctrica, telecomunicaciones o agua potable sin estar legalmente facultada, mediante concesión, autorización, licencia, permiso, convenios, registros o cualquier otra forma de contratación administrativa, será sancionada con pena privativa de libertad de uno a tres años. Artículo 191.- **Reprogramación o modificación de información de equipos terminales móviles**.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años. Artículo 192.- **Intercambio, comercialización o compra de información de equipos terminales móviles**.- La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años. Artículo 193.- **Reemplazo de identificación de terminales**

	móviles.- La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años. Artículo 194.- **Comercialización ilícita de terminales móviles**.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. utoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. Artículo 195.- **Infraestructura ilícita**.- La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años. No constituye delito, la apertura de bandas para operación de los equipos terminales móviles.
***Estafa desde el extranjero**: "El modus operandi de esta nueva modalidad, la realizan con personas que están buscando empleo vía internet, utilizando portales habilitados como bolsas de trabajo, mediante los cuales ofrecen empleos,	***ESTAFA**: Les comparto otra forma de **estafa vía internet**. "El perfil que describe en su CV es adecuado para la vacante "Supervisor de Sistemas" que oferta un sueldo bruto mensual de $15,000 + PSL, por lo que le

usurpando el nombre de alguna empresa nacional o transnacional de renombre. A esta modalidad se le llama Phishing. "Cuando la víctima contacta a la supuesta empresa de renombre, le solicitan sus datos personales, con finalidad de evaluar su perfil personal y profesional, pero la intención es conocer exactamente su información personal. Cuando el delincuente tiene completamente identificada a la víctima, empieza la extorsión por medio de un correo electrónico con amenazas a la víctima y a su familia si no deposita cierta cantidad de dinero en una cuenta bancaria (tarjeta de débito), intimidándolos por tener pleno conocimiento de los datos personales (dirección y puesto de trabajo, teléfonos personales etc) información sensible que proporciono, con la cual estos delincuentes estarán amenazándolo en hacerle daño a usted o a su familia si se niega a darles el dinero. La intimidación vía electrónica es con la siguiente leyenda "Sabemos que se te facilita conseguir $5000 para tu tranquilidad, a cambio obtendrás que te eliminemos de nuestra base de datos, lo que te garantiza que jamás te volvamos a contactar…" Fuente: http://mariomenesescpo.com/2013/06/16/extorsion-via-internet/	solicitamos atentamente presentar los exámenes médicos correspondientes para cubrir la plaza disponible (…) sólo esta ocasión la prueba tiene un costo mínimo que debe ser cubierto por usted y el mismo se reembolsa en su primer quincena laboral. El procedimiento es el siguiente: 1-.Cubrir mediante un depósito bancario la cantidad de $250.00 (Doscientos cincuenta pesos 00/100 MN.)…".En el mismo correo se instruye a la víctima sobre dónde y cómo hacer el depósito. Una vez que la víctima entrega la cantidad solicitada, se pierde el contacto, sin que haya recibido su dinero de vuelta y, mucho menos, un empleo.(IBIDEM http://mariomenesescpo.com/2013/06/16/extorsion-via-internet/)
SECCIÓN DÉCIMA **Delitos contra el derecho a la identidad**	Artículo 211.- **Supresión, alteración o suposición de la identidad y estado civil.-** La persona que ilegalmente impida, altere, añada o suprima la inscripción de los datos de identidad suyos o de otra persona en programas informáticos, partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la Dirección General de Registro Civil, Identificación y de Cedulación o sus

	dependencias o, inscriba como propia, en la Dirección General de Registro Civil, Identificación y de Cedulación a una persona que no es su hijo, será sancionada con pena privativa de libertad de uno a tres años. La persona que ilegalmente altere la identidad de una niña o niño; la sustituya por otra; entregue o consigne datos falsos o supuestos sobre un nacimiento; usurpe la legítima paternidad o maternidad de niña o niño o declare falsamente el fallecimiento de un recién nacido, será sancionada con pena privativa de libertad de tres a cinco años. Artículo 212.- **Suplantación de identidad**.- La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.
CAPÍTULO TERCERO DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR SECCIÓN TERCERA **Delitos contra la seguridad de los activos de los sistemas de información y comunicación.**	Art. 229.- **Revelación ilegal de base de datos**.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular

	y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años. Art. 230.- **Interceptación ilegal de datos**.- Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.***(Jurisprudencia)**

	Art. 231.- **Transferencia electrónica de activo patrimonial.**- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. Art. 232.- **Ataque a la integridad de sistemas informáticos.**- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que: 1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos

	señalados en el primer inciso de este artículo. 2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general. Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. Art. 233.- **Delitos contra la información pública reservada legalmente**.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad. Art. 234.- **Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.**- La

	persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.
***Jurisprudencia:** Gaceta Judicial, CIRCUNSTANCIAS ATENUANTES, 18-nov-1963Gaceta Judicial, CIRCUNSTANCIA AGRAVANTE DE LA INFRACCION, 10-nov-1993. Gaceta Judicial, PENA DE RECLUSION MAYOR ORDINARIA, 28-ene-1994. Gaceta Judicial, ATENUANTES EN LA PENA, 15-feb-1995. Gaceta Judicial, MODIFICACION DE LA PENA, 29-sep-2000.	
CAPÍTULO QUINTO DELITOS CONTRA LA RESPONSABILIDAD CIUDADANA SECCIÓN QUINTA Delitos contra el régimen de desarrollo	Art. 298.- **Defraudación tributaria**.- La persona que simule, oculte, omita, falsee o engañe en la determinación de la obligación tributaria, para dejar de pagar en todo o en parte los tributos realmente debidos, en provecho propio o de un tercero, será sancionada cuando: 1. Utilice identidad o identificación supuesta o falsa en la solicitud de inscripción, actualización o cancelación de los registros que llevan las administraciones tributarias. 2. Utilice datos, información o documentación falsa o adulterada en la solicitud de inscripción, actualización o cancelación de los

	registros que llevan las administraciones tributarias. 3. Realice actividades en un establecimiento a sabiendas de que se encuentre clausurado. 4. Imprima o haga uso de comprobantes de venta o de retención o de documentos complementarios que no sean autorizados por la Administración Tributaria. 5. Proporcione a la administración tributaria informes, reportes con mercancías, datos, cifras, circunstancias o antecedentes falsos, incompletos, desfigurados o adulterados. 6. Haga constar en las declaraciones tributarias datos falsos, incompletos, desfigurados o adulterados, siempre que el contribuyente no haya ejercido, dentro del año siguiente a la declaración, el derecho a presentar la declaración sustitutiva en la forma prevista en la ley. 7. Falsifique o altere permisos, guías, facturas, actas, marcas, etiquetas o cualquier otro tipo de control de fabricación, consumo, transporte, importación y exportación de bienes gravados. 8. Altere libros o registros informáticos de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos. 9. Lleve doble contabilidad con distintos asientos en libros o registros informáticos, para el mismo negocio o actividad económica. 10. Destruya total o parcialmente, los libros o registros informáticos de contabilidad u otros exigidos por las

	normas tributarias o los documentos que los respalden, para evadir el pago o disminuir el valor de obligaciones tributarias. 11. Venda para consumo aguardiente sin rectificar o alcohol sin embotellar y declare falsamente volumen o grado alcohólico del producto sujeto al tributo, fuera del límite de tolerancia establecido por el INEN, así como la venta fuera del cupo establecido por el Servicio de Rentas Internas, del alcohol etílico que se destine a la fabricación de bebidas alcohólicas, productos farmacéuticos y aguas de tocador. 12. Emita, acepte o presente a la administración tributaria comprobantes de venta, de retención o documentos complementarios por operaciones inexistentes o cuyo monto no coincida con el correspondiente a la operación real. 13. Emita comprobantes de venta por operaciones realizadas con empresas fantasmas, inexistentes o supuestas. 14. Presente a la administración tributaria comprobantes de venta por operaciones realizadas con empresas fantasmas, inexistentes o supuestas. 15. Omita ingresos, incluya costos, gastos, deducciones, exoneraciones, rebajas o retenciones falsas o inexistentes o superiores a las que procedan legalmente, para evitar el pago de los tributos debidos. 16. Extienda a terceros el beneficio de un derecho a subsidios, rebajas, exenciones, estímulos fiscales o se beneficie de los mismos sin derecho. 17. Simule uno o más actos, contratos para obtener o dar un beneficio de subsidio, rebaja, exención o estímulo fiscal.

	18. Exista falta de entrega deliberada, total o parcial, por parte de los agentes de retención o percepción de los impuestos retenidos o percibidos, después de diez días de vencido el plazo establecido en la norma para hacerlo. 19. Exista obtención indebida de una devolución de tributos, intereses o multas. Las **penas aplicables** al delito de defraudación son: En los casos de los numerales **del 1 al 11,** será sancionada con pena privativa de libertad de uno a tres años. En los casos de los numerales del 12 al 14, será sancionada con pena privativa de libertad de tres a cinco años. Cuando el monto de los comprobantes de venta supere los cien salarios básicos unificados del trabajador en general, será sancionada con el máximo de la pena privativa de libertad prevista para estos delitos. En los casos de los numerales del 15 al 17, será sancionada con pena privativa de libertad de cinco a siete años. Cuando los impuestos defraudados superen los cien salarios básicos unificados del trabajador en general, será sancionada con el máximo de la pena privativa de libertad prevista para estos delitos. En el caso de los numerales 18 y 19, será sancionada con pena privativa de libertad de cinco a siete años. Cuando los impuestos retenidos o percibidos que no hayan sido declarados o pagados, así como en los casos de impuestos que hayan sido devueltos dolosamente, superen los cien salarios básicos unificados del trabajador en general, será sancionada con pena

	privativa de libertad de siete a diez años. Constituye defraudación agravada y será sancionada con el máximo de la pena prevista para cada caso, la cometida con la participación de uno o más funcionarios o servidores de la administración tributaria y acarreará, además, la destitución del cargo de dichos funcionarios o servidores. En el caso de personas jurídicas, sociedades o cualquier otra entidad que, aunque carente de personería jurídica, constituya una unidad económica o un patrimonio independiente de la de sus miembros, de conformidad con lo dispuesto en este Código, serán sancionadas con pena de extinción de la persona jurídica y multa de cincuenta a cien salarios básicos unificados del trabajador en general. Las personas que ejercen control sobre la persona jurídica o que presten sus servicios como empleadas, trabajadoras o profesionales, serán responsables como a utoras si han participado en la defraudación ributaria en beneficio de la persona jurídica, aunque no hayan actuado con mandato alguno. En los casos en los que la o el agente de retención o agente de percepción sea una institución del Estado, la o el funcionario encargado de la recaudación, declaración y entrega de los impuestos percibidos o retenidos al sujeto activo, además de la pena privativa de libertad por la defraudación, sin prejuicio de que se configure un delito más grave, será sancionado con la destitución y quedará inhabilitado para ocupar cargos públicos por seis meses.

	Cada caso será investigado, juzgado y sancionado sin perjuicio del cumplimiento de las obligaciones tributarias, así como del pago de los impuestos debidos.

JURISPRUDENCIA EUROPEA:

Que el novio se vengue..... si tiene precio -35.000 €- Las venganzas personales están a la vuelta de la esquina y, sino sorpréndanse con la sanción que ha impuesto el Tribunal Regional de Marburgo a un ciudadano por publicar videos caseros de su ex novia manteniendo relaciones sexuales con él. En efecto, este ciudadano alemán de 40 años se sintió tan afligido por el término de su relación con su "amada" -el ego masculino- que decidió publicar un video casero a través de la Red, incluyendo los datos reales de contacto de ella, además de las imágenes donde aparecían ambos manteniendo relaciones sexuales. La mujer empezó a sospechar, cuando varios desconocidos comenzaron a ponerse en contacto con ella -caso parecido al del vecino que por venganza incluyó los datos de su vecina en un portal de contactos-. Finalmente y, como no podía haber sido menos, los jueces han dictado sentencia a favor de la mujer, declarándole a él culpable de injuria, difusión pornográfica y violación de derechos de imagen, además de tener que pagar una indemnización económica de 35.000 €. *(Fuente: www.delitosinformaticos.com).

COMERCIO INTERNET. La compra en Internet suplantando la identidad del titular de una tarjeta no es estafa. El pasado mes de febrero el juzgado de Málaga hizo público su fallo en el que consideraba que no constituye estafa la compra en Internet facilitando los datos de una tarjeta tercera. Los hechos fueros los que a continuación se detallan. Dos sujetos adquirieron por Internet un DVD facilitando los datos identificativos de una tarjeta, cuya titularidad pertenecía a otro sujeto diferente. La Sentencia señala que no es posible calificar el hecho como estafa, puesto que no producen los requisitos necesarios contenidos en el artículo 248 CP: manipulación de un programa y; la

alteración, supresión u ocultación de datos en el sistema manipulado. Así mismo, el comerciante no realizó las comprobaciones necesarias para identificar al titular. Art. 579 (Registro electrónico de actos procesales).* (Fuente: www.delitosinformaticos.com).

ECUADOR:

DELITO DE INJURIA A TRAVES DE CORREO ELECTRÓNICO Las expresiones que constan en el correo o mensaje electrónico enviado desde la dirección electrónica augustaespinosa(arroba)autec-mb.com, en el que se dice que "El señor Páez ha sido separado de Autec y que los abogados han entablado una acción judicial en su contra con los cargos de abuso de confianza, disponibilidad indebida de fondos y boicot", enviados al señor Gino Saer, Gerente de Exportaciones para América Latina de la Empresa Freightliner, distribuidora de Mercedes Benz y a otros altos ejecutivos de la misma empresa, en México, así como a un alto ejecutivo de la casa matriz de Estados Unidos, constituyen, sin lugar a dudas, una falsa imputación de varios delitos supuestamente cometidos por el ciudadano Gino José Páez Puga (abuso de confianza, disponibilidad indebida de fondos y boicot) y que fueron difundidos con la deliberada intención de causar daño a la honra, reputación y dignidad del acusado "animus injuriando", elemento fundamental de la injuria calumniosa, de parte de la señora María Augusta Galarza Dávila de Espinosa, es evidente al haber ésta, hecho conocer a importante empresarios vinculados con las actividades habituales del acuerdo, la serie de delitos por los cuales, según ella, estaba siendo enjuiciado, pues del proceso, no existe constancia alguna de tales acciones judiciales. El primer inciso del Art. 481 del Código Penal, manifiesta que injuria calumniosa "consiste en la falsa imputación de un delito" y eso es precisamente lo que se evidencia del correo electrónico, que siendo supuestamente "privado y confidencial", como dice la acusada, sin embargo de aquello se lo difundió, para conocimiento de terceras personas. En ninguna parte de la ley se menciona que para que exista injuria calumniosa, es necesario narrar los hechos que constituyen el delito imputado, siendo aquella premisa alejada de la realidad jurídica Gaceta Judicial. Año CVIII. Serie XVIII, No. 3. Página 1012.(Quito, 7 de mayo de 2007)

JUICIO POR PRODUCCIÓN, COMERCIALIZACIÓN IMÁGENES PORNOGRÁFICAS. La Sala Penal de la Corte Nacional de Justicia considera, que una resolución dentro de un proceso judicial se debe fundamentar en dos elementos: La coherencia, que es la lógica interna del discurso, juicios que sirven para la construcción lógica del razonamiento; y: La congruencia, que es la relación entre la decisión y la realidad procesal; por ello se resuelve que, la quaestiofacti planteada por la Fiscalía es conducente, clara, e inequívoca sobre la actividad que realizaba el hoy recurrente, quien efectivamente tenía en su local comercial de películas, discos compactos con imágenes pornográficas de personas menores de 18 años, y que las comercializaba, considerando que el comercio de fotografías y películas, que representan actividades sexuales explícitas realizadas por niños, niñas y adolescentes, está intrínsecamente relacionada con el abuso y explotación sexual. En el tipo penal acusado, la función protectora de la norma es más amplia, por tratarse de un grupo de atención prioritaria y de un alto nivel de vulnerabilidad, como son los niños, niñas y adolescentes, en los delitos de explotación sexual (pornografía), no se puede hablar solamente de la libertad sexual como bien jurídico protegido, dada la edad de las víctimas, que no tienen la condición de prestar válidamente su consentimiento ni de decidir sobre su libertad sexual, por lo que el Estado precautela en este caso, la indemnidad o intangibilidad sexual de los niños, niñas y adolescentes, buscándose dar seguridad y protección al libre desarrollo de su personalidad, sin intervenciones traumáticas de terceros. Se casa parcialmente de oficio la sentencia recurrida, en cuanto a la modificación de la pena, por haberse aplicado erróneamente atenuantes, le impone la pena privativa de libertad de dieciséis años de reclusión mayor extraordinaria; y, por ser el sentenciado el único recurrente, de conformidad al artículo 77.14, de la Constitución de la República, y al artículo 328 del Código de Procedimiento Penal, se mantiene la pena de 8 años de reclusión mayor ordinaria. Gaceta Judicial. Año CXIII. Serie XVIII, No. 12. Página 4462.(Quito, 06 de Agosto del 2012)

SUPUESTO ERROR DE DATOS DE PANTALLA. Expediente 362, Registro Oficial Suplemento 150, 8 de Julio del 2014. No. 362-

2010 JUICIO DE IMPUGNACIÓN QUE SIGUE: CIA. FERRERO DEL ECUADOR S. A. EN CONTRA DEL DIRECTOR GENERAL DEL SRI. Juez Ponente: Dr. José Suing Nagua. CORTE NACIONAL DE JUSTICIA SALA ESPECIALIZADA DE LO CONTENCIOSO TRIBUTARIO Quito, a 2 de Septiembre del 2011, las 11H00. VISTOS: LEONARDO LIMITONE, Gerente y Representante Legal de la compañía FERRERO DEL ECUADOR S.A., interpone recurso de casación en contra de la sentencia dictada el 15 de julio de 2010, por la Quinta Sala Temporal del Tribunal Distrital de lo Fiscal No. 1, con sede en la ciudad de Quito, dentro del juicio de impugnación No. 25916 que sigue en contra del Servicio de Rentas Internas. Esta Sala acepta el recurso y el representante de la Administración Tributaria lo contesta el 7 de septiembre de 2010.

ABUSO DE CONFIANZA. Expediente 381, Registro Oficial Suplemento 178, 23 de Abril del 2010. No. 381-07 Recurso de casación en el juicio penal No. 594-06 seguido en contra de Hugo Fabián Reisancho Ruiz por el delito tipificado y reprimido en el Art. 563 del Código Penal, en perjuicio de Martha Parra Cadena. Al examinar la sentencia impugnada, en relación con el recurso interpuesto, la Sala encuentra, en ella: En el considerando cuarto, que mediante 1as actuaciones producidas en el juicio, se encuentra comprobada la existencia del delito y 1a responsabilidad del acusado Hugo Fabián Reisancho Ruiz, con: 1.- Los testimonios: del Cabo Primero de Policía, señor Nelson Leonel Chasi Velásquez, quien manifiesta haber elaborado el parte informativo a base de la delegación fiscal, conociendo por versiones de Marianela Parra, que ella a mediados de mayo del 2002 al acusado Hugo Fabián Reisancho Ruiz, le entregó $ 4.920.00 a través de una transferencia bancaria, por haberle aquél ofrecido enviar desde España ampolla de Pergonol para la esterilidad; que por la verificación realizada en el Banco de Pichincha de esta ciudad de Quito y en los correos electrónicos enviados desde España, se constató esa transferencia de dinero al acusado, a través del Banco Caixa Catalunya, efectuada según el e-mail por el envío de esas ampollas las que no fueron enviadas según argumentos evasivos del ahora acusado: por haber sido detenido en España y otros justificativos incoherentes con la realidad y enviadas desde España, cuando el movimiento migratorio

determinaba que el acusado Hugo Fabián Reisancho Ruiz, estaba en el país; que tampoco se devolvió el dinero.- Con la testimonial del Cabo de Policía Edwin Germán Martíratifica en el parte informativo realizado también sobre la base de la alegación fiscal, indicando que se receptaron las versiones de Silvio Párraga, Geovanny Párraga y Beatriz Cadena, los que señalaron que Martha Parra había depositado en una cuenta de España una cantidad aproximada a cinco mil dólares a nombre de Hugo Reisancho Ruiz, para que le envíe ampollas de Pergonol, pero que éste no cumplió con el envío y 2.- Con las copias certificadas, introducidas en el juicio, relativas a esta transferencia de dinero realizado por Marth Parra Cadena a nombre de Hugo Fabián Reisancho Ruiz, por el valor de $ 4.920,00 al Banco de Caixa Catalunya, Barcelona España, el 29 de mayo del 2002.

PROCESO 10-IP-99, ECUADOR, PLAGIO DE DATOS A LEXIS POR PRODINFO. Resolución del Tribunal Andino 10, Registro Oficial 302 de 20 de Octubre de 1999. TRIBUNAL DE JUSTICIA DE LA COMUNIDAD ANDINA INTERPRETACION PREJUDICIAL 10-IP-99 Interpretación prejudicial de los artículos 28 y 58 de la Decisión 351 de la Comisión del Acuerdo de Cartagena, solicitada por el Presidente del Tribunal de lo Contencioso Administrativo, Distrito de Quito, República del Ecuador, con motivo de la acción de daños y perjuicios interpuesta por LEXIS S.A. contra la empresa Productora e Información Compañía Ilimitada (PRODINFO), por supuesto plagio de la base de datos "MERLIN"; e interpretación de oficio de los artículos 3 y 4 párrafos 1ro. y 2do., de la Decisión 351. Proceso Interno No. 5316-LR, en el Tribunal solicitante. Quito, 11 de junio de 1999

CONVENIOS Y TRATADOS INTERNACIONALES.

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las tecnologías, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

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

El GATT, se transformó en lo que hoy conocemos como la Organización Mundial de Comercio (OMC), por consecuencia todos los acuerdos que se suscribieron en el marco del GATT, siguen estando vigentes. En el Art. 61 se establece que para los casos de falsificación dolosa de marcas de fábrica o de comercio o de piratería lesiva del derecho de autor a escala comercial se establecerán procedimientos y sanciones penales además de que "Los recursos disponibles comprenderán la pena de prisión y/o la imposición de sanciones pecuniarias suficientemente disuasorias"

*El convenio de Berna
*La convención sobre la Propiedad Intelectual de Estocolmo
*La Convención para la Protección y Producción de Fonogramas de 1971
*La Convención Relativa a la Distribución de Programas y Señales

En 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación. Las posibles implicaciones económicas de la delincuencia informática tienen carácter internacional e incluso transnacional, cuyo principal problema es la falta de una legislación unificada que, facilita la comisión de los delitos.

En 1986 la OCDE público un informe titulado Delitos de informática: análisis de la normativa jurídica, donde se reseñaban las normas legislativas vigentes y las propuestas de reforma en diversos Estados miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales.

En 1992 elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran erigir un marco de seguridad para los sistemas informáticos. En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, se dijo que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos. La ONU ha publicado una descripción de "Tipos de Delitos Informáticos", que se transcribe al final de ésta sección.

En 1992 La Asociación Internacional de Derecho Penal durante el coloquio celebrado en Wurzburgo en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Hay otros Convenios no ratificados aún por nuestro País, realizados por la Organización Mundial de la Propiedad Intelectual (OMPI), de la que nuestro país es parte integrante.

En Noviembre de 1997 se realizaron las II Jornadas Internacionales sobre el Delito Cibernético en Mérida España, donde se desarrollaron temas tales como:

Aplicaciones en la Administración de las Tecnologías Informáticas / cibernéticas.
Blanqueo de capitales, contrabando y narcotráfico.
Hacia una policía Europea en la persecución del delito Cibernético.
Internet: a la búsqueda de un entorno seguro.
Marco legal y Deontológico de la Informática.

En los últimos años se ha perfilado en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas

derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

Convenio sobre ciberdelincuencia

The Conventionon Cybercrime (CETS: n. 185) o **Convenio sobre cibercriminalidad de Budapest** o Convención sobre Delitos Informáticos o Convenio sobre ciberdelincuencia, es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la ciberdelincuencia.

Fue adoptado por el Comité de Ministros del Consejo de Europa en su sesión N. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

En abril de 2001 el Consejo Europeo publicó el proyecto destinado a armonizar las legislaciones en los estados miembros (47 miembros y 8 observadores al día de la fecha) y abierta a otros países como Australia, Japón, Canadá, Sudáfrica y los EE.UU. en noviembre de 2001.

Actualmente países como Argentina (que ha basado su ley de delitos informáticos en este convenio y Ecuador están analizando adherirse.

(Ver Anexo 35)

Por ende, este convenio es el único que se encarga de la seguridad de la informacióny trata los delitos contra la Confidencialidad, Integridad y Disponibilidad de los datos y los sistemas informáticos.

(Ver Anexo 36)

Los tipos de delitos informáticos reconocidos por **Naciones Unidas:**

Clasificación de delitos informáticos Naciones Unidas

Fraudes cometidos mediante manipulación de computadoras	Estos pueden suceder al interior de Instituciones Bancarias o cualquier empresa en su nómina, ya que la gente de sistemas puede accesar a tos tipo de registros y programas.
La manipulación de programas	Mediante el uso de programas auxiliares que permitan estar manejando los distintos programas que se tiene en los departamentos de cualquier organización.
Manipulación de los datos de salida	Cuando se alteran los datos que salieron como resultado de la ejecución de una operación establecida en un equipo de cómputo.
Fraude efectuado por manipulación informática	Accesando a los programas establecidos en un sistema de información, y manipulando para obtener una ganancia monetaria.
Falsificaciones Informáticas	Manipulando información arrojada por una operación de consulta en una base de datos.
Sabotaje informático	Cuando se establece una operación tanto de programas de cómputo, como un suministro de electricidad o cortar líneas telefónicas intencionalmente.
Virus	Programas contenidos en programas que afectan directamente a la máquina que se infecta y causa daños muy graves.
Gusanos	Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse.
Bomba lógica o cronológica	Su funcionamiento es muy simple, es una especie de virus que se programa para que explote en un día determinado causando daños a él equipo de cómputo afectado.
Piratas Informáticos	Hackers y Crackers dispuestos a conseguir todo lo que se les ofrezca en la red, tienen gran conocimiento de las técnicas de cómputo y pueden causar graves daños a las empresas.
Acceso no autorizado a Sistemas o Servicios	Penetrar indiscriminadamente en todo lugar sin tener acceso a ese sitio.

Reproducción no autorizada de programas informáticos de protección Legal	Es la copia indiscriminada de programas con licencias de uso para copias de una sola persona, se le conoce también como piratería.

FUENTE: http://www.monografias.com/trabajos96/delitos-informaticos-panama/delitos-informaticos-panama.shtml#ixzz3IsBBOsrS

El **Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos** señala que cuando el problema se eleva a la escena internacional, se magnifican los problemas y las insuficiencias, por cuanto, los delitos informáticos constituyen una forma de crimen trasnacional y su combate requiere de una eficaz cooperación concertada. Asimismo la ONU resume de la siguiente manera a los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

A) Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.
B) Ausencia de acuerdos globales en la definición de dichas conductas delictivas.
C) Falta de especialización en las policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.
D) Falta de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.
E) Carácter trasnacional de muchos delitos cometidos mediante el uso de las computadoras.
F) Ausencia de tratados de extradición, de acuerdos de ayuda mutua y de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

RED 24/7.

Un buen ejemplo de cooperación internacional es la **red de hoy 24/7** de investigadores cibernéticos. La red, creada entre las naciones del G-8 en 1997, ha crecido desde entonces a 55 países miembros, todos los cuales han dedicado los investigadores de delitos cibernéticos

que pueden responder a avance rápido los casos que se mueve a un momento previo aviso, a menudo con la capacidad de "congelación rápida" tráfico de correo electrónico y otros datos electrónicos almacenados, que pueden preservar la huella digital de otra manera fugaz de un ladrón.

Aquí está un ejemplo hipotético de cómo opera la red: Un delincuente cibernético hackea un banco en la ciudad de México. Investigadores mexicanos rastrear el equipo usado en el ataque a la ciudad de Nueva York, y en contacto rápidamente agentes del FBI, que descubren que el equipo de Nueva York está vinculado a un ordenador en Corea del Sur. Ellos agentes coreanos de alerta, que se enteran de que el ataque se originó en Bangkok. Agentes tailandeses hacen el arresto. Gracias a la red, el proceso de investigación puede tardar horas o días en lugar de semanas o meses.

Para Christopher Pintor, Subdirector de División cibernética,este nivel de cooperación oportuna es esencial, pero la cooperación tiene que ir de la mano con leyes consistentes para los delitos cibernéticos, sanciones uniformes deben ser adoptadas, o delincuentes cibernéticos experimentados simplemente basar sus operaciones en los países con las leyes más laxas cibernéticos."El resultado final es asegurarse de que hay consecuencias por las acciones criminales cibernéticos y consecuencias similares en todas partes",

Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia.

El 28 de mayo de 2014, en la sede de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB) en Madrid, los representantes de los gobiernos de Guatemala, Nicaragua, Portugal, Perú y Uruguay firmaron el **"Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia".** Los cuatro primeros

países mencionados, a los que se suma Argentina, suscribieron además la **"Recomendación de COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia"**, que busca tener impacto en las legislación nacional de los países miembros de la COMJIB.

En el evento participaron el Vicepresidente de la Corte Suprema de Justicia de Nicaragua, Marvin Aguilar; el Secretario de Estado de Justicia de Portugal, Antonio Costa Mouro; el Viceministro de Tecnología de Guatemala, Juan Carlos Argueta Medina; el Embajador de Perú en España, Francisco Eguiguren; el Ministro Consejero Embajada Argentina, Gustavo Fernández; y el Embajador de Uruguay en España, Francisco Bustillo Bonasso.

Al respecto de la importancia de los textos firmados, el Secretario General de la COMJIB, Fernando Ferraro, señala: "El Convenio aporta una amplia definición de Ciberdelincuencia que permite que los instrumentos de cooperación internacional se puedan aplicar para muchos tipos de delitos; y la Recomendación se presenta como un aporte adicional a los Estados para que puedan actualizar y modernizar sus legislaciones penales para combatir de forma efectiva la cibercriminalidad, y evitar que estos hechos delictivos queden en la impunidad, contribuyendo a la modernización de las legislaciones penales internas de los países."

Estos son los primeros instrumentos iberoamericanos que hacen frente al problema de la cibercriminalidad.

Países como Costa Rica, El Salvador y México, anuncian que en el futuro próximo se estarán adhiriendo a ambos instrumentos.

En calidad de observadores, representantes de las embajadas de Costa Rica, Ecuador, El Salvador, Venezuela, Brasil y Honduras, Procuraduría General de México, de la Secretaría General Iberoamericana (SEGIB), así como de la Policía Nacional de España, la Agencia Española de Cooperación para el Desarrollo (AECID), Microsoft, y el Ministerio de Asuntos Exteriores y Cooperación de España.

12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Salvador (Brasil), 12 a 19 de abril de 2010.

(Ver Anexo 37)

Una forma de abordar la dimensión transnacional del delito cibernético y mejorar la cooperación internacional es desarrollar y normalizar la legislación pertinente. En los últimos años se han adoptado varias iniciativas regionales.

En 2002, el Commonwealth elaboró una ley modelo sobre el delito cibernéticoe informático con la finalidad de mejorar la legislación para combatir la ciber delincuencia en los Estados miembros del Commonwealth e intensificar la cooperación internacional. Sin esas mejoras, se necesitarían por lo menos1.272 tratados bilaterales entre los Estados del Commonwealth para que los países pudieran cooperar entre sí en esta materia. La ley modelo contiene disposiciones sobre el derecho penal sustantivo, el derecho procesal y la cooperación internacional. Debido al enfoque regional de la ley modelo, el efecto en la armonización se limita a los Estados miembros del Commonwealth.

La Unión Europea también ha hecho esfuerzos por armonizar la legislación sobre el delito cibernético entre sus 27 Estados miembros, por ejemplo mediante lo siguiente: la directiva 2000/31/EC del Parlamento Europeo y el Consejo sobre ciertos aspectos jurídicos de los servicios en la sociedad de la información, en particular el comercio electrónico, en el mercado interno; la decisión marco 2000/413/JHA del Consejo de la Unión Europea sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo; la decisión marco 2004/68/JHA del Consejo de la Unión Europea sobre la lucha contra la explotación sexual de los niños y la pornografía infantil; la decisión marco 2005/222/JHA del Consejo de la Unión Europea sobre los ataques contra los sistemas de información23; la directiva 2006/24/EC del Parlamento Europeo y del Consejo de la Unión Europea sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modificó la directiva 2002/58/EC; y la decisión marco 2008/919/JHA del Consejo de la

Unión Europea por la que se modificó la decisión marco 2002/475/JHA sobre la lucha contra el terrorismo. A diferencia de lo que ocurre en la mayoría de los otros enfoques regionales, la aplicación de los instrumentos adoptados por la Unión Europea es obligatoria para todos los Estados miembros. Si bien los instrumentos son efectivos, el principal obstáculo a la armonización dentro de la Unión Europea era, al menos hasta comienzos de 2010, el limitado poder de la legislación en la esfera del derecho penal. La diversidad de enfoques obedecía a que la capacidad de la Unión Europea de armonizar el derecho penal nacional se limitaba a algunas esferas especiales 25. El Tratado de Lisboa, por el que se modificó el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, ha cambiado la situación y confiere a la Unión Europea mayores atribuciones para armonizar la legislación sobre el delito informático en el futuro; ello, sin embargo, se limita a los 27 Estados miembros.

El Consejo de Europa ha elaborado tres instrumentos principales para armonizar la legislación sobre el delito cibernético. El más conocido es el Convenio sobre la Ciberdelincuencia, redactado entre 1997 y 2001. Este Convenio contiene disposiciones sobre el derecho penal sustantivo, el derecho procesal y la cooperación internacional. Al mes de diciembre de 2009 había sido firmado por 46 Estados y ratificado por 26. Puesto que, durante la negociación del Convenio, no fue posible llegar a un acuerdo sobre la penalización del racismo y la distribución de material xenófobo, en 2003 se estableció el Protocolo Adicional del Convenio sobre la Ciberdelincuencia, relativo a la penalización de los actos de naturaleza racista y xenófoba cometidos por medio de sistemas informáticos. Al mes de diciembre de 2009, 34 Estados 27 habían firmado el Protocolo Adicional, y 15 de ellos 28 lo habían ratificado. En 2007 se abrió a la firma el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual. Este Convenio contiene disposiciones específicas que penalizan el intercambio de pornografía infantil así como la obtención, a sabiendas, de acceso a pornografía infantil a través de las tecnologías de la información y las comunicaciones (párrafo 1 f) del artículo 20). Al mes de diciembre de 2009 habían firmado este Convenio 38 Estados 30, y tres de ellos 31 lo habían ratificado.

Además, cabe mencionar el proyecto de convención internacional para mejorarla protección contra el delito cibernético y el terrorismo, elaborado como medida de seguimiento de una conferencia acogida por la Universidad de Stanford (Estados Unidos) en 1999, y el proyecto de manual de la UIT sobre la legislación contra el delito cibernético, elaborado por representantes de la American Bar Association y otros expertos.

El XIII Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, se celebrará en QATAR en el año 2015.

(Ver Anexo 38)

Commonwealth Cybercrime Initiative.
Iniciativa de la Mancomunidad para la Ciberdelincuencia.

La Ley Modelo de la Commonwealth sobre Delitos Informáticos contiene disposiciones relativas al derecho penal y procesal y la cooperación internacional. Sin embargo,el impacto se limita a los países de la Commonwealth.

La iniciativa ayuda a desarrollar la "Commonwealth" mancomunidad de los países miembros, a fortalecer sus capacidades institucionales, recursos humanos y técnicos con respecto a la política, la legislación, la investigación y la aplicación de la ley con el objetivo de hacer de sus jurisdicciones lugares más seguros al negar refugio a los delincuentes cibernéticos, y la asistencia a los Estados Miembros sean más eficaces en los esfuerzos mundiales para combatir el delito cibernético.

La Iniciativa de la ciberdelincuencia promueve el intercambio de conocimientos y mejores prácticas de los recursos existentes, centrándose en la Ley Modelo de la Commonwealth en el equipo y los delitos informáticos (Ley Modelo) y también la elaboración de otros existentes tratados, juegos de herramientas, recursos e instrumentos para que los países de la dirección las lagunas legislativas para que puedan hacer frente a los incidentes de ciberdelincuencia.*Fuente: http://www.commonwealthigf.org/

Dirigiéndose a los delitos informáticos en Internet es un requisito clave para asegurar que Internet siga siendo un espacio confiable para la interacción y el crecimiento en la economía digital. Un enfoque de múltiples partes interesadas es clave para abordar con éxito este reto. Por ejemplo, La Iniciativa de Ciberdelincuencia de la Commonwealth (ICC) es un esfuerzo de colaboración de las organizaciones internacionales, los gobiernos y el sector privado para hacer frente a los delitos cibernéticos. Desarrollado en colaboración con la Fundación para el Desarrollo de las TIC COMNET, Organización Telecom Commonwealth, Consejo de Europa, Gobierno del Reino Unido, y la Unión Internacional de Telecomunicaciones CCI ayuda a los Estados miembros de la Comunidad en el desarrollo de capacidades para combatir la ciberdelincuencia.

CCI ha adoptado una fórmula única y sostenible para la operación:

Al recibir una solicitud formal por parte de un estado miembro de la Commonwealth, CCI envía un equipo de evaluación de las necesidades para llevar a cabo una evaluación en el país. Un equipo típico se compone de expertos en la materia en los sistemas de justicia penal y de seguridad de la información, que evalúan la capacidad legal, técnica, institucional y humana presente en el Estado requirente.

El equipo de evaluación de las necesidades se reúne con una amplia gama de organismos en el país, los actores del sector privado, y los operadores de infraestructura y produce un informe temático que identifica las áreas donde se necesita la creación de capacidades.
El Estado solicitante revisa el informe temático y presenta una nueva carta de solicitud a la Secretaría del Commonwealth para ayudar a "llenar los vacíos" (asistencia en el país de las áreas donde se necesita la creación de capacidades).

Miembros de CCI cooperan para planificar y ejecutar en la construcción de capacidad. En esta segunda fase del programa, miembros de la iniciativa que se han ofrecido recursos trabajarán en el país para aumentar las capacidades a través de una gama de áreas u operaciones de cibercrimen afectadas, incluyendo la estrategia nacional

y la política, el marco legislativo, la capacidad del sistema de justicia penal (incluida la formación de la ley la aplicación, el poder judicial, y el enjuiciamiento), la infraestructura de las TIC, el establecimiento de centros de excelencia y los equipos de respuesta a emergencias informáticas, campañas de sensibilización del público, y la facilitación de alianzas estratégicas con el sector privado.

Más de 30 organizaciones participan en el CCI para coordinar los recursos internacionales disponibles, para extender la asistencia a los Estados Miembros, y para superar las restricciones de mandatos y limitaciones de financiación estados miembros puedan encontrar. Hasta la fecha, CCI ha llevado a cabo cinco evaluaciones de las necesidades en las Regiones del Caribe y de África. Cinco gobiernos han aprobado los informes temáticos.

Programas de "Fase 2" son excelentes ejemplos de colaboración de múltiples partes interesadas y la contribución. Para el programa de la Fase 2 del trabajo en curso en el África occidental, por ejemplo, la Agencia de Crimen Nacional del Reino Unido está coordinando la entrega por miembros de la Iniciativa para el fortalecimiento de la capacidad del sistema de justicia penal, un programa de sensibilización del público, la preparación de la infraestructura de las TIC para apoyar las investigaciones de delitos informáticos, y legislativo marco necesita.

Las consultas están actualmente en curso en otros cuatro países de la Commonwealth. Se espera que éstas se pongan en marcha en el primer trimestre de 2014. *Fuente: Dave Piscitello, ICANN y Lara Pace, Secretaría del Commonwealth. http://www.internetac.org/?p=1787

Algunas iniciativas de los miembros: Ética Cibernética Chipre; Centro para la Seguridad de Internet Canberra; Coalición de los niños de las Caridades en Seguridad en Internet; Fundación COMNET para las TIC; Desarrollo Commonwealth Business Council; Mancomunidad de Abogados; asociación Commonwealth Parlamentaria; Asociación Mancomunidad de Telecomunicaciones; Organización Consejo de Europa; Fundación Diplo; Alianza Europea de ONG para niños de la seguridad en línea; ICANN; Seguridad Cibernética Internacional;

Alianza de Protección de la unión Internacional de Telecomunicaciones; Oficina de las Naciones Unidas para la Droga y el Crimen.

Documento de contenido de la iniciativa, se lo puede visualizar en idioma ingles en esta dirección:
http://issuu.com/comnetfoundation/docs/commonwealth_cybercrime_initiative__version_11.1?e=5045719/3081230

Proyecto de Stanford

El Centro Internacional de la Seguridad y la Cooperación (CISAC) de Stanford publicó el Proyecto de Convención Internacional para Mejorar la Seguridad de la Delincuencia en el Ciberespacio y el Terrorismo,conocido como Proyecto de Stanford, con el cual se busca un convenio multilateral entre las naciones en materia de delito informático y terrorismo. Es de destacarlos artículos:

Artículo 6. Asistencia Legal Mutua Artículo 7. Extradición Artículo 12. Agencia de Protección de la Infraestructura de Información (AIIP) Artículo 14. Informes anuales de los Estados Partes.

La AIIP como organismo internacional integrado por todos los Estados Partes en calidad de Miembros,actuaría como un eje central para asegurar la ejecución de los objetivos de tal Convenio.

División de Capacidad Institucional del Estado (ICS)
Departamento de Instituciones para el Desarrollo (IFD)
Banco Interamericano de Desarrollo (BID)

El informe "Tendencias en Seguridad Cibernética en América Latina y el Caribe" (ALC) publicado en junio de 2014 indica que a pesar de los avances logrados en la región en la lucha contra el cibercrimen, un análisis de la situación de la región en el año 2013 deja un claro mensaje acerca de la necesidad de que todos los involucrados redoblen sus esfuerzos en lo que concierne a reformar leyes y políticas, desarrollar capacidad técnica, generar mayor conciencia, compartir información y cooperar con otras partes interesadas. La realidades que muchos de

estos mensajes aplican a la mayor parte las naciones de nuestro planeta de acuerdo con el "Internet Security Threat Report 2014".

A la luz de este movimiento mundial para crear conciencia sobre la importancia de la defensa cibernética proactiva, de acuerdo con su compromiso de salvaguardar los intereses de la región de ALC y apoyar a los gobiernos para servir mejor a sus ciudadanos, el Departamento de Instituciones para el Desarrollo (IFD)a través de la División de Capacidad Institucional del Estado (ICS) ha puesto en marcha una Cooperación Técnica Regional con el objetivo último de asistir a los países beneficiarios en el diseño de estrategias de seguridad cibernética nacional de acuerdo con los estándares internacionales más reconocidos fortaleciendo así la seguridad ciudadana.

Para lograr este objetivo, el BID llevará a cabo diferentes actividades de generación de conocimiento, asistencia técnica, capacitación e intercambio de experiencias que permitan a sus países miembros comprender mejor los desafíos y las amenazas que emanan del uso de las nuevas tecnologías y aprovechar el conocimiento de otros países para enfrentarlas con garantías de éxito; en la sociedad del conocimiento, el progreso socioeconómico de la región y la seguridad de sus ciudadanos se construyen sobre un entorno cibernético seguro.

Comité Interamericano contra el Terrorismo (CICTE)
Organización de los Estados Americanos (OEA)

En el 2004, la Asamblea General de la OEA aprobó por unanimidad la Estrategia Integral de Seguridad Cibernética Interamericana.

Desde entonces, las amenazas cibernéticas han crecido descomunalmente,adaptándose a los intentos de los gobiernos para hacerles frente. Esto, a su vez, ha forzado que la OEA prevea y anticipe las amenazas nuevas a los Estados Miembros. El diseño de programas se ejecuta de acuerdo a las necesidades y enfoques de preferencia de los Estados Miembros de la OEA, los cuales varían en función de sus realidades políticas, económicas y sociales.

Los primeros esfuerzos se centraron en crear y generar una cultura de seguridad cibernética entre los funcionarios de los Estados Miembros

de la OEA. Simultáneamente, la OEA se embarcó en un programa de establecer Equipos Nacionales de Respuesta a Incidentes Cibernéticos (CSIRT por sus siglas en ingles) en las Américas. Desde el 2006, el número de CSIRTs nacionales en las Américas ha aumentado de 5 a 18. Además de trabajar en el desarrollo de capacidades técnicas, la OEA ha abordado el desarrollo de estrategias y políticas de seguridades cibernéticas sostenibles y pragmáticas en los Estados Miembros, ayudando a Colombia,Panamá, y Trinidad y Tobago a adoptar tales políticas.

El enfoque original del Programa de Seguridad Cibernética del CICTE ha informado el desarrollo de varias líneas principales de acción, incluyendo la prestación de asistencia en: la respuesta a incidentes técnicos;estrategias nacionales de seguridad cibernética y el desarrollo de CSIRTs; ejercicios de gestión de crisis cibernéticas; talleres de mejores prácticas; cursos y talleres sobre seguridad cibernética y la protección de infraestructuras críticas; concienciación del público; diplomacia cibernética; y alianzas estratégicas con el sector privado y la sociedad civil.

Otros documentos y limitaciones.

Existen diversos documentos que reflejan el esfuerzo de diferentes países y organizaciones tal como el Cybercrime Legislation Toolkit de la Unión Internacional de Telecomunicaciones (ITU) que busca dar un marco de referencia para los Estados con el fin crear una legislación eficaz que permita enfrentar estos delitos.

La Ley Modelo de la Commonwealth sobre Delitos Informáticos, que al igual que el Convenio de Budapest,contiene disposiciones sobre material penal, procesal y de cooperativa internacional para sus actuales 54 países miembros.

Una de las principales limitaciones que presentan estos acuerdos es la reducida cantidad de países miembros con los que cuenta, a abril de 2010 la Convención sobre el Delito Cibernético del Consejo de Europa tenía elmás amplio alcance: ha sido firmada por 46 Estados y

ratificada por 26, son los países desarrollados quienes cuentan con la experiencia y los recursos que demanda la implementación de este tipo de acuerdos.

Un vacío legal en países sin las competencias necesarias para la persecución ofrece una oportunidad para los delincuentes quienes pueden causar estragos muchas veces con solo contar con un ordenador y una conexión a internet sin importar mucho donde se encuentre al momento de realizar un ataque.

I.- MEDIOS DE PRUEBA PENAL DIGITAL.

Es importante manifestar que el Ecuador desde su conformación como Estado, en relación a norma sustantiva penal, se han promulgado cinco Códigos Penales, a saber: 1837; 1872; 1889, 1906, y 1938. En el año de 1971 se realizó una codificación, luego en el año 2010 se realizó una nueva codificación. De la primera a la segunda se agregaron cuarenta y seis reformas penales. Y existían alrededor de doscientas normas no penales que tipifican infracciones, por lo que el contenido del régimen penal se volvió obsoleto.

El nuevo Código de Integración Penal, COIP, en vigencia desde el 10 de agosto del 2014, como su nombre lo dice integra en el libro II, el código de procedimiento penal que en el año 2000 introdujo un cambio fundamental en relación al código procesal de 1983, pasamos del sistema inquisitivo, al actual sistema acusatorio oral, sin embargo esta ley procesal para que se adapte a la constitución anterior a la del 2008, se modificó en catorce oportunidades, ahora se lo ha integrado sin mayor cambio en su contenido.

De igual forma se integran algunas leyes relativas a rehabilitación social, cárceles, como el Código de Ejecución de Penas, que data de 1982, ley de tránsito (permanentemente reformada), aduanas, normas tributarias,etc.,leyes con contenidos sustantivos y procesales, con el objetivo de que estas normas positivas estén acordes al

sistema sustantivo adversarial, humanitario moderno, y adjetivo de procedimiento del sistema oral acusatorio.

Los autores del COIP se han basado en el mandato constitucional del 2008, con el objetivo de garantizar la dignidad del ser humano, adecuando formal y materialmente esta norma, a la constitución, así como a los tratados internacionales y principios de derechos humanos.

La explicación se fundamenta en que la Constitución al declarar al Estado como "constitucional de derechos y justicia", define un nuevo orden de funcionamiento jurídico, político y administrativo.

Esta fuerza normativa es directa, los principios y normas en el sentido de constitucionalidad, legitiman al Código Orgánico Integral Penal, ya que las normas no requieren de la "intermediación" de la Ley, para que sean aplicables directamente por la administración de justicia, es decir por los jueces.

Lo anotado lo establece la Constitución en el TÍTULO III. GARANTÍAS CONSTITUCIONALES. Capítulo primero. Garantías normativas. Art. 84.- "La Asamblea Nacional y todo órgano con potestad normativa tendrá la obligación de adecuar, formal y materialmente, las leyes y demás normas jurídicas a los derechos previstos en la Constitución y los tratados internacionales, y los que sean necesarios para garantizar la dignidad del ser humano o de las comunidades, pueblos y nacionalidades. En ningún caso, la reforma de la Constitución, las leyes, otras normas jurídicas ni los actos del poder público atentarán contra los derechos que reconoce la Constitución".

En el título IX. Supremacía de la Constitución. Capítulo primero. Principios. Art. 424.- "La Constitución es la norma suprema y prevalece sobre cualquier otra del ordenamiento jurídico. Las normas y los actos del poder público deberán mantener conformidad con las disposiciones constitucionales; en caso contrario carecerán de eficacia jurídica.

La Constitución y los tratados internacionales de derechos humanos ratificados por el Estado que reconozcan derechos más favorables a los contenidos en la Constitución, prevalecerán sobre cualquier otra norma jurídica o acto del poder público".

Y, como conclusión, el artículo 76 de constitución ordena que las penas estén acorde con el "principio de proporcionalidad", es decir debe existir cierta relación coherente entre el grado de vulneración de un derecho y la gravedad de la pena. Por lo que es importante determinar la correspondencia constitucional de los bienes jurídicos protegidos y las garantías de quienes se someten a un proceso penal en calidad de víctimas o procesados para que estén adecuadamente regulados y protegidos.

En el sistema adversarial - acusatorio, instaurado en el COIP, el derecho penal como tal, tiene una doble función frente a los derechos, por un lado, protege derechos, y por otro, los restringe. Es decir cuando el Art. 76 ordena que las penas estén acorde con el principio de proporcionalidad, significa que debe existir relación entre el grado de vulneración del derecho y la gravedad de la pena, y, el Art. 78 dispone que las victimas de infracciones penales gozarán de protección especial, se les garantizará su no revictimización, particularmente en la obtención y valoración de las pruebas, y se les protegerá de cualquier amenaza u otras formas de intimidación.

La finalidad del código es instaurar el debido proceso, consagrado en la constitución y en el "Art. 1, del COIP, "...con estricta observancia del debido proceso.....", aplicando los principios que emanan de la Constitución, los principios de probidad, celeridad y sobre todo el de dignidad humana, para lograr una justicia ágil y oportuna.

La intervención penal está legitimada siempre y cuando sea necesaria para la protección de las personas. Constituye el último recurso, cuando no son suficientes los mecanismos extrapenales. Art3.COIP. *Jurisprudencia: Gaceta Judicial, JUICIO DE COMPETENCIA, 21-jun-1973; Gaceta Judicial, COMPETENCIA EN MATERIA PENAL, 21-mar-1984.Gaceta Judicial, CRITERIO DE EQUIDAD, 29-ago-1996.

Los principios procesales, es decir, el derecho al debido proceso penal, sin perjuicio de otros establecidos en la Constitución de la República, en instrumentos internacionales ratificados por el Estado u otras normas jurídicas, se regirán por los siguientes (Art.4.COIP)*:

1. **Legalidad:**	no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho. Este principio rige incluso cuando la ley penal se remita a otras normas o disposiciones legales para integrarla.
2. **Favorabilidad:**	en caso de conflicto entre dos normas de la misma materia, que contemplensanciones diferentes para un mismo hecho, se aplicará la menos rigurosa aun cuando supromulgación sea posterior a la infracción.
3. **Duda a favor del reo:**	la o el juzgador, para dictar sentencia condenatoria, debe tener elconvencimiento de la culpabilidad penal de la persona procesada, más allá de toda duda razonable.
4. **Inocencia:**	toda persona mantiene su estatus jurídico de inocencia y debe ser tratada como tal,mientras no se ejecutorie una sentencia que determine lo contrario.
5. **Igualdad:**	es obligación de las y los servidores judiciales hacer efectiva la igualdad de losintervinientes en el desarrollo de la actuación procesal y proteger especialmente a aquellas personas que, por su condición económica, física o mental, se encuentren en circunstancias de vulnerabilidad.
6. **Impugnación procesal:**	toda persona tiene derecho a recurrir del fallo, resolución o auto definitivo en todo proceso que se decida sobre sus derechos, de conformidad con lo establecido en la Constitución de la República, los instrumentos internacionales de derechos humanos y este Código.
7. **Prohibición de empeorar la situación del procesado:**	al resolver la impugnación de una sanción, no se podrá empeorar la situación de la persona procesada cuando esta es la única recurrente.
8. **Prohibición de autoincriminación:**	ninguna persona podrá ser obligada a declarar contra sí misma en asuntos que puedan ocasionar su responsabilidad penal.

9. **Prohibición de doble juzgamiento:**	ninguna persona podrá ser juzgada ni penada más de una vez por los mismos hechos. Los casos resueltos por la jurisdicción indígena son considerados para este efecto. La aplicación de sanciones administrativas o civiles derivadas de los mismos hechos quesean objeto de juzgamiento y sanción penal no constituye vulneración a este principio.
10. **Intimidad:**	toda persona tiene derecho a su intimidad personal y familiar. No podrán hacerse registros, allanamientos, incautaciones en su domicilio, residencia o lugar de trabajo, sino en virtud de orden de la o el juzgador competente, con arreglo a las formalidades y motivos previamente definidos, salvo los casos de excepción previstos en este Código.
11. **Oralidad:**	el proceso se desarrollará mediante el sistema oral y las decisiones se tomarán en audiencia; se utilizarán los medios técnicos disponibles para dejar constancia y registrar las actuaciones procesales; y, los sujetos procesales recurrirán a medios escritos en los casos previstos en este Código.
12. **Concentración:**	la o el juzgador concentrará y realizará la mayor cantidad de actos procesales en una sola audiencia; cada tema en discusión se resolverá de manera exclusiva con la información producida en la audiencia destinada para el efecto.
13. **Contradicción:**	los sujetos procesales deben presentar, en forma verbal las razones o argumentos de los que se crean asistidos; replicar los argumentos de las otras partes procesales;presentar pruebas; y, contradecir las que se presenten en su contra.
14. **Dirección judicial del proceso:**	la o el juzgador, de conformidad con la ley, ejercerá la direcciónde l proceso, controlará las actividades de las partes procesales y evitará dilaciones innecesarias. En función de este principio, la o el juzgador podrá interrumpir a las partes para solicitaraclaraciones, encauzar el debate y realizar las demás acciones correctivas.
15. **Impulso procesal:**	corresponde a las partes procesales el impulso del proceso, conforme con elsistema dispositivo.

16. **Publicidad:**	todo proceso penal es público salvo los casos de excepción previstos en este Código.
17. **Inmediación:**	la o el juzgador celebrará las audiencias en conjunto con los sujetos procesales y deberá estar presente con las partes para la evacuación de los medios de prueba y demás actosprocesales que estructuran de manera fundamental el proceso penal.
18. **Motivación:**	la o el juzgador fundamentará sus decisiones, en particular, se pronunciará sobre losargumentos y razones relevantes expuestos por los sujetos procesales durante el proceso.
19. **Imparcialidad:**	la o el juzgador, en todos los procesos a su cargo, se orientará por el imperativode administrar justicia de conformidad con la Constitución de la República, los instrumentosinternacionales de derechos humanos y este Código, respetando la igualdad ante la Ley.
20. **Privacidad y confidencialidad:**	las víctimas de delitos contra la integridad sexual, así como todaniña, niño o adolescente que participe en un proceso penal, tienen derecho a que se respete suintimidad y la de su familia. Se prohíbe divulgar fotografías o cualquier otro dato que posibilite su identificación en actuacionesjudiciales, policiales o administrativas y referirse a documentación, nombres, sobrenombres, filiación,parentesco, residencia o antecedentes penales.
21. **Objetividad:**	en el ejercicio de su función, la o el fiscal adecuará sus actos a un criterio objetivo, ala correcta aplicación de la ley y al respeto a los derechos de las personas. Investigará no solo loshechos y circunstancias que funden o agraven la responsabilidad de la persona procesada, sinotambién los que la eximan, atenúen o extingan.
***Jurisprudencia:** Gaceta Judicial, TIPIFICACIÓN DE INFRACCIONES, 30-may-1891; Gaceta Judicial, TIPIFICACIÓN DE DELITOS, 07-jul-1911;Gaceta Judicial, TIPIFICACIÓN DE INFRACCIONES PENALES, 25-feb-1924; Gaceta Judicial, JUSTICIA POR PROPIA MANO, 19-oct-1950; Gaceta Judicial, PRINCIPIO REFORMATIO IN PEJUS, 17-dic-1980; Gaceta Judicial, DOCTRINA REFORMATIO IN PEJUS, 15-sep-1981;Gaceta Judicial, REFORMATIO IN PEJUS, 26-ene-1982; Gaceta Judicial, REFORMATIO IN PEJUS, 09-mar-1982; Gaceta Judicial, PRINCIPIO REFORMATIO IN PEJUS, 07-oct-1982;Gaceta Judicial, PRINCIPIO REFORMATIO IN PEJUS, 02-jun-1988;Gaceta Judicial, LEY APLICABLE A LA SANCIÓN DEL DELITO, 17-jun-1993.Gaceta Judicial, LA TIPIFICACIÓN DE UN HECHO LO HACE EL LEGISLADOR, NO EL JUEZ, 22-ago-1994.	

Elaboración: Juan José Páez Rivadeneira

Los medios de prueba están garantizados en la constitución del Ecuador, la del año 2008, en el capítulo tercero, sobre Garantías jurisdiccionales, Sección primera, Disposiciones comunes, articulo ochenta y seis, se dispone que las garantías jurisdiccionales se regirán, en general, por las siguientes disposiciones:

1. Cualquier persona, grupo de personas, comunidad, pueblo o nacionalidad podrá proponer las acciones previstas en la Constitución.	
2. Será competente la jueza o juez del lugar en el que se origina el acto o la omisión o donde se producen sus efectos, y serán aplicables las siguientes normas de procedimiento:	a) El procedimiento será sencillo, rápido y eficaz. Será oral* en todas sus fases e instancias. b) Serán hábiles todos los días y horas. c) Podrán ser propuestas oralmente o por escrito, sin formalidades, y sin necesidad de citar la norma infringida. No será indispensable el patrocinio de un abogado para proponer la acción. d) Las notificaciones se efectuarán por los medios más eficaces que estén al alcance del juzgador, del legitimado activo y del órgano responsable del acto u omisión. e) No serán aplicables las normas procesales que tiendan a retardar su ágil despacho.
***ORAL**: Juicio oral. Conjunto de actos procesales previstos en la ley, que tienen lugar en el último período del proceso de conocimiento, en torno a la producción y práctica de los medios de prueba, con el objetivo de permitir a las partes la confrontación y refutación de sus respectivas alegaciones y pretensiones, y de que el órgano jurisdiccional alcance la certeza plena y fundamentada acerca del objeto del proceso, y consecuentemente sancione al acusado, o en su defecto, declare su absolución por imperio	*Fuente: http://www.ecured.cu/index.php/Juicio_oral

del principio in dubio pro reo o por concurrir alguna circunstancia legal que oriente esta decisión*.	
3. Presentada la acción,	la jueza o juez convocará: inmediatamente a una audiencia pública, y en cualquier momento del proceso podrá ordenar la práctica de pruebas y designar comisiones para recabarlas. Se presumirán ciertos los fundamentos alegados por la persona accionante cuando la entidad pública requerida no demuestre lo contrario o no suministre información. La jueza o juez resolverá la causa mediante sentencia, y en caso de constatarse la vulneración de derechos, deberá declararla, ordenar la reparación integral, material e inmaterial, y especificar e individualizar las obligaciones, positivas y negativas, a cargo del destinatario de la decisión judicial, y las circunstancias en que deban cumplirse. Las sentencias de primera instancia podrán ser apeladas ante la corte provincial. Los procesos judiciales sólo finalizarán con la ejecución integral de la sentencia o resolución.
4. Si la sentencia o resolución no se cumple por parte de servidoras o servidores públicos, la jueza o juez ordenará su destitución del cargo o empleo, sin perjuicio de la responsabilidad civil o penal a que haya lugar. Cuando sea un particular quien incumpla la sentencia o resolución, se hará efectiva la responsabilidad determinada en la ley.	
5. Todas las sentencias ejecutoriadas serán remitidas a la Corte Constitucional, para el desarrollo de su jurisprudencia.	

Ya anotamos en capítulos anteriores que se debe certificar que la evidencia que sirve de prueba no se ha cambiado desde el momento en que es identificada, levantada, rotulada, numerada y descrita por el perito en la inspección ocular técnica de la escena del delito, hasta que es utilizada en la audiencia del juicio. Por lo que entremos a tratar el tema de la Prueba.

El COIP establece laÇ "finalidad" de la prueba, en el TÍTULO IV. PRUEBA. CAPÍTULO PRIMERO. DISPOSICIONES

GENERALES. Art. 453.- "Finalidad.- La prueba tiene por finalidad llevar a la o al juzgador al convencimiento de los hechos y circunstancias materia de la infracción y la responsabilidad de la persona procesada".

La prueba es el resultado de la producción de la verdad, es demostrar la verdad real o material, es el convencimiento del juez, sobre el resultado de la investigación, ya que el principal propósito del proceso penal es la búsqueda de la verdad material para cuya consecución el COIP establece los medios de prueba, basados en la valoración de la prueba y elaboración del veredicto.

Por eso el anuncio y práctica de la prueba se rige por los siguientes principios:

Art. 454.- Principios: *Jurisprudencia: Gaceta Judicial, PRESUNCIONES DE RESPONSABILIDAD PENAL, 27-ene-1914

1. Oportunidad.-	Es anunciada en la etapa de evaluación y preparatoria de juicio y se practica únicamente en la audiencia de juicio. Los elementos de convicción deben ser presentados en la etapa de evaluación y preparatoria de juicio. Las investigaciones y pericias practicadas durante la investigación alcanzarán el valor de prueba, una vez que sean presentadas, incorporadas y valoradas en la audiencia oral de juicio. Sin embargo, en los casos excepcionales previstos en este Código, podrá ser prueba el testimonio producido de forma anticipada.
2. Inmediación.-	Las o los juzgadores y las partes procesales deberán estar presentes en la práctica de la prueba.
3. Contradicción.-	Las partes tienen derecho a conocer oportunamente y controvertir las pruebas, tanto las que son producidas en la audiencia de juicio como las testimoniales que se practiquen en forma anticipada.

4. Libertad probatoria.-	Todos los hechos y circunstancias pertinentes al caso, se podrán probar por cualquier medio que no sea contrario a la Constitución, los instrumentos internacionales de derechos humanos, los instrumentos internacionales ratificados por el Estado y demás normas jurídicas.
5. Pertinencia.-	Las pruebas deberán referirse, directa o indirectamente a los hechos o circunstancias relativos a la comisión de la infracción y sus consecuencias, así como a la responsabilidad penal dela persona procesada.
6. Exclusión.-	Toda prueba o elemento de convicción obtenidos con violación a los derechos establecidos en la Constitución, en los instrumentos internacionales de derechos humanos o en la Ley, carecerán de eficacia probatoria, por lo que deberán excluirse de la actuación procesal. Se inadmitirán aquellos medios de prueba que se refieran a las conversaciones que haya tenido la o el fiscal con la persona procesada o su defensa en desarrollo de manifestaciones preacordadas. Los partes informativos, noticias del delito, versiones de los testigos, informes periciales y cualquier otra declaración previa, se podrán utilizar en el juicio con la única finalidad de recordar y destacar contradicciones, siempre bajo la prevención de que no sustituyan al testimonio. En ningún caso serán admitidos como prueba.
7. Principio de igualdad de oportunidades para la prueba.-	Se deberá garantizar la efectiva igualdad material y formal de los intervinientes en el desarrollo de la actuación procesal.

Elaboración: Juan José Páez Rivadeneira.

En México de manera general siguen los lineamientos del Código Modelo de la Comisión Nacional de Tribunales Superiores de Justicia A.C. (CONATRIB), en donde se presentan las etapas y funcionamiento general de dicho sistema, de la siguiente manera:

1.- Etapa Inicial o de Investigación
2.- Etapa Intermedia o de Preparación a juicio oral
3.- Etapa de Juicio Oral
4.- Etapa de Ejecución de Sentencia.

Casos en que se penaliza la prueba.

En el COIP, se establece sanción o no admisibilidad de la Prueba en tres casos: Calumnia; Fraude procesal; y, Alteración de evidencia y elementos de prueba.

"No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo".Art. 182.

"Fraude procesal.- La persona que con el fin de inducir a engaño a la o al juez, en el de curso de un procedimiento civil o administrativo, antes de un procedimiento penal o durante él, oculte los instrumentos o pruebas, cambie el estado de las cosas, lugares o personas, será sancionada con pena privativa de libertad de uno a tres años.

Con igual pena será sancionada quien conociendo la conducta delictuosa de una o varias personas, les suministren alojamiento o escondite, o les proporcionen los medios para que se aprovechen de los efectos del delito cometido, o les favorezcan ocultando los instrumentos o pruebas materiales de la infracción, o inutilizando las señales o huellas del delito, para evitar su represión y los que, estando obligados por razón de su profesión, empleo, arte u oficio, a practicar el examen de las señales o huellas del delito o el esclarecimiento del acto punible, oculten o alteren la verdad, con propósito de favorecerlos". Art. 272.

"Alteración de evidencias y elementos de prueba.- La persona o la o el servidor público, que altere o destruya vestigios, evidencias materiales

u otros elementos de prueba para la investigación de una infracción, será sancionado con pena privativa de libertad de uno a tres años". Art. 292.

CAUSALIDAD.

En sentido amplio, es la relación existente entre el resultado y la acción, que permite afirmar que aquel ha sido producido por esta. En sentido más restringido solo se puede hablar de relación de causalidad para referirse a uno de los grupos de teorías que han tratado de explicar aquella relación, las llamadas teorías de la causalidad: teoría de la equivalencia de las condiciones o de la conditio sine qua nom (causa del resultado es toda condición que colabora en su producción y sin la cual aquel no se hubiera producido; Todas las condiciones tienen idéntica relevancia causal), teorías de la causalidad eficiente y de la causalidad adecuada (intentos teóricos de limitar la excesiva amplitud de la anterior teoría).

En la actualidad estas teorías de la causalidad vienen siendo corregidas en sus resultados por otras que, no entendiendo la relación acción-resultado como simple relación natural causa-efecto, y partiendo de criterios normativos basados en la naturaleza de lo ilícito penal, deducen sus principios de la naturaleza de la norma y de su fin de protección (teoría de la imputación objetiva). *DICCIONARIO JURÍDICO ESPASA

La prueba y los elementos de prueba deberán tener un nexo causal entre la infracción y la persona procesada, el fundamento tendrá que basarse en hechos reales introducidos o que puedan ser introducidos a través de un medio de prueba y nunca, en presunciones. Art. 455.-

Es decir que para garantizar este nexo es importante proteger la prueba, para eso es la cadena de custodia conforme estudiamos anteriormente. Establecido en el art. 456.

Los criterios de valoración de la prueba se hará teniendo en cuenta su legalidad, autenticidad, sometimiento a cadena de custodia y grado

actual de aceptación científica y técnica de los principios en que se fundamenten los informes periciales.

La demostración de la autenticidad de los elementos probatorios y evidencia física no sometidos a cadena de custodia, estará a cargo de la parte que los presente. Art. 457.

La preservación de la escena del hecho o indicios La o el servidor público que intervenga o tome contacto con la escena del hecho e indicios será la responsable de su preservación, hasta contar con la presencia del personal especializado.

Igual obligación tienen los particulares que por razón de su trabajo o función entren en contacto con indicios relacionados con un hecho presuntamente delictivo. Art. 458.

ACTUACIONES Y TÉCNICAS ESPECIALES DE INVESTIGACIÓN.

Las actuaciones de investigación se sujetarán a las siguientes reglas:

1. Para la obtención de muestras, exámenes médicos o corporales, se precisa el consentimiento expreso de la persona o la autorización de la o el juzgador, sin que la persona pueda ser físicamente constreñida. Excepcionalmente por las circunstancias del caso, cuando la persona no pueda dar su consentimiento, lo podrá otorgar un familiar hasta el segundo grado de consanguinidad.
2. Las diligencias de reconocimiento constarán en actas e informes periciales.
3. Las diligencias de investigación deberán ser registradas en medios tecnológicos y documentales más adecuados para preservar la realización de la misma y formarán parte del expediente fiscal.
4. El registro que conste en el expediente fiscal deberá ser suficiente para determinar todos los elementos de convicción que puedan fundamentar la formulación de cargos o la acusación.
5. En caso de no existir una institución pública acreditada, las autopsias, exámenes médicos, de laboratorio o pruebas biológicas, podrán ser

realizados en una institución de salud privada acreditada y los costos serán asumidos por el Consejo de la Judicatura. Los mismos tendrán valor pericial. Art. 459.

ACTUACIONES TÉCNICAS:

Reconocimiento del lugar de los hechos.- Art. 460.	La o el fiscal con el apoyo del personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, o el personal competente en materia de tránsito, cuando sea relevante para la investigación, reconocerá el lugar de los hechos de conformidad con las siguientes disposiciones:	1. La o el fiscal o el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, podrá impedir a cualquier persona, incluso haciendo uso de la fuerza pública, que ingrese o se retire del lugar donde se cometió la infracción, por un máximo de ocho horas, hasta que se practiquen las actuaciones de investigación necesarias. 2. En las infracciones de tránsito, las diligencias de reconocimiento del lugar de los hechos,investigaciones, inspección técnica ocular y peritajes serán realizados por el personal especializado del organismo competente en materia de tránsito en su respectiva jurisdicción. 3. Los agentes de tránsito tomarán procedimiento y elaborarán el parte correspondiente. Se harán cargo de los presuntos infractores quienes serán puestos inmediatamente a órdenes de la autoridad competente y se requerirá la participación del personal especializado del organismo competente en materia de tránsito en su respectiva jurisdicción. 4. Se remitirá a la o al fiscal correspondiente, los partes policiales y demás documentos relativos a la infracción, en el plazo de veinticuatro horas. 5. La fijación y recolección de las evidencias, huellas, vestigios encontrados en el lugar ingresarán

		encadena de custodia para la investigación a cargo de la o el fiscal, quien dispondrá las diligencias pertinentes. 6. Los vehículos aprehendidos por accidentes de tránsito, en los que resulten personas heridas o fallecidas, se trasladarán a los patios de retención vehicular respectivo hasta su reconocimiento pericial. 7. La diligencia de reconocimiento pericial de los vehículos ordenada por la o el fiscal será practicada dentro del plazo de setenta y dos horas, contadas desde que la o el fiscal recibe el parte policial correspondiente. Posteriormente al reconocimiento pericial se entregará el automotor a su propietario, poseedor o a quien legalmente corresponda. **8. Se realizarán diligencias de reconocimiento del lugar de los hechos en territorio digital, servicios digitales, medios o equipos tecnológicos.**
Actuaciones en caso de muerte. Art. 461.	Cuando se tenga noticia de la existencia de un cadáver o restos humanos, la o el fiscal dispondrá:	1. La identificación y el levantamiento del cadáver. 2. El reconocimiento exterior que abarca la orientación, posición, registro de vestimentas y descripción de lesiones. 3. En el informe de la autopsia constará de forma detallada el estado del cadáver, el tiempo transcurrido desde el deceso, el probable elemento empleado, la manera y las causas probables dela muerte. Los peritos tomarán las muestras correspondientes, las cuales serán conservadas. 4. En caso de muerte violenta, mientras se realizan las diligencias investigativas, la o el fiscal de considerarlo necesario, solicitará a

		la autoridad de salud competente que no otorgue el permiso previo para la cremación.
Exhumación. Art. 462.	En caso de ser necesaria la exhumación de un cadáver o sus restos, seseguirán las siguientes reglas:	1. La o el fiscal, la o el defensor público o privado o la víctima podrán solicitar la realización de una exhumación dentro de la investigación de una presunta infracción penal a la o al juzgador competente, quien podrá autorizar su práctica, para lo cual la o el fiscal designará los peritos médicos legistas que intervendrán. 2. La autorización judicial procederá solamente si por la naturaleza y circunstancias de la infracción,la exhumación es indispensable para la investigación de una presunta infracción penal. 3. El personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, deberá revisar y establecer las condiciones del sitio exacto donde se encuentre el cadáver o sus restos. 4. El traslado y exhumación deberá respetar la cadena de custodia.
Obtención de muestras. Art. 463.	Para la obtención de muestras de fluidos corporales, componentes orgánicos y genético-moleculares se seguirán las siguientes reglas:	1. No se podrá realizar pruebas de carácter biológico, extracciones de sangre, de objetos situados en el cuerpo u otras análogas, si se teme menoscabo en la salud y dignidad de la persona objeto de examen. 2. Cuando el examen deba realizarse en víctimas de infracción contra la integridad sexual o en una niña, niño o adolescente, se tomarán las medidas necesarias en función de su edad y género para precautelar su dignidad e integridad física y psicológica. Los exámenes se practicarán con estrictas condiciones de confidencialidad y respeto a la intimidad.

		Salvo que sea imprescindible, se prohibirá someterle a la persona nuevamente a un mismo examen o reconocimiento médico legal. Los profesionales de la salud que realicen estos exámenes estarán obligados a conservar los elementos de prueba encontrados en condiciones de seguridad, que serán entregados inmediatamente al personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, y deberán rendir testimonio anticipado o podrán ser receptados mediante videoconferencias de acuerdo con las reglas del presente Código.
Ingesta de alcohol y sustancias catalogadas sujetas a fiscalización. Art. 464.	En materia de tránsito, se seguirán las siguientes reglas:	1. Los niveles máximos de concentración de alcohol en la sangre, tolerables para la conducción de vehículos automotores, están determinados en este Código. 2. Cuando existan elementos que revelen la necesidad de practicar al conductor de un vehículo un análisis de ingesta de alcohol o de intoxicación por haber ingerido sustancias catalogadas sujetas a fiscalización, el agente de tránsito realizará la prueba alcohotest o narcotest o en su defecto lo conducirá a una institución acreditada para la práctica de los exámenes correspondientes dentro de las veinticuatro horas subsiguientes. Los resultados de los exámenes servirán como elementos de convicción. 3. Para realizar los exámenes de alcohotest, los agentes de tránsito portarán un detector o cualquier otro aparato dosificador de medición. 4. Si las condiciones físicas de quien conducía imposibilitan realizar las mencionadas pruebas, el agente

		el traslado del o de los heridos a un establecimiento de salud acreditado, en el que se le realizará los exámenes correspondientes. 5. En caso de que la o el conductor se niegue a que se le practiquen los exámenes de comprobación, se presumirá que se encuentra en el máximo grado de embriaguez o de intoxicación por efecto de alcohol o de sustancias catalogadas sujetas a fiscalización. De igual manera serán válidas las pruebas psicosomáticas que los agentes de tránsito realicen en el campo, registradas mediante medio audiovisuales.
Exámenes médicos y corporales. Art. 465.	Podrán efectuarse exámenes médicos o corporales dela persona procesada o de la víctima en caso de necesidad para constatar circunstancias relevantespara la investigación, de acuerdo con las siguientes reglas:	1. En los casos de delitos contra la integridad sexual y reproductiva, trata de personas e infracciones de violencia contra la mujer o miembros del núcleo familiar, cuando una persona ponga en conocimiento que ha sido víctima de una de tales infracciones penales y exista peligro de destrucción de huellas o rastros de cualquier naturaleza en su persona, los centros de salud públicos o privados acreditados a los que se acuda, deberán practicar, previo consentimiento escrito de la víctima o de su representante, los reconocimientos, exámenes médicos y pruebas biológicas correspondientes. 2. Realizados los exámenes, se levantará un acta en duplicado de los mismos, la que será suscrita por la o el jefe del establecimiento o de la respectiva Sección y por los profesionales que lo practicaron. 3. Una copia será entregada a la persona que ha sido sometida al reconocimiento o quien la tenga bajo su cuidado y la otra copia, así como

		las muestras obtenidas y los resultados de los análisis practicados, serán remitidos dentro de las siguientes veinticuatro horas al personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, el que informará inmediatamente a la o al fiscal, o la o al juzgador. 4. Si se trata de exámenes corporales, la mujer a quien deba practicárselos podrá exigir la atención de personal de su mismo sexo. 5. Se podrá solicitar un peritaje psicológico en los casos de violencia sexual, contra la mujer o miembros del núcleo familiar u otros delitos, especialmente cuando la víctima sea niña, niño,adolescente, adulto mayor o mujer embarazada. Estos se realizarán en centros especializados acreditados en esta temática.
Identificación personal. Art. 466.	Cuando no sea posible identificar por otros medios a una persona investigada y sea necesaria la identificación por parte de la víctima o un tercero, se procederá con las siguientes reglas:	1. La o el fiscal dirigirá el reconocimiento. 2. La persona por identificar, tendrá derecho a contar con una o un defensor público o privado. 3. La persona por identificar será puesta entre un mínimo de diez personas de similares características. 4. La víctima o la persona que cumpla el reconocimiento deberá permanecer en un lugar separado antes y después de esta diligencia. No podrá presenciar la formación o ruptura de la fila que se reconoce. 5. Ninguna persona podrá ver al investigado en circunstancia alguna que permita a este identificarlo. 6. Si son varias las personas que deban realizar esta diligencia, no podrán ver a los investigados queintegran la fila y efectuarán el reconocimiento una por una.

		7. La o el fiscal encargado del reconocimiento en la fila, así como el agente encargado de escoltar a cada una de las personas que deban realizarlo, no deberán saber quién es el investigado ni podrán comunicar a las otras personas que deban cumplirlo. 8. En la diligencia se utilizarán medios técnicos adecuados que eviten la exposición de la víctima con la o el investigado. 9. De ser posible, todos los reconocimientos se lo hará a través de la cámara de Gesell, sujetos al debido proceso. 10. Si la identificación se realiza mediante fotografías o vídeos, se presentarán e incorporarán en la audiencia de juzgamiento.
Reconocimiento de objetos. Art. 467.	Los objetos que sirvan como elementos de convicciónde beran ser reconocidos y descritos.	Practicado el reconocimiento, previa suscripción del acta respectiva, se los entregará a sus propietarios, poseedores o a quien legalmente corresponda, a condición de que se los vuelva a presentar cuando la o el fiscal o la o el juzgador lo ordenen, bajo apercibimiento de apremio personal, en caso de no hacerlo. En los casos de objetos sustraídos o reclamados que son recuperados al momento de la detención en delitos flagrantes, se procederá a su reconocimiento y entrega a los propietarios, poseedores o a quien legalmente corresponda en la misma audiencia de formulación de cargos, previa suscripción del acta respectiva. No será necesario realizar un nuevo reconocimiento si los objetos han sido descritos en el informe pericial solicitado inicialmente por la o el fiscal, en el lugar de los hechos.

Reconstrucción del hecho. Art. 468.	La o el fiscal, cuando considere necesario	practicará con el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, o el personal competente en materia de tránsito, la reconstrucción del hecho, con el fin de verificar si la infracción se ejecutó o pudo ejecutarse de un modo determinado, considerando los elementos de convicción que existan en el proceso. En esta reconstrucción el procesado, la víctima o los testigos, si voluntariamente concurren, relatarán los hechos en el lugar donde ocurrieron, teniendo a la vista, si es posible, los objetos relacionados con la infracción.
Maquinarias y vehículos. Art. 469.	Para recoger elementos materiales y evidencia física	que se encuentren en objetos de gran tamaño, como naves, aeronaves, automotores, maquinarias,contenedores, grúas y otros similares, los peritos deben practicar el peritaje en el plazo señalado por la o el fiscal; luego de lo cual la o el fiscal ordenará la entrega a los dueños o legítimos poseedores,-salvo aquellos susceptibles decomiso o destrucción. Los elementos de convicción o evidencia física obtenidos serán embalados y quedarán bajo custodia del organismo respectivo.
Comunicaciones personales. Art. 470.	No podrán grabar o registrar	por cualquier medio las comunicaciones personales de terceros sin que ellos hayan conocido y autorizado dicha grabación o registro, salvo los casos expresamente señalados en la ley. La información obtenida ilegalmente carece de todo valor jurídico. Los riesgos, daños y perjuicios que genere para las personas involucradas, serán imputables a quien forzó la revelación de la información, quedando obligada a efectuar la reparación integral de los daños.

Registros relacionados a un hecho constitutivo de infracción. Art. 471.	No requieren autorización judicial	las grabaciones de audio, imágenes de video o fotografía relacionadas a un hecho constitutivo de infracción, registradas de modo espontáneo al momento mismo de su ejecución, por los medios de comunicación social, por cámaras de vigilancia o seguridad, por cualquier medio tecnológico, por particulares en lugares públicos y de libre circulación o en los casos en que se divulguen grabaciones de audio o video obtenidas por uno de los intervinientes, en cuyo caso se requerirá la preservación de la integralidad del registro de datos para que la grabación tenga valor probatorio. En estos casos, las grabaciones se pondrán inmediatamente a órdenes de la o el fiscal en soporte original y servirán para incorporar a la investigación e introducirlas al proceso y de ser necesario, la o el fiscal dispondrá la transcripción de la parte pertinente o su reproducción en la audiencia de juicio.
Información de circulación restringida. Art. 472.	No podrá circular libremente la siguiente información:	1. Aquella que esté protegida expresamente con una cláusula de reserva previamente establecida en la ley. 2. La información acerca de datos de carácter personal y la que provenga de las comunicaciones personales cuya difusión no haya sido autorizada expresamente por su titular, por la ley o por la o el juzgador. 3. La información producida por la o el fiscal en el marco de una investigación previa y aquella originada en la orden judicial relacionada con las técnicas especiales de investigación. 4. La información acerca de niñas, niños y adolescentes que viole sus derechos según lo establecido en el Código Orgánico de la Niñez y Adolescencia y la Constitución.

		5. La información calificada por los organismos que conforman el Sistema nacional de inteligencia.
Alteración, disposición o destrucción de bienes o sustancias. Art. 473.	Si para practicar la pericia es necesario	alterar o destruir el bien o sustancia que ha de reconocerse, la o el fiscal dispondrá que,de ser posible, se reserve una parte para que se conserve bajo su custodia. Tratándose de hidrocarburos y sus derivados, la o el fiscal luego del reconocimiento respectivo,solicitará al juzgador, ordene la entrega de dichas sustancias a la entidad estatal encargada de la explotación de hidrocarburos, guardándose muestras que permanecerán en cadena de custodia. Tratándose de explosivos u otras sustancias peligrosas, luego del reconocimiento se procederá a su destrucción o entrega a entidades que puedan reutilizarlos.
Análisis y destrucción de sustancias catalogadas sujetas a fiscalización. Art. 474	Las sustancias catalogadas sujetas a fiscalización aprehendidas se someterán al análisis químico, para cuyo efecto se tomarán muestras, que la Policía Nacional entregará a los peritos designados por la o el fiscal, quienes presentarán su informe en el plazo determinado. En el informe se deberán determinar el peso bruto y neto de las sustancias. Las muestras testigo se quedarán bajo cadena de custodia hasta	1. Cuando las sustancias catalogadas sujetas a fiscalización se encuentren impregnadas, diluidas o contenidas en bienes u objetos, los peritos determinarán la cantidad de estas sustancias de ser posible, mediante el análisis cualitativo y cuantitativo. 2. Realizado el análisis químico y la determinación del peso, se entregarán las sustancias en depósito al organismo competente en materia de sustancias catalogadas sujetas a fiscalización, con su respectivo informe, guardando la cadena de custodia. 3. Dentro de los quince días siguientes al inicio de la instrucción, la o el juzgador dispondrá que se proceda a la destrucción de las sustancias catalogadas sujetas a fiscalización aprehendidas y que se encuentran en depósito, salvo que, se trate de insumos, precursores químicos u

	que sean presentadas en juicio. En las actuaciones periciales y de destrucción, se seguirán las siguientes reglas	otros productos químicos específicos, en cuyo caso el organismo competente en materia de sustancias catalogadas sujetas a fiscalización, podrá disponer, dentro de los sesenta días siguientes a la recepción, su utilización o donación a una entidad del sector público, su enajenación para fines lícitos o su destrucción. La donación o enajenación se realizará en la forma que determine este organismo y a favor de las personas naturales o jurídicas, previamente calificadas. 4. Para la destrucción se verificará la integridad de la envoltura o el bien que la contenga y la identidad de las sustancias, se comprobará el peso bruto y el peso neto, verificando si corresponde al que consta en el informe de investigación. En esta diligencia intervendrán la o el juzgador, el funcionario judicial respectivo y el depositario5. Cuando en la investigación se hayan aprehendido sustancias catalogadas sujetas a fiscalización y no se pueda establecer la responsabilidad de persona alguna en la comisión de los delitos por producción o tráfico ilícitos de estas sustancias, realizado el análisis químico, determinado el peso bruto y neto, previa orden judicial, el personal del Sistema especializado integral de investigación, de medicina legal y ciencias forenses, deberá remitir dichas sustancias para depósito al organismo competente en materia de sustancias catalogadas sujetas a fiscalización. 6. El juzgador deberá ordenar la destrucción de aquellas sustancias, dentro de los quince días de haber iniciado la investigación, cumpliendo las formalidades establecidas en este

		Código y, en cuanto a los demás bienes, estos se entregarán en depósito al organismo competente en materia desustancias catalogadas sujetas a fiscalización en el caso de ser incautados.

Elaboración: Juan José Páez Rivadeneira.

Actuaciones especiales de investigación.

Retención de correspondencia. Art. 475.	La retención, apertura y examen de la correspondencia y otros documentos se regirá por las siguientes disposiciones:	1. La correspondencia física, electrónica o cualquier otro tipo o forma de comunicación, es inviolable, salvo los casos expresamente autorizados en la Constitución y en este Código. 2. La o el juzgador podrá autorizar a la o al fiscal, previa solicitud motivada, el retener, abrir y examinar la correspondencia, cuando haya suficiente evidencia para presumir que la misma tiene alguna información útil para la investigación. 3. Para proceder a la apertura y examen de la correspondencia y otros documentos que puedan tener relación con los hechos y circunstancias de la infracción y sus participantes, se notificará previamente al interesado y con su concurrencia o no, se leerá la correspondencia o el documento en forma reservada, informando del particular a la víctima y al procesado o su defensor público o privado. A falta de los sujetos procesales la diligencia se hará ante dos testigos. Todos los intervinientes jurarán guardar reserva. 4. Si la correspondencia u otros documentos están relacionados con la infracción que se investiga, se los

		agregará al expediente fiscal después de rubricados; caso contrario, se los devolverá al lugar de donde son tomados o al interesado. 5. Si se trata de escritura en clave o en otro idioma, inmediatamente se ordenará el desciframiento por peritos en criptografía o su traducción.
Interceptación de las comunicaciones o datos informáticos. Art. 476.	La o el juzgador ordenará la interceptación de las comunicaciones o datos informáticos previa solicitud fundamentada de la o el fiscal cuando existan indicios que resulten relevantes a los fines de la investigación, de conformidad con las siguientes reglas:	1. La o el juzgador determinará la comunicación interceptada y el tiempo de intercepción, que no podrá ser mayor a un plazo de noventa días. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de noventa días. Cuando sean investigaciones de delincuencia organizada y sus delitos relacionados, la interceptación podrá realizarse hasta por un plazo de seis meses. Transcurrido el tiempo autorizado se podrá solicitar motivadamente por una sola vez una prórroga hasta por un plazo de seis meses. 2. La información relacionada con la infracción que se obtenga de las comunicaciones que se intercepten durante la investigación serán utilizadas en el proceso para el cual se las autoriza y con la obligación de guardar secreto de los asuntos ajenos al hecho que motive su examen. 3. Cuando, en el transcurso de una interceptación se conozca del cometimiento de otra infracción, se comunicará inmediatamente a la o al fiscal para el inicio de la investigación correspondiente. En el caso de delitos flagrantes, se procederá conforme con lo establecido en este Código.

		4. Previa autorización de la o el juzgador, la o el fiscal, realizará la interceptación y registro de los datos informáticos en transmisión a través de los servicios de telecomunicaciones como: telefonía fija, satelital, móvil e inalámbrica, con sus servicios de llamadas de voz, mensajes SMS, mensajes MMS, transmisión de datos y voz sobre IP, correo electrónico, redes sociales, videoconferencias, multimedia, entre otros, cuando la o el fiscal lo considere indispensable para comprobar la existencia de una infracción o la responsabilidad de los partícipes. 5. Está prohibida la interceptación de cualquier comunicación protegida por el derecho a preservar el secreto profesional y religioso. Las actuaciones procesales que violenten esta garantía carecen de eficacia probatoria, sin perjuicio de las respectivas sanciones. 6. Al proceso solo se introducirá de manera textual la transcripción de aquellas conversaciones o parte de ellas que se estimen útiles o relevantes para los fines de la investigación. No obstante, la persona procesada podrá solicitar la audición de todas sus grabaciones, cuando lo considere apropiado para su defensa. 7. El personal de las prestadoras de servicios de telecomunicaciones, así como las personas encargadas de interceptar, grabar y transcribir las comunicaciones o datos informáticos tendrán la obligación de guardar reserva sobre su contenido, salvo cuando se las llame a declarar en juicio. 8. El medio de almacenamiento de la información obtenida durante la

		interceptación deberá ser conservado por la o el fiscal en un centro de acopio especializado para el efecto, hasta que sea presentado en juicio. 9. Quedan prohibidas la interceptación, grabación y transcripción de comunicaciones que vulneren los derechos de los niños, niñas y adolescentes, especialmente en aquellos casos que generen la revictimización en infracciones de violencia contra la mujer o miembros del núcleo familiar, sexual, física, sicológica y otros.
Reconocimiento de grabaciones. Art. 477.	La o el juzgador autorizará a la o al fiscal	el reconocimiento de las grabaciones mencionadas en el artículo anterior, así como de vídeos, datos informáticos, fotografías, discos u otros medios análogos o digitales. Para este efecto, con la intervención de dos peritos que juren guardar reserva, la o el fiscal, en audiencia privada, procederá a la exhibición de la película o a escuchar el disco o la grabación y a examinar el contenido de los registros informáticos. Las partes podrán asistir con el mismo juramento. La o el fiscal podrá ordenar la identificación de voces grabadas, por parte de personas que afirmen poder reconocerlas, sin perjuicio de ordenar el reconocimiento por medios técnicos.

Elaboración: Juan José Páez Rivadeneira.

MEDIOS DE PRUEBA PENAL DIGITAL.

Los medios de prueba que adopta el COIP en el Art. 498 son:

1. El documento;
2. El testimonio; y,

3. La pericia.*Jurisprudencia: Gaceta Judicial, COARTADA, 22-dic-1980; Gaceta Judicial, LA PRUEBA EN LO PENAL, 19-may-1999; Gaceta Judicial, APRECIACIÓN DE LA PRUEBA EN LO PENAL, 31-may-1999:

1.- EL DOCUMENTO.

Sobre la prueba documental existen reglas respecto de la presunción de autenticidad; en algunos sistemas se presumen auténticos todos aquellos documentos que se presentan en juicio, salvo prueba en contrario, y en otros no existe tal presunción por lo que se deben presentar pruebas anexas que acompañen al documento para probar su autenticidad.
Es importante recordar que auténtico no es sinónimo de verdadero. Un documento auténtico es respecto del cual se sabe la persona que lo elaboró o lo firmó, sin embargo,sobre la verdad o falsedad de su contenido, será tema de discusión en la audiencia.

El Art. 499, dispone las reglas de la prueba documental, entre estas:

Persona procesada y el fiscal	1. No se obligará a la persona procesada a que reconozca documentos ni la firma constante en ellos, pero se aceptará su reconocimiento voluntario. 2. La o el fiscal o la o el defensor público o privado, podrá requerir informes sobre datos que consten en registros, archivos, incluyendo los informáticos, que se valorarán en juicio.
Utilización de documentos y correspondencia	3. No se hará otro uso de la correspondencia y de los otros documentos agregados al proceso que el necesario para esclarecer los hechos y circunstancias materia del juicio y de sus posibles responsables. 4. Si los documentos forman parte de otro proceso o registro o si reposan en algún archivo público, se obtendrá copia certificada de ellos y no se agregará originales sino cuando sea indispensable para constancia del hecho. En este último caso, la copia quedará en dicho archivo, proceso o registro y satisfecha la

	necesidad se devolverán los originales, dejando la copia certificada en el proceso.
Uso de datos y medios de prueba	5. No se podrá hacer uso procesal o extraprocesal de ninguno de los datos que suministren los documentos si versan sobre asuntos que no tienen relación con el proceso. 6. Podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este Código

¿QUÉ ES EL CONTENIDO DIGITAL.?

El contenido digital es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí.Art.500.

REGLAS PARA LA INVESTIGACIÓN DEL CONTENIDO DIGITAL.

1. El análisis, valoración, recuperación y presentación del contenido digital almacenado en dispositivos o sistemas informáticos se realizará a través de técnicas digitales forenses.
2. Cuando el contenido digital se encuentre almacenado en sistemas y memorias volátiles o equipos tecnológicos que formen parte de la infraestructura critica del sector público o privado, se realizará su recolección, en el lugar y en tiempo real, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.
3. Cuando el contenido digital se encuentre almacenado en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido.
4. Cuando se recolecte cualquier medio físico que almacene, procese o transmita contenido digital durante una investigación, registro

o allanamiento, se deberá identificar e inventariar cada objeto individualmente, fijará su ubicación física con fotografías y un plano del lugar, se protegerá a través de técnicas digitales forenses y se trasladará mediante cadena de custodia a un centro de acopio especializado para este efecto.

Memorias volátil y no volátil.

(Ver Anexo 39)

1.- La memoria volátil de una computadora, es aquella memoria cuya información se pierde al interrumpirse el flujo eléctrico.

Algunos tipos de memorias volátiles son:

DRAM.- (Random Access Memory - Memoria de acceso aleatorio). Tipo de memoria donde la computadora guarda información para que pueda ser procesada más rápidamente. En la memoria RAM se almacena toda información que está siendo usada en el momento. Su capacidad de almacenamiento se mide en megabytes y más recientemente en gigabytes. La información que contienen es renovada continuamente y cuando la computadora se reinicia o se apaga, toda la información contenida se pierde, por eso es llamada memoria volátil. *Fuente: http://www.alegsa.com.ar/Dic/ram.php#sthash.9cAblf0C.dpuf

Este es un tipo de memoria que utilizan las computadoras y otros dispositivos. Por lo general es usada para el almacenamiento temporal de información. Este tipo de memoria es volátil, por lo tanto su contenido se pierde al faltar la energía eléctrica.

Su nombre se debe a que puede accederse a cualquier sector (o celda) de la memoria directamente con una dirección, a diferencia de las memorias de acceso secuencial. A nivel hardware estas memorias poseen un cableado interno que permite acceder a cada byte, pues cada uno de ellos tiene un camino prefijado para accederlo.

RAM.- Las memorias RAM se pueden dividir en estáticas o dinámicas. Las estáticas (SRAM) mantienen la información mientras tengan

corriente eléctrica, en cambio las dinámicas (DRAM) la información contenida en ellas debe ser restaurada constantemente (operación de refresco). Estas últimas suelen ser más baratas, y deben refrescar su contenido cientos de veces por segundo; es por esto que los chips que las componen consumen gran energía y deben ser controlados constantemente.

Las SRAM no sólo son más rápidas que las DRAM, sino que no necesitan refrescar su contenido constantemente ya que físicamente están diseñadas para que los datos se mantengan estables en el tiempo mientras dispongan de electricidad. Estas memorias son más caras por su elevado número de transistores por bit y por lo tanto sólo se utiliza como memoria caché de los microprocesadores y poseen poca capacidad.

Actualmente, las memorias RAM pueden ser, según los tipos de conectores, SIMM, DIMM o RIMM.

SRAM.- (Static random access memory - Memoria de acceso aleatorio estática) Tipo de memoria RAM La palabra "estática" indica que estas memorias retienen su contenido el tiempo que reciben energía, a diferencia de las RAM (DRAM) que necesitan refrescarse periódicamente (SRAM no debe ser confundida con las ROM y las memorias flash, dado que es una memoria volátil y preserva los datos sólo cuando recibe energía).

Es un tipo de memoria que es más rápida y más fiable que las más comunes DRAM.

SRAM tiene un tiempo de acceso de 10 nanosegundos, en cambio en las DRAM es de 60 nanosegundos.

Además, su ciclo es mucho más corto que el de las DRAM porque no necesitan una pausa entre accesos. Desafortunadamente estas son mucho más caras de producir que las DRAM; debido a su alto costo las memorias SRAM sólo son usadas en pequeñas memorias caché.

Dos puntos muy importantes que es necesario explicar sobre las memorias:

1. En informática, dispositivo basado en circuitos que posibilitan el almacenamiento limitado de información y su posterior recuperación. Las memorias suelen ser de rápido acceso, y pueden ser volátiles o no volátiles. La clasificación principal de memorias son RAM y ROM. Estas memorias son utilizadas para almacenamiento primario.
2. Se emplea el término memoria también para llamar a cualquier dispositivo, circuito o medio de grabación que permite almacenar información desde una computadora. Existen memorias de almacenamiento secundario como los discos duros, discos ópticos, etc.

Otros tipos de memoria:

Memoria virtual; Memoria caché; Memoria flash; Las memorias pueden clasificarse en memoria externa o memoria interna; Tarjeta de memoria; Dirección de memoria; Ancho de banda de la memoria; Latencia de memoria.* Fuente: http://www.alegsa.com.ar/Dic/memoria.php#sthash.EhQ56e8H.dpuf

2.- Memoria no volátil, contraria a memoria volátil, es un tipo de memoria que no necesita energía para perdurar.

Algunos dispositivos listados en esta categoría son:

BD-ROM, BD-R, BD-RW.- Tipo de formato de los discos ópticos Blu-Ray que permiten ser grabados una sola vez. http://www.alegsa.com.ar/Dic/bd-r.php#sthash.XrWAPbF1.dpuf

CD, CD-ROM, CD-R, CD-RW.- Compact disk o disco compacto. Disco óptico circular para el almacenamiento de información de forma binaria. Generalmente de 12 cm. de diámetro y que pesa unos pocos gramos. La información se almacena de forma digital, o sea, unos y ceros. Almacenan hasta 640 MB, aunque puede extenderse esa capacidad un poco más.

La información en un CD es leída por una láser desde una lectora de CDs, al usar luz, no hay contacto físico con la superficie, por lo tanto, no hay deterioro de los datos.

Existen gran variedad de tipos de CDs: CD-ROM, CD-RW o CD-R,: http://www.alegsa.com.ar/Dic/cd.php#sthash.ThZQPqoV.dpuf

Cinta magnética.- (Magnetic tape). Tipo de soporte de almacenamiento de información que permite grabar datos en pistas sobre una banda de material magnético (como óxido de hierro o algún cromato). Puede grabarse cualquier tipo de información de forma digital o analógica. Los antiguos sistemas utilizaban cintas tipo riel abierto (reel-to-reel), en cambio los nuevos suelen usar cartuchos tipo casetes.

Las cintas magnéticas son dispositivos de acceso secuencial, pues si se quiere tener acceso al enésimo (n) bloque de la cinta, se tiene que leer antes los n-1 bloques precedentes.

Las cintas magnéticas son muy utilizadas para realizar backups de datos, especialmente en empresas. Algunos formatos de cintas son: DLT, DDS, SLR, AIT, Travan, VXA, etc.

La densidad en las cintas magnéticas es medida en BPI (bits por pulgada), que pueden ir desde los 800 bpi hasta los 6250 bpi. A mayor densidad en la cinta, más datos se guardan por pulgada.

Las cintas magnéticas se dividen en bloques lógicos; un archivo debe abarcar, como mínimo, un bloque completo (si los datos del archivo no lleguen a cubrir el bloque completo, el resto del espacio queda desperdiciado). http://www.alegsa.com.ar/Dic/cinta%20magnetica.php#sthash.EKENWWSk.dpuf

DVD.- (Digital Versatile/Video Disc - Disco Versátil/Video Digital). Formato de almacenamiento digital de datos. Tienen el mismo tamaño físico que un CD, 12 cm de diámetro, u 8 cm para los mini; aunque almacenan mucha más información. Los DVD guardan los datos utilizando un sistema de archivos denominado UDF, el cual es una

extensión del estándar ISO 9660, usado para CD de datos. Un DVD de capa simple puede guardar hasta 4,7 gigabytes (se le conoce como DVD-5). Discos DVD±R DL (DVD-9): una cara, capa doble. 8.5 GB. Discos DVD±R/RW (DVD-10): dos caras, capa simple en ambas. 9.4 GB. Discos DVD+R (DVD-18): dos caras, capa doble en ambas. 17.1 GB. Según el contenido, los DVD pueden clasificarse en: DVD-Video: Películas (vídeo y audio). DVD-Audio: Audio de alta definición. DVD-Data: Datos cualesquiera. Según su capacidad de regrabado: DVD-ROM: Sólo lectura, manufacturado con prensa. DVD R: Grabable una sola vez. DVD RW: Regrabable. DVD R DL: Grabable una sola vez de doble capa DVD RW DL: Regrabable de doble capa. La velocidad de transferencia de datos de una unidad DVD está dada en múltiplos de 1.350 kB/s, lo que significa que una unidad lectora de 16x, permite una transferencia de datos de 16 x 1.350 = 21.600 kB/s (21,09 MB/s). Como las velocidades de las unidades de CD se dan en múltiplos de 150 kB/s, cada múltiplo de velocidad en DVD equivale a nueve múltiplos de velocidad en CD. En términos de rotación física (revoluciones por minuto), un múltiplo de velocidad en DVD equivale a tres múltiplos de velocidad en CD, así que la cantidad de datos leída durante una rotación es tres veces mayor para el DVD que para el CD, y la unidad de DVD 8x tiene la misma velocidad rotacional que la unidad de CD 24x. *http://www.alegsa.com.ar/Dic/dvd.php#sthash.F9qQFsh1.dpuf

Entre otros tenemos: Diskette; Disco duro; EPROM; EEPROM; MRAM; Memoria de tambor; FlashNVRAM; PRAM; PROM; ROM; Memoria racetrack.*

**Para* revisar conceptos ver: http://www.alegsa.com.ar/Diccionario/diccionario.php

Como anotamos en el capítulo correspondiente a la técnica digital forense, para la prolija actuación de esta prueba hay que ajustarse a la estandarización de métodos y normas internacionales, para la plena validez de la prueba.

2.- EL TESTIMONIO.

El testimonio es el medio a través del cual se conoce la declaración de la persona procesada, la víctima y de otras personas que han presenciado el hecho o conocen sobre las circunstancias del cometimiento de la infracción penal. Art. 501.- *Jurisprudencia: Gaceta Judicial, PRUEBA TESTIMONIAL A FALTA DE PRUEBA MATERIAL, 13-may-1993.

La prueba y los elementos de convicción, obtenidos mediante declaración, se regirán por las siguientes reglas:

1. El testimonio se valorará en el contexto de toda la declaración rendida y en relación con las otras pruebas que sean presentadas.
2. La o el juzgador podrá recibir como prueba anticipada los testimonios de las personas gravemente enfermas, de las físicamente imposibilitadas, de quienes van a salir del país, de las víctimas o testigos protegidos, informantes, agentes encubiertos y de todas aquellas que demuestren que no pueden comparecer a la audiencia de juicio. En el caso de audiencia fallida, y en los que se demuestre la imposibilidad de los testigos de comparecer a un nuevo señalamiento, el tribunal, podrá receptar el testimonio anticipado bajo los principios de inmediación y contradicción.
3. Si la persona reside en el extranjero, se procederá conforme con las normas internacionales o nacionales para el auxilio y la cooperación judicial. Si es posible se establecerá comunicación telemática.
4. Nadie podrá ser llamado a declarar en juicio penal contra su cónyuge, pareja o parientes hasta el cuarto grado de consanguinidad o segundo de afinidad, excepto en el caso de violencia contra la mujer o miembros del núcleo familiar, sexual y de género. Serán admisibles las declaraciones voluntarias de las víctimas de una infracción o de sus parientes con independencia del grado de parentesco.
5. Las niñas, niños y adolescentes declararán sin juramento, pero con la presencia de sus representantes o un curador que será nombrado y posesionado en la misma audiencia de juicio.
6. La o el juzgador nombrará y posesionará en el mismo acto a un traductor, cuando el declarante o sepa el idioma castellano.

7. Si la persona que declara es sordomuda, la o el juzgador recibirá el testimonio por escrito; si no sabe escribir, con el auxilio de un intérprete o, a falta de éste, de una persona acostumbrada a entender al declarante, a quien se le posesionará en el mismo acto.
8. Los testimonios no podrán ser interrumpidos, salvo que exista una objeción por parte de los sujetos procesales.
9. Las personas que sean llamadas a declarar y que se encuentren en situación de riesgo tendrán derecho al resguardo proporcionado por la o el fiscal a través del Sistema nacional de protección y asistencia de víctimas, testigos y otros participantes en el proceso, o disposición a la Policía Nacional, a fin de que se garantice su integridad personal, su testimonio y comparecencia a la audiencia de juicio, en la que puedan rendir su testimonio a través de medios tecnológicos o de caracterización que aseguren su integridad.
10. El testimonio se practicará en la audiencia de juicio, ya sea en forma directa o a través de videoconferencia, con excepción de los testimonios anticipados.
11. Las o los servidores públicos que gozan de fuero de Corte Nacional, podrán rendir su testimonio mediante informe juramentado.
12. Quienes rindan testimonio deberán informar sobre sus nombres, apellidos, edad, nacionalidad, domicilio o residencia, estado civil, oficio o profesión, salvo el caso del testigo protegido, informante, agente encubierto o persona cuya integridad se encuentre en riesgo. Permanecerán en un lugar aislado, declaran individualmente y de forma separada de modo que no puedan oír mutuamente sus declaraciones.
13. Al momento de rendir testimonio, se prestará juramento en todo cuanto conoce y se es preguntada. Se le advertirá sobre las penas con las cuales será sancionado el perjurio.
14. Los sujetos procesales podrán realizar preguntas u objetarlas, y la o el juzgador deberán resolver la objeción para que la persona las conteste o se abstenga de hacerlo.
15. No se podrán formular preguntas autoincriminatorias, engañosas, capciosas o impertinentes.
16. No se podrán formular preguntas sugestivas en el interrogatorio, excepto cuando se trate de una pregunta introductoria o que recapitule información ya entregada por el mismo declarante.
17. Podrán hacerse preguntas sugestivas durante el contra examen.

3.- LA PERICIA.

En el campo de las nuevas tecnologías, el perito digital forense, como perito acreditado en la función judicial, tiene un ámbito de actuación muy amplio y cada vez mayor en todo tipo de procesos de enjuiciamiento, tanto civil como penal, bien en aquellos en los que existen algunas pruebas digitales, como en aquellos en los que las tecnologías de la información están en el centro del proceso y, más aun en aquellos calificados específicamente como delitos informáticos.

El nuevo COIP, ha expuesto algunas reglas generales, para el perfil de las y los peritos entre estas:

1. Ser profesionales expertos en el área, especialistas titulados o con conocimientos, experiencia o experticia en la materia y especialidad, acreditados por el Consejo de la Judicatura.
2. Desempeñar su función de manera obligatoria, para lo cual la o el perito será designado y notificado con el cargo.
3. La persona designada deberá excusarse si se halla en alguna de las causales establecidas en este Código para las o los juzgadores.
4. Las o los peritos no podrán ser recusados, sin embargo el informe no tendrá valor alguno si el perito que lo presenta, tiene motivo de inhabilidad o excusa, debidamente comprobada.
5. Presentar dentro del plazo señalado sus informes, aclarar o ampliar los mismos a pedido de los sujetos procesales.
6. El informe pericial deberá contener como mínimo el lugar y fecha de realización del peritaje,identificación del perito, descripción y estado de la persona u objeto peritado, la técnica utilizada, la fundamentación científica, ilustraciones gráficas cuando corresponda, las conclusiones y la firma.
7. Comparecer a la audiencia de juicio y sustentar de manera oral sus informes y contestar los interrogatorios de las partes, para lo cual podrán emplear cualquier medio.
8. El Consejo de la Judicatura organizará el sistema pericial a nivel nacional, el monto que se cobre por estas diligencias judiciales o procesales, podrán ser canceladas por el Consejo de la Judicatura.

De no existir persona acreditada como perito en determinadas áreas, se deberá contar con quien tenga conocimiento, especialidad, experticia o título que acredite su capacidad para desarrollar el peritaje. Para los casos de mala práctica profesional la o el fiscal solicitará una terna de profesionales con la especialidad correspondiente al organismo rector de la materia.

Cuando en la investigación intervengan peritos internacionales, sus informes podrán ser incorporados como prueba, a través de testimonios anticipados o podrán ser receptados mediante video conferencias de acuerdo a las reglas del presente Código. (Art. 511).

(Ver Anexo 40)

EL REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL.

El reglamento del sistema pericial integral de la función judicial, vigente, fue emitido por resolución número 40 – 20014, por el Consejo Nacional de la Judicatura, y, publicado en Registro Oficial Suplemento 125 del 28 de abril del 2014, regula el funcionamiento y administración del sistema pericial integral, en relación a la calificación, designación, obligaciones, evaluación,capacitación, régimen disciplinario y cualquier otro aspecto de los peritos que participen en los procesos judiciales, pre procesales, o de cualquier otra naturaleza que se lleven a cabo en la administración de Justicia o Función Judicial.

Se rige por los principios de igualdad, probidad, no discriminación, publicidad, cumplimiento de méritos y requisitos, así como transparencia y acceso a la información pública.

El perito que sea designado como tal en cualquier tipo de proceso judicial o pre procesal, debe estar previamente calificado por el Consejo de la Judicatura, y debe cumplir con las regulaciones y la normativa de esta resolución.

No será obligatoria la calificación en caso de que se trate de un perito que no tenga su domicilio en el Ecuador, y que sea designado

como tal en un juicio cuando no existan peritos de la especialidad correspondiente en el país.

En casos extraordinarios, cuando en un proceso judicial o pre procesal se requiera un perito en determinada especialidad para la cual no existan peritos calificados, excepcionalmente se requerirá la participación de una experta o experto en la especialidad requerida, en cuyo caso tampoco se exigirá la calificación, y se procederá conforme a lo establecido en el artículo 31 de este reglamento.

Los requisitos, para las personas que deseen calificarse como peritos de la Función Judicial, y deben cumplir entre otros los siguientes:

1. Ser mayores de edad, ser capaces y estar en ejercicio de sus derechos de participación;
2. Ser conocedoras o conocedores y/o expertas o expertos en la profesión, arte, oficio, o actividad para la cual soliciten calificarse;
3. En el caso de profesionales, tener al menos dos (2) años de graduadas o graduados a la fecha dela solicitud de calificación, y cumplir con los requisitos de experiencia establecidos en este reglamento. Para las y los demás expertos tener al menos dos (2) años de práctica y experiencia a la fecha de la solicitud de calificación, en el oficio, arte o actividad en la cual tengan interés de calificarse;
4. También se podrán presentar, para justificar la experticia y conocimiento de la o el solicitante,hasta diez (10) informes periciales realizados en los últimos dos (2) años, los cuales serán analizados por el Consejo de la Judicatura para determinar si acreditan experticia; y,
5. No hallarse incursas o incursos en las inhabilidades o prohibiciones para ser calificada o calificado como perito previstas en la ley y este reglamento.

No podrán obtener su calificación como peritos.-, así como no podrán renovar la calificación obtenida, quienes incurran en las siguientes causales de inhabilidades y prohibiciones:

1. Las personas contra quienes se hubiere dictado sentencia condenatoria ejecutoriada por un delito en contra de la administración

pública, perjurio, lesa humanidad, odio, sexual o por violencia contra la mujer o miembros del núcleo familiar.
2. Las personas contra quienes se hubiere dictado sentencia condenatoria ejecutoriada por un delito sancionado con pena de privación de la libertad durante el último año, previo a la fecha de la presentación de la solicitud de calificación o su renovación, mientras dure la condena correspondiente.
3. Las personas que han recibido sanción de suspensión o destitución por responsabilidad administrativa, civil o penal, con ocasión del desempeño de una función pública, mientras dure la inhabilidad de conformidad con la ley.
4. Las personas que al momento de la solicitud, no se encuentren al día en sus obligaciones tributarias con el Servicio de Rentas Internas.
5. Las personas que incurrieren en falsedad, adulteración o inexactitud de los datos incluidos en los formularios de calificación, o de los documentos que anexen o presenten como parte de su proceso de calificación ante el Consejo de la Judicatura.

DESIGNACIÓN DE PERITOS.

Para la designación de peritos en los distintos procesos judiciales o pre procesales de la Función Judicial, se respetarán los principios de profesionalidad, especialidad, transparencia, alternabilidad, e igualdad.

Las juezas, los jueces, y las y los fiscales, procederán por sorteo a la designación de peritos, a través del Sistema Informático Pericial de la Función Judicial. En caso de que no existan, o no se cuente con peritos en un cantón determinado, el sorteo se realizará con los registros de peritos de los cantones más cercanos. En caso de que no existan o no se cuente con peritos en los cantones cercanos, el sorteo se realizará con los registros de peritos a nivel provincial. En caso de que no existan peritos a nivel provincial, el sorteo se realizará con los registros de peritos de las provincias limítrofes de la provincia en cuestión. En caso de que no existan peritos en este último supuesto, se designará directamente un perito del registro nacional, previa consulta a la Dirección Provincial correspondiente que lo coordinará con la o el administrador del sistema pericial. Cuando una o un fiscal se encuentre

en este caso, previo a la designación de perito lo consultará con la dependencia encargada de asuntos periciales de la Fiscalía General del Estado.

En el caso de que no exista un perito a nivel nacional para la experticia solicitada en un proceso en particular, o se requiera de un pronunciamiento de mayor complejidad y alcance; y, no exista el perito, la jueza o el juez, previo a la designación del mismo, consultará el particular a la Dirección Provincial correspondiente que lo coordinará con la o el administrador del sistema pericial, para la ubicación del perito. Cuando la o el fiscal se encuentre en este caso, previo a la designación del perito lo consultará con la dependencia encargada de asuntos periciales de la Fiscalía General del Estado.

De forma excepcional, y ante la imposibilidad de contar con peritos calificados con determinada experticia y conocimiento específico, y habiéndose agotado el cumplimiento de los procesos establecidos en los incisos precedentes, la jueza o el juez, designará perito directamente previa audiencia de las partes. Cuando la o el fiscal se encuentre en este caso, previo a la designación de perito lo consultará con la dependencia encargada de asuntos periciales de la Fiscalía General del Estado.

En procesos no penales y cuando la normativa legal lo permita, las partes procesales podrán solicitarla designación de peritos de forma directa en la persona de una experta o experto específico. Todos los peritos que se nombren de esta forma tienen que estar previamente calificados, y deberán cumplir con todas las demás obligaciones y deberes previstos en la presente normativa.

Al momento de la designación del perito, se dejará constancia en el sistema informático del código de calificación de la escogida o escogido. En los casos excepcionales en que el perito designado no tuviese código de calificación, igualmente se dejará constancia de su designación en el sistema informático.

Los peritos que pertenezcan a instituciones del sector público cuando sean designadas o designados por la jueza o juez de la causa,

actuarán únicamente en los procesos contencioso administrativos o tributarios inherentes a sus dependencias, excepto en el caso de los peritos pertenecientes a la Subdirección Técnica y Científica de la Policía Judicial y a la Fiscalía General del Estado, quienes podrán ser designadas o designados en cualquier otro proceso.

En los procesos de familia, mujer, niñez, adolescencia, violencia contra la mujer o intrafamiliar; en procesos judiciales que se sustancien en las Unidades de Flagrancia de la Función Judicial; o,cualquier otro considerado por el Pleno del Consejo de la Judicatura o su Presidenta o Presidente, la autoridad judicial podrá designar directamente como perito exclusivamente a las y los funcionarios públicos pertenecientes a la Función Judicial, a las instituciones del sistema de salud pública y a la Subdirección Técnica y Científica de la Policía Judicial, que se encuentren previamente calificados como tales para desarrollar su labor en este tipo de procesos. Solo en caso de que no existan estos peritos para este tipo de procesos, la autoridad judicial procederá a designarles siguiendo el proceso determinado en el artículo 12 del reglamento.

Las y los funcionarios competentes de la Fiscalía General del Estado, que conocen procesos preprocesales o de indagación previa, obligatoriamente designarán peritos por sorteo del Registro de Peritos del Consejo de la Judicatura, de conformidad con los principios y criterios establecidos en los artículos precedentes. Al efecto, esta dependencia pública determinará y ajustará sus procedimientos internos e informáticos para que se cumpla con esta obligación.

Es requisito que al momento de la posesión, la calificación pericial se encuentre vigente. En caso de que la calificación pericial venza luego de la posesión del perito, este tendrá igualmente la obligación de presentar su informe y cumplir con todos los deberes inherentes al encargo judicial. El informe y las actuaciones periciales cumplidas en este supuesto, tendrán toda la validez legal y procesal que el caso lo amerite.

Las juezas y los jueces, y las y los fiscales, al momento de la posesión de un perito designado, dejarán constancia en el acta procesal a más de

las fórmulas jurídicas de rigor, el número de código de calificación de la o el posesionado; así como, copia de la identificación de calificación emitida por la Dirección Provincial del Consejo de la Judicatura correspondiente.

En los casos de peritajes extraordinarios en que el perito designado no tuviese código de calificación,igualmente se dejará constancia de este particular en el acta correspondiente al momento de la posesión.

En todos los casos y sin excepción, la jueza, el juez, y la o el fiscal dejará constancia de la posesión del perito en el módulo del sistema informático de peritos.

En cualquier caso que un perito designado no se posesione de su cargo, la jueza, el juez o la o el fiscal competente dejarán constancia de este particular en el sistema informático de administración de peritos, y designará inmediatamente y de oficio a un nuevo perito de conformidad con los principios, criterios y procedimientos dispuestos.

*Fuente: REGLAMENTO DEL SISTEMA PERICIAL INTEGRAL DE LA FUNCIÓN JUDICIAL.

OBLIGACIONES DE LOS PERITOS.

Los peritos calificados desempeñarán su función de auxiliares dela justicia con objetividad, imparcialidad, responsabilidad, oportunidad, puntualidad, rectitud,corrección y honestidad. Su trabajo deberá enmarcarse en todo momento en la ética, con la presentación de su criterio técnico y especializado, exento de juicios de valor de ningún tipo.

La obligación del perito es única e integral y comprende las siguientes actividades: la posesión, la presentación del informe verbal y escrito, la presentación de aclaraciones, ampliaciones u observaciones al informe, la defensa y/o exposición del informe en audiencias orales, de prueba

o de juicio; así como, cualquier otra actividad necesaria para cumplir con su encargo judicial.

Son obligaciones específicas de los peritos:

1. Posesionarse obligatoriamente una vez que han sido designados, salvo causas de fuerza mayor ocaso fortuito, ausencia de la ciudad, tener a su cargo más de tres informes periciales pendientes de presentación, tener el mismo día y hora previsto para su posesión otra diligencia en otra judicatura o fiscalía, o cualquier otra salvedad establecida por la ley.

En todos estos casos, el perito deberá probar documentadamente en el proceso su falta a la posesión;

2. Presentar el informe correspondiente oportunamente, en la forma, plazos y términos previstos por la normativa o por la autoridad judicial correspondiente. En caso de dificultad o complejidad en su trabajo, tendrá la posibilidad de solicitar motivadamente a la autoridad competente, un solo plazo adicional para presentar su informe, la ampliación o aclaración al mismo, salvo que la normativa legal disponga lo contrario. Se podrán solicitar plazos adicionales al antes establecido de forma excepcional y tomando en consideración las dificultades para la presentación del informe. La jueza, el juez, o la o el fiscal, motivarán la aceptación o no de esta nueva solicitud de ampliación de plazo que presente la o el perito;
3. Presentar el informe correspondiente, de forma verbal y escrita según lo que la normativa establezca, y con los requisitos mínimos establecidos en este reglamento y la ley;
4. Presentar obligatoriamente y dentro del plazo otorgado, las aclaraciones, ampliaciones o complementos al informe presentado que ordene la autoridad judicial competente. Estas aclaraciones se presentarán de forma verbal y escrita según la normativa que lo establezca;
5. Explicar y defender el informe presentado y sus conclusiones, en las audiencias orales, de prueba,o de juicio para las cuales fuere notificado legalmente, si la ley así lo prevé;

6. Presentar conjuntamente con su informe en todos los procesos judiciales o pre procesales, la copia certificada de la factura de honorarios emitida por su persona, por el trabajo pericial realizado;
7. Abstenerse de cobrar valores adicionales a los incluidos en la factura presentada en el proceso judicial o pre procesal, por el informe presentado, por las aclaraciones o ampliaciones hechas, por la defensa del informe en audiencia oral, de prueba o de juicio, o por cualquier otra actividad inherente a su actividad pericial. Los valores de honorarios facturados son únicos, y abarcan todas las obligaciones de los peritos constantes en el presente artículo;
8. Aprobar los cursos de capacitación determinados en el presente reglamento; y,
9. Cualquier otra obligación establecida en la normativa legal, en este reglamento y/o por la o el administrador del sistema pericial.

INFORME PERICIAL

El informe pericial, sus explicaciones o aclaraciones, se presentarán de forma verbal y por escrito, de conformidad con la normativa procesal correspondiente. En caso de que el informe sea escrito, la jueza o juez o la o el fiscal obligatoriamente lo subirá sin los anexos al sistema informático que administra el proceso correspondiente, dejando constancia e incluyendo al momento de hacerlo, el número del código de calificación de perito.

Los informes periciales realizados en procesos calificados por la ley como reservados, o que tienen que ver con información restringida por la ley, no se subirán al sistema informático que administra el proceso correspondiente.

Contenido del Informe Pericial.

Los requisitos mínimos obligatorios de todo informe pericial son los siguientes:

1. Parte de antecedentes, en donde se debe delimitar el objeto del peritaje, esto es, se tiene que especificar claramente el tema sobre el que informará en base a lo ordenado por la jueza o juez, la o el fiscal y/o lo solicitado por las partes procesales;

2. Parte de consideraciones técnicas o metodología a aplicarse, en donde se debe explicar claramente, cómo aplican sus conocimientos especializados de una profesión, arte u oficio, al caso o encargo materia de la pericia;
3. Parte de conclusiones, luego de las consideraciones técnicas, se procederá a emitir la opinión técnica, o conclusión de la aplicación de los conocimientos especializados sobre el caso concreto analizado. La conclusión será clara y directa en relación a la pericia realizada. Se prohíbe todo tipo de juicios ambiguos, así como cualquier tipo de juicio de valor sobre la actuación de las partes en el informe técnico; y,
4. Parte de Inclusión de documentos de respaldo, anexos, o explicación de criterios técnicos, deberá sustentar sus conclusiones ya sea con documentos y objetos de respaldo (fotos, láminas demostrativas, copias certificadas de documentos, grabaciones de audio y video, etc.); y/o, con la explicación clara de cuál es el sustento técnico o científico para obtener un resultado o conclusión específica. Se debe exponer claramente las razones especializadas del perito para llegar a la conclusión correspondiente. No se cumplirá con este requisito si no se sustenta la conclusión con documentos, objetos, o con la explicación técnica y científica exigida en este numeral.

A más de las obligaciones mínimas establecidas en los numerales anteriores de este artículo, el perito deberá incluir también en el informe cualquier otro requisito determinado de forma específica por la ley correspondiente.

Sin perjuicio de los requisitos que deben constar obligatoriamente en todo informe pericial, verbal y/o escrito, el perito designado puede incluir cualquier otra información que considere relevante como parte de su trabajo.

Toda aclaración o ampliación del informe pericial deberá ser pertinente a la pericia dispuesta, y el perito responderá directamente a los requerimientos ordenados por la o el funcionario judicial competente.

En lo posible se mantendrá el formato del informe pericial contenido en el artículo anterior.

Formato del Informe Pericial.

El formato del informe pericial con los requisitos mínimos delmismo constará en el módulo de peritos del Sistema Informático Pericial del Consejo de la Judicatura a efectos de que pueda ser descargado, conocido, estudiado y utilizado por las y los interesados.

Peritajes extraordinarios.

Se consideran peritajes extraordinarios aquellas pericias especializadas de alta complejidad técnica, tales como las relacionadas con el medio ambiente,áreas hidrocarburífera y minera, propiedad intelectual, sistemas informáticos complejos, genética,alta tecnología, entre otras, así como en peritajes de mayor dificultad que requieran el uso de conocimientos científicos, materiales especiales y procesos complicados. Así mismo, se encuentran dentro de esta categoría aquellos peritajes que requieran especialistas que no se encuentren calificados dentro del catálogo pericial de especialidades y su concurso sea indispensable y extraordinario para un proceso judicial o pre procesal en particular. En estos casos el valor de los honorarios periciales serán fijados por la jueza, el juez, o la o el fiscal, bajo su responsabilidad,tomando en cuenta la complejidad de la actividad, la especialidad requerida, los aspectos científicos y técnicos que solicitan la jueza, juez, la o el fiscal, y las partes, y los productos materia del informe,motivando en todos los casos las razones por las cuales se aplicó esta norma.

Cuando la jueza o el juez aplique esta disposición en procesos no penales, necesaria y previamente deberá contar con la aprobación de la Dirección Provincial del Consejo de la Judicatura correspondiente quien coordinará tal decisión con el administrador del sistema pericial, dentro del plazo de cinco (5) días desde la petición realizada por la autoridad judicial.

La Fiscalía General del Estado, en cumplimiento de este artículo y de conformidad con su normativa interna, en los trámites pre procesales y juicios penales en los que el Estado en representación delos intereses

de la sociedad requiera la práctica de pericias en estas materias y especialidades, así como en otras de alta complejidad, podrá fijar el monto de los honorarios del perito.

En los casos de mediación y justicia de paz, las partes deberán convenir conjuntamente el pago de los honorarios periciales, previamente a la realización del peritaje, tomando en consideración los criterios y parámetros de este reglamento. En los casos de jurisdicción voluntaria, las partes directamente interesadas, asumirán los costos de los honorarios de conformidad con los criterios y parámetros del reglamento.

Salvo norma legal en contrario, los gastos, tales como movilización, utilización de insumos o equipos, logística, o los relacionados directamente con la realización de la pericia, en que incurrieren los peritos calificados para la realización del informe y el cumplimiento de sus obligaciones, deberán ser reconocidos por los obligados al pago de los honorarios. Al efecto, se presentarán ante la autoridad judicial correspondiente las facturas vigentes y autorizadas por el Servicio de Rentas Internas a nombre del perito, que justifique el gasto en cuestión. La jueza, el juez y/o la o el fiscal, al comprobar la pertinencia del gasto ordenará motivadamente el pago al obligado hasta en un plazo de veinte (20) días.

En el caso de procesos penales, el Consejo de la Judicatura y la Fiscalía General del Estado, en base a los justificativos correspondientes, reconocerá y pagará a la Policía Judicial o a las instituciones u organismos públicos, el valor de los materiales que hubieren utilizado para el desempeño del cargo por parte del perito.

RÉGIMEN DISCIPLINARIO DE LOS PERITOS.

El régimen disciplinario para peritos calificados y acreditados por el Consejo de la Judicatura, tiene como objetivo el regular las conductas motivo del proceso disciplinario de estos auxiliares de la justicia, así como las consecuencias originadas por las mismas.

Serán eliminados del Registro de Peritos calificados, los peritos que incurran en las siguientes conductas:

1. Por comprobarse conforme a derecho inexactitud manifiesta, falsedad o adulteración en los datos y/o documentos entregados para la calificación, o su renovación.
2. Por comprobarse violación, y/o no cumplimiento de algunas de las obligaciones generales de todo perito establecidas en el artículo 18 de este reglamento.
3. No concurrir injustificadamente a las posesiones y/o no aceptar el encargo para el que fue designada o designado dentro del plazo establecido por las juezas o jueces, o por las y los fiscales, más de tres veces en un mismo año calendario. Sólo se aceptarán como excusa válida las determinadas en el numeral 1 del artículo 19 de este reglamento.
4. Renunciar injustificadamente al encargo para el que fue designada o designado, más de dos veces en un mismo año calendario. La renuncia solamente se justificará por temas provocados por caso fortuito o fuerza mayor, debidamente comprobados; en caso de enfermedad, para justificarla se presentarán las certificaciones otorgadas y/o validadas por el IESS o el Ministerio de Salud.
5. Cuando se comprobare conforme a derecho que el informe pericial, o sus ampliaciones,aclaraciones o complementos, fueron realizados y/o expuestos distorsionando los hechos, o las conclusiones de forma intencional con el fin de favorecer indebidamente un criterio o conclusión, o existe error esencial.
6. No presentar injustificadamente el informe pericial dentro de los plazos otorgados para el efecto.
7. No presentar injustificadamente las ampliaciones, aclaraciones o complementos del informe pericial, dentro del plazo ordenado por la autoridad competente.
8. No concurrir injustificadamente a explicar y/o defender el informe pericial en las audiencias orales,de prueba o de juicio para las cuales fueren convocadas o convocados y/o notificadas o notificados.
9. Cobrar y/o percibir valores correspondientes a honorarios y/o gastos, diferentes a los establecidos por la jueza o el juez, o la o el fiscal de conformidad con este reglamento.

10. No adjuntar ni presentar en el proceso judicial o pre procesal, en todos los casos, la copia certificada de la factura de honorarios autorizada por el Servicio de Rentas Internas.
11. No aprobar el Curso Básico de Peritos dentro de los plazos establecidos por este reglamento.

La exclusión de la calificación del perito del Registro de Peritos Calificados se hará sin perjuicio delas responsabilidades legales a que hubiere lugar.

Los peritos que se encontraren inmersos en las actuaciones determinadas en los numerales 3, 4, 6, 7, 8 y 10 del artículo anterior, no podrán renovar su calificación en el plazo de dos (2) años desde la fecha de la resolución en la que se decidió la eliminación de su nombre del Registro de Peritos de la Función Judicial por el cometimiento de estas conductas.

Los peritos que se encontraren inmersos en los comportamientos determinados en los numerales 1,2, 5 y 9 del artículo anterior, quedarán inhabilitados permanentemente para el desempeño de las funciones de perito, sin que puedan renovar su calificación y acreditación desde la fecha de la resolución en la cual se decidió la eliminación de su nombre del Registro de Peritos de la Función Judicial por el cometimiento de estas conductas.

En caso de que los peritos no aprueben el Curso Básico de Peritos dentro de los plazos previstos en este reglamento, su calificación será excluida del registro de peritos calificados. Podrá calificarse nuevamente de forma inmediata cumpliendo con todos los requisitos establecidos en este reglamento, previa la aprobación del Curso Básico de Peritos.

El proceso administrativo para conocer y resolver los informes y/o denuncias de conductas irregulares, o violatorias de sus obligaciones de los peritos establecidas en este reglamento, se desarrollará de la siguiente forma:

1. De oficio o a petición de parte, la Dirección Provincial del Consejo de la Judicaturacorrespondiente iniciará el proceso administrativo en

contra de un perito. Al efecto tanto en el informe como en la denuncia respectiva, se deben adjuntar las pruebas que los sustenten y justifiquen.
2. Una vez revisados el informe y/o denuncia con las pruebas de respaldo, se notificará dentro de las siguientes setenta y dos (72) horas al perito sujeto al proceso administrativo. Esta notificación se la hará personalmente o a través de los medios electrónicos autorizados para el efecto.
3. El perito tendrá el término de tres (3) días para contestar al informe y/o a la denuncia presentada,a efectos de hacer valer su derecho de defensa. El perito tendrá en todo momento acceso al expediente administrativo y sus documentos, pudiendo solicitar a su costa, copias certificadas del mismo.
4. Con la contestación o sin ella, la Directora o Director Provincial del Consejo de la Judicatura correspondiente, tendrá tres (3) días desde la fecha de preclusión del término anterior, para dictar la resolución motivada que corresponda, la cual será notificada a las personas interesadas.
5. Las decisiones de la Directora o Director provincial serán apelables, dentro del término de tres (3)días desde la notificación, para ante el Pleno del Consejo de la Judicatura, que lo decidirá previo informe de la Subdirección Nacional de Organismos Auxiliares y Sistema Pericial del Consejo de la Judicatura. De esta decisión no cabrá recurso alguno.

El informe se presentará cuando el Consejo de la Judicatura inicie de oficio el proceso administrativo o cuando sean las juezas o los jueces, así como las y los fiscales, quienes soliciten el inicio de tal proceso.

En caso de que sean las partes procesales, o la ciudadanía en general, quienes soliciten el inicio del proceso administrativo, obligatoriamente presentarán denuncia con los requisitos del artículo 113 del Código Orgánico de la Función Judicial.

En caso de que el perito sea excluido de su calidad de tal luego de un pronunciamiento administrativo definitivo, estará en la obligación de realizar y terminarlas pericias de las que se hubiese aceptado el encargo, caso contrario el Consejo de la Judicatura sereserva el derecho de iniciar las acciones legales del caso por el incumplimiento de esta obligación.

La acción disciplinaria prescribe:

1. Por las conductas previstas en el primer inciso del artículo 44 de este reglamento, en el plazo de 60 días; y,
2. Por las conductas previstas en el segundo inciso del artículo 44 de este reglamento, en el plazo de un (1) año, salvo que estas conductas estuvieren vinculadas con el cometimiento de un delito, caso en el cual prescribirán en cinco (5) años, sin perjuicio del régimen de prescripción del delito o de la acción establecida en la ley.

Los plazos de prescripción de la acción disciplinaria se contarán, en el caso de denuncia desde que se cometió la conducta materia del inicio del proceso administrativo; y, en el caso de acciones de oficio o por informes de funcionarios judiciales, desde que tuvo conocimiento la autoridad. La iniciación del proceso disciplinario interrumpe la prescripción hasta por un año. Vencido este plazo, la acción disciplinaria prescribe definitivamente.

Práctica peritaje digital forense.

(Ver Anexo 41)

La pericia digital forense puede versar sobre:

DELITOS	- Robo, hurto, borrado intencional o accesos no autorizados a la información de una determinada empresa o institución, procesada y/o generada por los sistemas de informáticos. - Duplicación no autorizada de datos procesados y/o generados por los sistemas informáticos. - Edición, divulgación, acceso o posesión de pornografía ilegal, como por ejemplo, la pornografía infantil. - Interceptación de las telecomunicaciones, por ejemplo, de los [usuarios], de las empresas, de los partidos políticos, etc. - Inyección de programas infecciosos, como virus y gusanos, dentro de sistemas informáticos. -Publicidad engañosa o correo electrónico spam. - Vulneración de claves hashing*

PROPIEDAD INTELECTUAL	-Control, actualización y adquisición de licencias de software -Delitos contra la propiedad industrial por espionaje o por revelación de secretos. -Delitos contra la propiedad intelectual, por ejemplo, por copia o difusión de libros en formato digital, de música, de vídeos, etc. - Infracción a la ley de propiedad intelectual del software. - Manipulación indebida de programas. Uso indebido de la información por empleados desleales. - Piratería informática, por ejemplo, por difusión o uso de software sin licencia o sin autorización. - Valoración del coste del desarrollo de aplicaciones.
SISTEMAS	- Métodos y normas a seguir en cuestión de seguridad y privacidad de la información procesada y/o generada por los sistemas informáticos. - La realización de auditorías de áreas de sistemas y centros de cómputos así como de los sistemas informáticos utilizados. -Recuperación de datos borrados y rastreo de información en los distintos medios informáticos (magnéticos – ópticos). -Métodos y normas a seguir en cuestión de salvaguarda y control de los recursos físicos y lógicos de un sistema informático. Desarrollo, manejo e implementación de proyectos informáticos - Ataques a sistemas informáticos, tanto internos como externos de personas, empresas o de la Administración Pública. - Delitos económicos o societarios, como estafas, fraudes, alteración de precios, etc. usando medios electrónicos. - Despido de personal a causa de la introducción de tecnologías de la información. - Uso de programas ocultos como son los caballos de Troya, los backdoors, los rootkits. - Uso ilegal o abusivo de sistemas informáticos.
INTIMIDAD, PRIVACIDAD	- Aspectos laborales vinculados con la informática. - Uso de Internet en el trabajo, uso indebido de las facilidades de la organización otorgadas a los empleados (servicio de correo electrónico, acceso a la navegación por Internet, uso de computadoras, entre otros elementos).

	-Robos o determinación de identidad a través de correos electrónicos. -Apropiación y difusión de datos o información reservada. - Protección de datos personales y de datos reservados de personas jurídicas. - Robo de datos bancarios, por ejemplo, mediante phising. - Robo de identidad o falsificación por medios electrónicos. - Robo de información personal, por ejemplo, mediante keyloggers. - Vulneración de la intimidad mediante lectura del correo electrónico privado.
SERVICIOS	-Contratos en los que la informática se encuentre involucrada (contratación de servicios, adquisición de equipamiento informático y de sistemas, tercerización de servicios). -Aspectos vinculados al comercio electrónico y operaciones realizadas a través de Internet. - Acceso o copia de ficheros de empresa con planos, fórmulas, costes, precios, datos de clientes. -Acoso a través de las redes sociales, como Facefook, Twitter o Tuenti, o por medios electrónicos, por ejemplo, por correo electrónico o SMS. -Delitos contra el mercado o contra los consumidores. Vulneración de la buena fe contractual existiendo documentos electrónicos.
DISPOSITIVOS	- Dispositivos de telefonía celular. - Sabotaje y daños por destrucción de hardware o alteración de datos. - Valoración de bienes informáticos, tanto hardware como software.

*Hashing: Técnica para la generación de direcciones dentro de una estructura de datos, por ejemplo, una tabla o un fichero, a partir de una clave. Se realiza mediante una función, llamada función hash, que a partir de la clave retorna una posición en la estructura. Si es en inserción y esa posición está libre se inserta en esa posición y si no lo está se inserta en la siguiente posición libre. Si es en búsqueda y en esa posición está el elemento buscado se retorna y si no está el elemento se busca en las siguientes posiciones de forma secuencial hasta que aparece o se encuentra una posición libre que quiere decir que lo buscado no está en la estructura. A veces, en vez de búsquedas secuenciales a partir de posición retornada por la función hash,

se vuelve a aplicar la función hash pasándole como parámetro adicional en número de intento. Existen diversos métodos de definir las funciones hash, su mayoría basados en distribuciones aleatorias uniformes de claves, con objeto de reducir al mínimo el número de colisiones. | Alias: Hash; Tabla hash | Bibliografía: Salmerón, A.; et ál.; 1996

Elaboración: Juan José Páez Rivadeneira.

CASOS.

1.- Radiografía a los Correos Electrónicos, ¿qué esconden?.

Últimamente procedente de las noticias proporcionadas por los medios de comunicaciones estamos recibiendo mucha información referente a tramas delictivas de las cuales parte principal de la investigación son las pruebas en correos electrónicos o bien se puede seguir su curso o el nivel de implicación de los acusados por medio de los mismos que se generaron y enviaron con motivo de las conversaciones y diálogos electrónicos mantenidos.

Al mismo tiempo, nos invaden con noticias contradictorias sobre la validez o invalidez, sobre la aceptación o impugnación de correos electrónicos como pruebas en las diferentes causas, desde esta perspectiva, quizás, ha llegado el momento de preguntarnos cómo debemos proceder ante una prueba o evidencia de un correo electrónico.

La consigna es muy clara en dos vías diferentes de actuación:

▪ **No se debe aceptar jamás en un proceso un correo electrónico que os perjudique y del que tengáis sospechas que éste sólo se presenta en papel.** El papel es muy fácilmente manipulable. Solicitad y hacer un peritaje del mismo para analizar la versión electrónica, puede que no la tengan o que en el análisis forense se descubran cosas interesantes a vuestro favor. Evidentemente si se tiene la certeza que es cierto el correo y que hay versión electrónica del mismo no hay lugar a realizar un peritaje, porque le estaríamos produciendo el beneficio a la otra parte.

▪ **Si presentas un correo electrónico importante o especialmente vinculante,** presentad la versión en papel porque es la más práctica de manejar pero, al mismo tiempo, **presentad el correo en versión electrónica y certificada su autenticidad por un perito,** evitando así que el correo pueda ser rechazado o impugnado por la parte contraria.

(Ver Anexo 42)

Se ha de ser consciente que los correos electrónicos incorporan elementos que no son visibles para el usuario convencional y que quedan ocultos o escondidos y que podrían aportar información significativa la cual se puede clasificar en tres áreas de análisis diferenciadas:

▪ **El Flujo:** Información obtenible sobre quienes participan (emisores y receptores), cómo se detectan los destinatarios ocultos, qué información se puede obtener del correo en el puesto emisor y en el receptor, cómo se identifican las máquinas y servidores por los cuales ha pasado el correo, cómo geo-localizar los servidores.

▪ **El Mensaje:** Cuál era el texto original, manipulaciones detectadas, en qué punto de la transmisión ha podido ser manipulado, verificar la coherencia temporal de los mensajes.

▪ **El Contenido:** Ficheros adjuntos, virus camuflados, direccionamientos intencionados, listas ocultas.

Un informe pericial sobre un correo electrónico permitiría actuar en contra de los correos de la otra parte demostrando su falsedad o revelando sus debilidades y, al mismo tiempo, actuar a favor de los correos electrónicos propios reforzando su validez probatoria con su autenticidad contrastada evitando sean rechazados o impugnados por la otra parte.* Fuente: Publicado el 28/05/2013 de Rafael_L_R.

2.- Dirección IP, la huella digital telemática del criminal.

A raíz de un debate y una noticia de un colega, llegó hasta mis manos la Sentencia de Tribunal Supremo STS 8316/2012 en la cual se

absuelven a dos acusados por delitos de estafa realizada por medios telemáticos. Lo interesante de esta sentencia desde el punto de vista de peritaje informático es que se pone en clara duda que el hecho de que se pueda relacionar una operación fraudulenta a una dirección IP, por ello el propietario o usuario asignado a la misma deba ser inequívocamente el delincuente y autor de la operación.

Esta relación unívoca aparentemente rotunda entre la dirección IP y el usuario de la misma, puede presentar dudas razonables sobre la veracidad y certeza a la hora de imputar la culpabilidad a un individuo (el propietario del dispositivo). Para establecer esta duda razonable sería necesario actuar en dos frentes en paralelo, por un lado en el aspecto tecnológico, por el otro lado, en el perfil y los aspectos circunstanciales del propio individuo.

Considerando los aspectos meramente tecnológicos, se ha de ser consciente que los delincuentes cibernéticos poseen un repertorio de herramientas y métodos para hacerse con la identificación y el uso de direcciones IP de terceros y operar a través de ellas, tales como:

- Sistemas Desactualizados o no protegidos.
- Puertos accesibles, vulnerabilidades del Sistema.
- Redes Wifis abiertas o protecciones WAP o WEP poco seguras.
- Malwares, Troyanos, backdoors, botnets, etc.

Por lo tanto para poder establecer una duda razonable sobre el propietario de la IP como presunto delincuente, se ha de analizar el PC y los dispositivos en búsqueda de estas vulnerabilidades que permitirían al ciberdelincuente la usurpación y utilización ilegítima de la dirección IP para cometer el delito.

(Ver Anexo 43)

Considerando el perfil y los aspectos circunstanciales del individuo acusado y para ello se ha de focalizar en encontrar evidencias de:

- Ausencia de lucro personal en la operación, por lo tanto ausencia de dolo respecto al acusado. Normalmente de hecho ni tan siquiera

sospecha que se han realizado transacciones económicas desde su equipo.

- La no posesión de conocimientos técnicos necesarios e imprescindibles para obtener claves bancarias y con ello la posibilidad de ejecución de la estafa.
- El no hallazgo de indicios de realización de la operación en el examen del equipo personal del individuo.

Ninguno de estos elementos (ni técnicos ni circunstanciales) por sí mismos son determinantes para el establecimiento de la duda razonable sobre la culpabilidad del individuo, pero trabajando todas estas posibilidades desde un punto global de conjunto se puede evidenciar más allá de la duda razonable si el presunto culpable propietario de la dirección IP involucrada, es realmente un delincuente, o lo que cabría esperar, una víctima más de la estafa.

Así pues desde el punto de vista del informe pericial y de la defensa del individuo se ha de considerar las posibles vías expuestas. (IBIDEM).

3.- Facebook y las evidencias electrónicas en delitos de injurias, calumnias y otros.

Facebook es una red social en la que se establecen relaciones personales y vínculos entre las personas (usuarios de Facebook) compartiendo material e información cotidiana de los mismos y, en algunas ocasiones, informaciones de contenido de carácter personal y sensible como podrían llegar a ser: reflexiones, pensamientos o material gráfico y visual.

Esta es la razón por la que Facebook como red social está enfocada a preservar la privacidad de la información por medio de la conjugación de dos parámetros básicos gestionados por el usuario:

- **Nivel de Publicidad:**_Definiendo en qué ámbito el usuario que publica hace visible una publicación, es decir, el alcance de nivel de relación el cual puede acceder a la misma.

- **Nivel de Relación:** Definiendo para cada usuario cuál es el nivel de relación designado y, por lo tanto, cuál es el nivel de visualización permitido.

Es el propio usuario propietario de la cuenta de Facebook en la cual se publica la información quien, por medio de las diferentes opciones que proporciona Facebook, puede realizar la gestión particularizada tanto en la creación de subgrupos de usuarios como en la gestión de un usuario en particular.

Los usuarios pueden ser invitados a establecer una relación en Facebook, y tras ser aceptados, pueden ser borrados o bloqueados como medidas de anulación del permiso o acceso a los contenidos del usuario propietario de la cuenta.

Al ser un medio de expresión personal y abierto al público o a un grupo selecto del mismo, es posible que se produzcan por medio del material publicado delitos contra el honor como las calumnias o injurias (los más comunes) o de otra índole como el enaltecimiento del terrorismo, o contra la propiedad intelectual, etc.

Es muy importante establecer los niveles de Publicación y de Relación para acotar claramente el alcance de lo publicado y ser consciente de dónde termina lo privado para convertirse en público.

En el siguiente esquema se muestran los diferentes niveles de Publicación y niveles de Relación que se vinculan para hacer visible la información publicada.

(Ver Anexo 44)

Consecuentemente, a la hora de recopilar las evidencias necesarias y que éstas no sean invalidadas se ha de tener en cuenta por parte del perito las siguientes consideraciones:

- Validar la legitimidad del usuario actuante con el que se está accediendo a la captura de la evidencia determinando de forma fehacientemente su identificación personal y usuario de Facebook.

- Obtener la autorización explícita para la realización de la captura de las evidencias en nombre del usuario actuante.
- Establecer el nivel de relación existente entre el usuario actuante que captura la información y el usuario que la ha publicado.
- Establecer el nivel de publicidad que se ha establecido a la publicación.
- Validación de la coherencia de los niveles de Relación y de Publicación con el hecho que se desea constatar.
- Llevar a cabo la identificación, registro y preservación de las evidencias electrónicas según las buenas prácticas profesionales y los protocolos establecidos.

Asimismo, es importante la preservación de la integridad de la evidencia y la cadena de custodia hasta su entrega e inclusión en el procedimiento judicial, ya que es del todo punto necesario garantizar la posibilidad de la aplicación posterior del principio de contradicción.

Dada la volatilidad de la información y de las relaciones establecidas en Facebook, puesto que pueden ser cambiadas o desaparecer en cualquier momento posterior a la captura por quien publica y gestiona la información, se recomienda realizar la captura de las evidencias bajo protocolo notarial.

No obstante, el fedatario público no ha de ser conocedor de las validaciones necesarias de legitimidad o de relación establecidas existentes y que son vinculantes y especialmente significativas para el contexto del caso. Estos conocimientos deben formar parte del bagaje y del saber del profesional perito. El fedatario público únicamente va a constatar en la diligencia presencial aquello que puede ver en la pantalla o que se puede capturar impreso para su incorporación en el acta que proporcionará soporte documental al informe pericial.

Consecuentemente, es responsabilidad del profesional perito que captura las evidencias el realizar las actuaciones de modo que una vez llevadas a cabo no se pueda impugnar las evidencias.

El incumplimiento de cualquiera de estas premisas comentadas, podría llegar a permitir el impugnar las evidencias presentadas y, con ello, la pérdida de las pruebas que soportan el caso.

4.- Localización y posicionamiento por medio de llamadas telefónicas. Peritaje Informático Tecnológico.

En los últimos meses he tenido la oportunidad de trabajar en varias causas y expedientes, los cuales se basaban en la localización y posicionamiento del individuo en base a ser captado por una o varias antenas de telefonía móvil y por medio de las llamadas de entrada recibidas o de salida realizadas.

Existe un gran desconocimiento en esta temática que hace que, en muchas ocasiones, se tome como dogma de fe el dictamen, la determinación o aquello que quede plasmado en las diligencias y en los informes y, con ello, ante la falta de una contradicción técnica cualificada sobre la temática, esta manifestación ya es suficiente para que quede presuntamente demostrada la localización y el posicionamiento del individuo sin que exista una posibilidad real de defensa.

De hecho, principalmente, ésta ha sido mi labor en estos expedientes, el demostrar que las presunciones que se han considerado no han sido del todo correctas o estaban poco oinsuficiente argumentadas y, consecuente, el resultado obtenido no es válido ni concluyente para el posicionamiento o la localización del individuo o bien, todo lo contrario, con la información recibida y analizada se ha podido "afinar" más si cabe sobre la localización y su posicionamiento real y, con ello, evaluar si lo presentado con anterioridad era o no correcto o coincidente con el resultado obtenido.

Normalmente, se parte de la idea simple que si una antena de telefonía establece comunicación con un teléfono a través de una llamada, este teléfono se encuentra en un radio aproximado de 1 Km de la estación emisora/receptora.

Esta presunción es totalmente inexacta puesto que, de ser así, el mapa geográfico debería estar dividido en paneles hexagonales regulares en los cuales hubiese una antena en el centro del hexágono y existiese 2 Km de distancia entre los centros los mismos, esta visión idílica es mera teoría y se ha de considerar como una idea simplificada para explicar el funcionamiento para los legos en la materia, pero no sirve como argumento técnico para basar una localización o posicionamiento en base a ello.

(Ver Anexo 45)

Para que nos hagamos a la idea de algunos de los aspectos que intervienen serían los siguientes:

- Características del tipo de llamada.
- Características de la antena / estaciones.
- Características de gestión de la comunicación.
- Características del entorno físico.
- Características de la dinámica de la acción.

Tal y como se puede apreciar, para realizar un estudio adecuado se han de considerar demasiados elementos como para concluir con una aproximación simplista por el mero hecho de que una antena o estación de telefonía haya captado una señal, de que el individuo se encuentra a menos de 1 Km de la misma o, lo que sería más grave aún, contando simplemente con esta evidencia intentar demostrar dónde estaba el individuo y llegar a afirmar que *"... estaba en el bar de PEPE..."*

Asimismo, ante este tipo de situaciones se ha de reaccionar con la máxima celeridad, lo antes posible, para que no se pierda la información que depende de los operadores de telefonía y, por supuesto, no dudar en contactar con peritos informático y tecnológicos expertos que sean capaces de trabajar con estos elementos, al fin y al cabo, ésta es nuestra labor, pero somos quienes pueden dar validez o rechazar una evidencia de este tipo y poder establecer, según sea el caso, la determinación, defensión y contradicción necesaria.* Fuente: http://peritoit.com/

5.- El tratamiento de la calidad de imágenes para procesos judiciales.

En los casos en los cuales es necesario el tratamiento de imágenes de video o fotografías para obtener una mayor nitidez de las mismas o bien una mejor comprensión visual que permita la identificación de objetos, individuos, escenarios o hechos, siempre se plantea el dilema de hasta dónde se puede llegar en las actuaciones técnicas sin tergiversar o distorsionar la realidad.

Es comúnmente conocido que existen potentes herramientas que permiten cambiar muchos parámetros y características a las imágenes, aplicar filtros y disponer cambios por medio de capas superpuestas que permiten con, una relativa rapidez, trabajar sobre las imágenes tratadas.

Desde el punto de vista pericial, a la hora de realizar el tratamiento de las imágenes siempre se busca la forma de proporcionar una mayor nitidez a las imágenes en su globalidad o bien en algún detalle en concreto y, en ocasiones, la aplicación de una "mejora" proporciona el detalle revelador que se estaba buscando.

Este efecto se puede conseguir por medio de diferentes técnicas:

Con la intensificación o la anulación de la luz y las sombras, el tono de color.

(Ver Anexo 46)
(Ver Anexo 47)

Con la variación del brillo y el contraste

(Ver Anexo 48)

El problema no se plantea cuando se está simplemente mejorando la "visualización" de la imagen sino cuando se está cambiando la

información de la propia imagen de tal modo que se está modificando la propia evidencia.

El punto de partida para determinar en qué proceso se está, concepto éste que no se puede perder de vista en estas situaciones, es el tener presente en todo momento cuál es la resolución de la imagen original y no olvidar nunca que ésta siempre depende de dos elementos básicos:

- La resolución del dispositivo con el cual se ha obtenido ópticamente la imagen.
- La resolución del dispositivo, medio o software con el que se ha transformado esa imagen en un fichero.

La imagen que se obtenga siempre tendrá la menor resolución de los dos parámetros anteriores y cualquier nivel de resolución diferente que se le proporcione se está modificando la propia imagen e información original contenida.

A partir de la fijación de esta premisa del nivel de resolución original de la imagen, un nivel de resolución mayor o menor siempre se obtiene por una transformación e interpretación por medio de software de la información original, a este proceso se le denomina "interpolación", y éste no deja de ser la utilización de estimaciones matemáticas y de aproximaciones de lo que pudiera ser, que no quiere decir que sea.

Por ejemplo, en la figura que se muestra puedo aumentar el nivel de píxeles de un cuadrado de 4 píxeles a 16, la herramienta por medio de a interpolación calcula la transición más suave entre los diferentes cuadrados considerando el gradiente de color en cada sentido, o bien la operación contraria, pasa de 16 píxeles a 4 píxeles reduciendo el "peso" de la imagen eliminando los píxeles intermedios.

(Ver Anexo 49)

Tal y como se puede observar, tanto en una operación como en la inversa, se está cambiando la información de origen y es la evaluación del resultado obtenido frente a este nivel de transformación realizado

el que se debe considerar para determinar hasta qué punto se ha mejorado la imagen o bien ésta ha sido modificada (manipulada no correspondiéndose fidedignamente con la información original), por suerte para el perito, esta última decisión no es una actividad que le competa, ya que es labor de los juzgadores.

En cualquier caso, el perito ha de tomar conciencia no sólo de qué es técnicamente correcto, sino también de qué es lo que está proporcionando como evidencia tras el proceso, no cayendo en interpretaciones personales que pudieran dar resultados diferentes según el individuo como, por ejemplo, ocurre en el conocido test de manchas de Rorschach

(Ver Anexo 50)

o con las imágenes de humo en las cuales cada individuo puede identificar y reconocer una imagen diferente en cada una de las formas o volutas de humo según su propia subjetividad y estado de ánimo del momento en el que lo interpreta.

(Ver Anexo 51)

La imaginación posee un alto nivel de convicción, ¿quién no ve un rostro humano en esta ecografía?

(Ver Anexo 52)

Asimismo, tampoco se puede caer en el error de pensar que todo lo que se muestra en las series televisivas sobre las "supercapacidades" de los técnicos es cierto y veraz, piensen de forma objetiva en lo que se ha comentado de la capacidad técnica del dispositivo de captura original de la imagen y del volumen de información que debería guardar este dispositivo para poder permitir el nivel de nitidez o de zoom que en ocasiones se necesita para la investigación.

El siguiente enlace proporciona acceso a un video del tratamiento de imagen en un capítulo de la serie CSI, www.youtube.com/watch?v=z9d0QLtGd7k

MEDIOS DE PRUEBA ELECTRÓNICA.

Desde que se puso en vigencia la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, (Ley No. 2002-67) en el Título IV. Se estableció la forma de como evacuar la prueba electrónica en los procesos judiciales.

Recordemos que este análisis ya lo hicimos en el tema correspondiente a la validez de jurídica de los mensajes de datos o documentos electrónicos.

Los medios de prueba electrónica, que establece esta ley son los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la Ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.

La prueba se practicará de conformidad con lo previsto en el Código de Procedimiento Civil y observando las normas siguientes:

a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos;
b) En el caso de impugnación del certificado o de la firma electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de firma electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados;

c) El faxcímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta ley.

En caso de que alguna de las partes niegue la validez de un mensaje de datos, deberá probar, conforme a la Ley, que éste adolece de uno o varios vicios que lo invalidan, o que el procedimiento de seguridad, incluyendo los datos de creación y los medios utilizados para verificar la firma, no puedan ser reconocidos técnicamente como seguros.

Cualquier duda sobre la validez podrá ser objeto de comprobación técnica.

La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectué con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

Para la valoración de las pruebas, el juez o árbitro competente que conozca el caso deberá designar los peritos que considere necesarios para el análisis y estudio técnico y tecnológico de las pruebas presentadas.

Todo el que fuere parte de un procedimiento judicial, designará el lugar en que ha de ser notificado, que no puede ser otro que el casillero judicial y/o el domicilio judicial electrónico en un correo electrónico, de un Abogado legalmente inscrito, en cualquiera de los Colegios de Abogados del Ecuador.

Las notificaciones a los representantes de las personas jurídicas del sector público y a los funcionarios del Ministerio Público que deben intervenir en los juicios, se harán en las oficinas que estos tuvieren o en el domicilio judicial electrónico en un correo electrónico que señalaren para el efecto.

PRINCIPIO	NORMA LEGAL
PRINCIPIO DE EQUIVALENCIA FUNCIONAL, basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer los objetivos y funciones del comercio telemático, es decir es *la función jurídica que cumple la instrumentación escrita y autógrafa respecto a todo acto jurídico, o su expresión oral, la cumple de igual forma la instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, extensión, alcance y finalidad del acto así instrumentado*". En otras palabras la equivalencia funcional permite aplicar a los soportes informáticos un principio de no discriminación respecto de las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas: los mismos efectos que surte la manifestación de la voluntad instrumentada a través de un documento en papel, deben producirse independientemente del soporte utilizado en su materialización.	**Artículo 2.- Reconocimiento jurídico de los mensajes de datos.-** Los mensajes de datos tendrá igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.
Mensajes de Datos como medio de prueba: procedimiento que establece la Ley para ingresar un elemento de prueba en el proceso	Artículo 53.- Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil.

PRINCIPIO	NORMA LEGAL
VALIDEZ DE LAS ACTUACIONES PROCESALES POR MEDIO DELAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN: Esta disposición del Código Orgánico de la Función Judicial ratifica el principio de equivalencia funcional existente en la Ley de Comercio Electrónico. Las características esenciales del mensaje de datos son: Es una prueba de la existencia y naturaleza de la voluntad de las partes de comprometerse; Es un documento legible que puede ser presentado ante las Entidades públicas y los Tribunales;	**Art. 147.- VALIDEZ Y EFICACIA DE LOS DOCUMENTOS ELECTRÓNICOS.**- Tendrán la validez y eficacia de un documento físico original los archivos de documentos, mensajes, imágenes, bancos de datos y toda aplicación almacenada o transmitida por medios electrónicos, informáticos, magnéticos, ópticos, telemáticos, satelitales o producidos por nuevas tecnologías, destinadas a la tramitación judicial. Ya sea que contengan actos o resoluciones judiciales. Igualmente los reconocimientos de firmas en documentos o la identificación de nombre de usuario, contraseñas, claves, utilizados para acceder a redes informáticas. Todo lo cual, siempre que cumplan con los procedimientos establecidos en las leyes de la materia. Las alteraciones que afecten la autenticidad o integridad de dichos soportes les harán perder el valor jurídico que se les otorga en el inciso anterior, sin perjuicio de la responsabilidad penal en caso de que constituyan infracción de esta clase. Todas las disposiciones legales que, sobre la validez y eficacia en juicio de los documentos que se hallan contenidas en el Código Civil, Código de Procedimiento Civil, Código de Procedimiento Penal, Ley de la Jurisdicción Contencioso Administrativa, Código Tributario y otros cuerpos legales, se interpretarán de conformidad con esta norma, salvo los casos de los actos y contratos en que la ley exige de la solemnidad del instrumento público, en que se estará a lo prevenido por el artículo 1718 del Código Civil. Cuando una jueza o juez utilice los medios indicados en el primer párrafo de este artículo, para consignar sus actos o

PRINCIPIO	NORMA LEGAL
	resoluciones, los medios de protección del sistema resultan suficientes para acreditar la autenticidad, aunque no se impriman en papel ni sean firmados, pero deberán ser agregados en soporte material al proceso o archivo por el actuario de la unidad. Las autoridades judiciales podrán utilizar los medios referidos para comunicarse oficialmente entre sí, remitiéndose informes, comisiones y cualquier otra documentación. El Consejo de la Judicatura dictará los reglamentos necesarios para normar el envío, recepción, trámite y almacenamiento de los citados medios; para garantizar su seguridad, autenticidad e integridad; así como para posibilitar el acceso del público a la información contenida en las bases de datos, conforme a la ley.
Admite su almacenamiento e inalterabilidad en el tiempo; facilita la revisión y posterior auditoria para los fines contables, impositivos y reglamentarios; afirma derechos y obligaciones jurídicas entre los intervinientes y, Es accesible para su ulterior consulta, es decir, que la información en forma de datos computarizados es susceptible de leerse e interpretarse.	

Sobre la eficacia probatoria propia de los documentos Electrónicos, el autor Ab. Juan Carlos Riofrío Martínez, en: "EFICACIA PROBATORIA DE LOS DOCUMENTOS ELECTRÓNICOS", manifiesta que ha sido enriquecida, concretada y fortalecida por la LCE de lasiguiente forma:

1.- Ha quedado consagrado legalmente el principio de la eficacia natural probatoria de los medios de prueba electrónicos (artículo52).
2.- Se otorga la misma aptitud probatoria de los documentos originales a todo mensaje de datos cuya integridad pueda comprobarse (Artículo 7).
3. Tales mensajes tienen igual valor jurídico que los documentos escritos (Artículo 2). En otras palabras, cuando la ley requiera adsubstantiam, ad probationem o ad solemnitatem que un acto jurídico determinado deba realizarse por escrito, este requisito se considerará cumplido cuando la información conste en forma de mensaje de datos.

Sin embargo, la LCE no puede obviar la realidad natural del documento electrónico, que adolece de una escasa corporalidad, y tiene que acotar que «su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento» (artículo 2).

4. «Se reconoce la validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes» (artículo 3).

Se resalta que el hipervínculo del que se habla deberá ser «directo», lo que tiene importantes repercusiones prácticas. Cuando aceptamos un mensaje de datos, aceptamos el texto que aparece en la pantalla (T1) y también el texto que no aparece (T2) pero al que nos remite el hipervínculo constante en TI Si en T2 existen otros hipervínculos que nos remiten a otros lados (T3), todo lo contenido en T3 no nos obliga, ni se presume que lo conocemos, porque los hipervínculos de T2 no son «directos».

Pero se ha de aclarar que por aceptar un Tl, no se acepta tácitamente todo T2, sino solamente aquel T2 que sea «conocido y aceptado expresamente por las partes». Naturalmente sólo podemos aceptar lo que conocemos, y solamente conocemos un documento cuando lo leemos. Por eso, la doctrina recomienda incluir junto al botón de aceptación de los contratos click, una leyenda que diga:

«Acepto, conozco y me obligo al texto anterior y a lo contenido en los hipervínculos que ahí aparecen».

5. La LCE ha fortalecido sustancialmente la eficacia probatoria de los documentos firmados digitalmente con un certificado expedido por una entidad autorizada, hasta darles un valor similar al de un instrumento reconocido'. Los artículos 10 y 53 de la Ley presumen válidos estos documentos, " mientras no se pruebe lo contrario".

Se ha trasladado la carga de la prueba: antes, quien debía demostrar la validez y autenticidad de un documento electrónico digitalmente firmado era quien lo aportaba; hoy se presume válido mientras la contraparte no compruebe que dicho documento «adolece de uno o varios vicios que lo invalida, o que el procedimiento de seguridad además, el legislador ha querido incrementar la confianza pública en la firma electrónica certificada, imponiendo la obligación de guardar bajo secreto la clave personal de la propia firma electrónica. Cuando hay este deber de secreto, es más fácil admitir que el que firmó un documento sólo pudo ser el propietario de la firma. De no existir este deber de custodia y confidencialidad, fácilmente el propietario de una firma digital podría alegar que un tercero se apoderó de su clave personal y firmó por él diversos documentos, sin mayores inconvenientes.

Nuestra LCE incluso responsabiliza al titular de la firma electrónica «por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia, para impedir su utilización, salvo que el destinatario conociere de la inseguridad de !a firma electrónica o no hubiere actuado con la debida diligencia.»

También existen importantes presunciones acerca del tiempo y lugar de emisión y recepción del mensaje de datos, para valorar la prueba el juez «deberá designar peritos que considere necesarios, Art.44, a fin de un mejor análisis de la seguridad y fiabilidad del documento electrónico. Ésta exigencia de nombrar peritos Art. 45 cesa en tres casos:

a) Cuando el juez estimare que la prueba aportada es impertinente, ineficaz o inadmisible, por razones de economía procesal o por evitar una colisión de derechos.
b) Cuando se considerare que la fiabilidad del documento no está cuestionada (v. gr. cuando la contraparte ha reconocido la autoría de un correo electrónico 46). En tal caso la pericia sería inadmitida por superficial.
c) Cuando el documento electrónico aportado contenga una firma digital autorizada, por cuanto se presume su validez según lo dispuesto en el artículo 10 y 53 de la LCE. No obstante, si alguien quisiera desvirtuar esa presunción, entonces sí se deberán nombrar los peritos que comprueben su validez.

En estos casos, no habiendo lugar a la designación de los peritos, el juzgador puede pasar directamente a valorar la prueba. Pero si debiendo nombrarlos no lo hizo, siempre queda al juez darle a las pruebas producidas el valor de meros indicios probatorios, y, a la luz de la «sana crítica», aumentarles o restarles su eficacia, según concuerden o no con el conjunto de pruebas aportadas al proceso.

*Fuente: http://www.revistajuridicaonline.com/index.php?option=com_content&task=view&id=155&Itemid=71

NUEVO PROCEDIMIENTO PENAL.-

Con la implementación del Código Orgánico Integral Penal, se han incorporado nuevos procedimientos penales, especiales, relacionando la gravedad de las infracciones, con las sanciones penales, se han creado juicios penales directos y expeditos, con el objetivo de lograr procesos ágiles, eficientes, bajo los principios constitucionales del debido proceso y tutela judicial.

En este Código, se reconocen tres tipos de procedimientos penales, tipificados en los Artículos 580 (ordinario), 634 (procedimientos especiales), y 647 (procedimiento para el ejercicio privado de la acción penal).

El primer procedimiento, el ordinario, establecido para las causas que se inician mediante formulación de cargos, en donde se establecen tres etapas:

1.- Instrucción fiscal; 2.- Evaluación y preparatoria de juicio, y 3.- Etapa del Juicio.

El segundo, procedimientos especiales, tenemos cuatro tipos:

1.- Abreviado, para los delitos sancionados hasta con diez años de pena privativa de la libertad, la que no podrá exceder de la acordada entre el fiscal y el procesado, se la puede presentar desde la formulación de cargos hasta la evaluación y preparatoria del Juicio.

2.- Directo, para delitos sancionados hasta con cinco años e iniciados mediante audiencia de flagrancia.

3.- Expedito, para las contravenciones penales. Y,

4.- Expedito para contravenciones de tránsito.

El tercer procedimiento, el ejercicio privado de la acción penal, es para tramitar las causas que se originan mediante querella y es un trámite especial, en el que consta citación al querellado, contestación, audiencia de conciliación y sentencia. Requiere el impulso del ofendido.

Procedimiento Abreviado y sus características.

El Procedimiento Abreviado se encuentra en los artículos 635, 636, 637, 638 y 639.

La anterior norma adjetiva ya contenía el Procedimiento Abreviado, sin embargo, existen algunos cambios significativos, por ejemplo, antes, la aplicación del procedimiento abreviado procedía en todos los delitos o tentativa, siempre y cuando la pena privativa de libertad sea hasta cinco años, mientras que ahora, con el COIP, se amplía, por cuanto, la aplicación de este procedimiento procede en todas las infracciones sancionadas con una pena privativa de la libertad de hasta diez años.

Las reglas para la aplicación del procedimiento abreviado son:

- Es aplicable en aquellas infracciones sancionadas con pena privativa de libertad de hasta diez años.

- El fiscal es quien debe presentar la propuesta de aplicación del Procedimiento Abreviado.

- La aplicación de este procedimiento puede realizarse desde la audiencia de formulación de cargos hasta la audiencia de evaluación y preparatoria de juicio.

- Constituye una condición fundamental la aceptación del hecho de forma libre y voluntaria, así como la aplicación de este procedimiento sin presión de ninguna naturaleza hacia el procesado, situación que deberá ser acreditado por el defensor público o su defensor particular.
- Pueden existir varios procesados y no constituye un obstáculo para la aplicación de este procedimiento.

- La pena acordada en ningún caso será superior o más grave a la que fuere sugerida por el fiscal.

Trámite del Procedimiento Abreviado.

El trámite a seguirse para la aplicación del procedimiento abreviado, se resume en lo siguiente:

El fiscal es el que plantea la aplicación del procedimiento abreviado tanto al procesado como a su abogado defensor, aceptado que sea, se procederá con el acuerdo sobre la calificación jurídica del hecho punible y la pena. Esta última, será el resultado del análisis de los hechos imputados y aceptados, para lo cual se tomará en cuenta la aplicación de las circunstancias atenuantes conforme lo prevé el COIP. La rebaja no podrá ser menor al tercio de la pena mínima prevista en el tipo penal.

En este proceso el defensor del procesado tiene la obligación ineludible de explicar de forma clara y sencilla, en términos entendibles en que consiste este procedimiento y las consecuencias de aceptarlo.

El fiscal solicitará al juzgador competente en forma escrita u oral, el sometimiento del procesado a este procedimiento abreviado, acreditando los requisitos que se han expuesto, así como la determinación de la pena reducida que se hubiere acordado. Si la petición se presenta en forma oral en una de esas audiencias, se sustanciará en la misma sin más dilaciones este procedimiento abreviado.

En la Audiencia, el juez competente para conocer y tramitar este procedimiento es el juez de garantías penales, conforme lo prescrito en el artículo 225.5 del Código Orgánico de la Función Judicial.

Recibida la solicitud del fiscal, el juez de garantías penales, convocará a audiencia oral y pública, a los sujetos procesales dentro de las 24 horas siguientes. En esta diligencia se definirá si se acepta o se rechaza este procedimiento.

Al ser aceptada se instalará en forma inmediata la audiencia y se dictará sentencia condenatoria. Cabe resaltar, que en esta audiencia el o la juez escuchará al fiscal y consultará obligatoriamente al procesado su conformidad con este procedimiento y todas las consecuencias que la aceptación le representará.

De la misma forma, la víctima podrá asistir a la audiencia y tendrá derecho a ser escuchada. En seguida el juzgador concederá la palabra al fiscal para que presente los hechos de la investigación y la fundamentación jurídica, para luego conceder la palabra al procesado, quien deberá manifestar expresamente su aceptación al procedimiento. Concluida que sea la audiencia, el juzgador dictará su resolución que incluirá la aceptación del acuerdo sobre la calificación del hecho punible, la pena solicitada por el fiscal bajo el principio de no agravar la pedida por el fiscal, y la reparación integral de la víctima, de ser el caso.

Procedimiento Expedito.

Este procedimiento es aplicable para tres tipos de contravenciones:

- Contravenciones penales.

- Contravenciones de tránsito.

- Contravenciones contra la mujer o miembros del núcleo familiar.

En lo referente a las contravenciones penales y de tránsito, se puede decir que la particularidad es que la situación se resolverá en una sola audiencia, donde víctima y el denunciado, en primer lugar, podrán lograr la conciliación frente al juzgador de contravenciones, excepto en los casos de violencia contra la mujer o miembros del núcleo familiar, sin embargo, en los demás casos en que se llegare a conciliar harán conocer el acuerdo al que han llegado para que el juzgador ponga fin al proceso, esto es, ordenando el archivo de la causa.

Características del Procedimiento expedito de contravenciones penales. Se aplicarán a petición de parte, por lo que, el juzgador deberá notificar a través de los servidores respectivos al denunciado, fijando día y hora para la audiencia de juzgamiento, señalando la obligación que tiene de ejercer su derecho a la defensa; esta diligencia se realizará en un plazo máximo de diez días, así mismo, hasta tres días antes de la realización de la audiencia, las partes anunciaran las pruebas por escrito, esto siempre que la contravención no sea flagrante, en cuyo caso se sustanciará en la audiencia única, por cuanto, si una persona es sorprendida en delito flagrante de una contravención, será aprehendida y trasladada en forma inmediata ante el juez respectivo para su juzgamiento, diligencia en la que se anunciaran las pruebas.

En caso de ausencia del procesado a la audiencia de juzgamiento, el juez de contravenciones dispondrá la detención, misma que no podrá exceder de las veinte y cuatro horas, esto contribuye al máximo respeto de uno de los derechos consagrados en la Constitución de la República, que nadie puede estar detenido por más de 24h00 sin formula de juicio.

Al concluir la audiencia de juzgamiento, el juez tiene la obligación de dictar la sentencia sea condenatoria o absolutoria, decisión que puede ser apelada ante la Corte Provincial.

Otro elemento que hay que considerar, es que si el juez en el proceso de juzgamiento de la contravención penal, encuentra que el caso sometido a su conocimiento se trata de un delito, éste se abstendrá de conocer y remitirá a la fiscalía para la correspondiente investigación, de la misma forma, el juez se encuentra facultado a rechazar cualquier forma de entorpecer la tramitación de la causa.

PROSPECTIVA TECNOLÓGICA

La prospectiva (proceso) tecnológica es un proceso sistemático que analiza el estado actual y las perspectivas de progreso científico y tecnológico para identificar áreas estratégicas de investigación y tecnologías emergentes en las que concentrar los esfuerzos de inversión y así obtener los mayores beneficios económicos o sociales.

La prospectiva tecnológica están orientadas a un conjunto de técnicas que permiten definir la relevancia de una tecnología en un momento futuro. Una característica principal de la prospectiva es que parte de la existencias de varios posibles futuros (futurables y futuribles) los cuales se enmarcan en un contexto dado, que puede ser bajo la jurisdicción de un país, un sector o una empresa. La finalidad de la prospectiva tecnológica es facilitar la toma de decisiones donde la tecnología constituye un factor cada vez más determinante, y en el que el propio ritmo de cambio tecnológico, cada día más acelerado, incorpora un grado creciente de incertidumbre.

Un análisis de prospectiva tecnológica parte de la identificación del tipo de tecnología que se desea analizar, que habitualmente se engloba en una de las tres categorías siguientes:

Tecnologías claves: son aquellas que tienen un mayor impacto sobre la rentabilidad de los productos o la mejora de la productividad. Su difusión es limitada y su posesión va a condicionar fuertemente la posición competitiva de la empresa.

Tecnologías de base: son tecnologías ampliamente disponibles por las empresas de un mismo sector y suele ser común a todos los productos de una actividad concreta.

Tecnologías emergentes: son aquellas que en una primera fase de su aplicación en la empresa muestran un notable potencial de desarrollo. El nivel de incertidumbre que rodea a estas tecnologías es particularmente elevado.

Esta clasificación está estrechamente relacionada con el concepto de ciclo de vida de la tecnología, donde se distinguen tres etapas: nacimiento, crecimiento y madurez . El nacimiento se asocia a tecnologías emergentes, el crecimiento a tecnologías claves y, finalmente, la madurez y el declive a tecnologías de base.

La prospectiva tecnológica se utiliza dentro de la gestión de la I+D+i para dar apoyo a las decisiones de inversión en tecnología, conjuntamente con la vigilancia tecnológica.

Investigación, desarrollo e innovación (habitualmente indicado por la expresión I+D+i o I+D+I) es un concepto de reciente aparición, en el contexto de los estudios de ciencia, tecnología y sociedad; como superación del anterior concepto de investigación y desarrollo (I+D). Es el corazón de las tecnologías de la información y comunicación.

Mientras que el de desarrollo es un término proveniente del mundo de la economía, los de investigación e innovación provienen respectivamente del mundo de la ciencia y la tecnología, y su dinámica relación se encuentra en el contexto de la diferenciación entre ciencia pura y ciencia aplicada; cualquiera de ellos es de compleja definición. EskoAho define provocativamente investigación como invertir dinero para obtener conocimiento, mientras que innovación sería invertir conocimiento para obtener dinero, lo que expresa muy bien el fenómeno de retroalimentación que se produce con una estrategia exitosa de I+D+i.1.

El nivel de actividad de I+D+i en un país se puede calcular mediante la ratio entre el gasto en I+D+i y el producto interior bruto (PIB),

desglosando el gasto en gasto público y gasto privado (Deducciones fiscales I+D+i).2.

Todos los países procuran, en la medida de sus posibilidades, potenciar las actividades ligadas a la I+D+i a través de políticas de apoyo (subvenciones, deducciones, préstamos bonificados y otras), debido a que un alto nivel de I+D+i implica una mayor fortaleza de los productos o procesos que se diferencian positivamente de los de su competencia. Además, muchas de las actividades son potencialmente generadoras de avances sociales en forma de calidad de vida, mejora del medio ambiente, la salud, etc. Para apoyar esas actividades existe un conjunto de normas UNE: la serie UNE 166000, que incluye la norma UNE 166001, dirigida a los proyectos de I+D+i, la UNE 166002 sobre requisitos del sistema de gestión de la I+D+i y la UNE 166006 relativa a requisitos sobre el sistema de vigilancia tecnológica.

La serie UNE 166000 es un conjunto de normas UNE dedicadas a apoyar la optimización de la gestión de la I+D+i.

Se compone de las siguientes normas:

UNE 166000, que establece las definiciones y terminología utilizadas en el resto de las normas.

UNE 166001, que establece los requisitos para los proyectos de I+D+i.

UNE 166002, que determina los requisitos que debe cumplir el sistema de gestión de la I+D+i.

UNE 166003 (ANULADA), que establece los criterios de competencia y evaluación de los auditores de proyectos de I+D+i.
UNE 166004 (ANULADA), que establece los criterios de competencia y evaluación de los auditores de sistemas de I+D+i.

UNE 166005, que es una guía de aplicación de la UNE 166002 a los bienes de equipo.

UNE 166006, que establece las características y requisitos de un sistema de vigilancia tecnológica e inteligencia competitiva.

UNE 166007, que es una guía de aplicación de la norma UNE 166002.
UNE 166008, que establece los requisitos para la transferencia de tecnología (activos intangibles).

Las normas de la familia UNE 166000 están alineadas con los requisitos de la norma ISO 9001.

Con estas normas se pretende proporcionar directrices para una eficaz planificación, organización, ejecución y control de las actividades de I+D+i, así como facilitar un reconocimiento en el mercado a las organizaciones innovadoras.

Cloud Computing.

El Cloud Computing, también conocido como "Nube", ha sido definido por el NIST (National Institute of Standards and Technology) como un modelo de servicios escalables bajo demanda para la asignación y el consumo de recursos de cómputo. Describe el uso de infraestructura, aplicaciones, información y una serie de servicios compuestos por reservas de recursos de computación, redes, información y almacenamiento. Estos componentes pueden orquestarse, abastecerse, implementarse y liberarse rápidamente, con un mínimo esfuerzo de gestión e interacción por parte del proveedor de Cloud Computing y de acuerdo a las necesidades actuales del cliente.

(Ver Anexo 53)
(Ver Anexo 54)
(Ver Anexo 55)

Modelos de Implementación.

Dependiendo de cómo se despliegan los servicios en la nube, existen cuatro modelos que caracterizan la implementación de los servicios de Cloud Computing.

Nube Pública: Es aquel modelo de Nube en el cual la infraestructura y los recursos lógicos que forman parte del entorno se encuentran disponibles para el público en general o un amplio grupo de usuarios. Suele ser propiedad de un proveedor que gestiona la infraestructura y los servicios ofrecidos. Ejemplo: Servicio de Google Apps.

Nube Privada: Es aquel modelo en el cual la infraestructura se gestiona únicamente por una organización. La administración de aplicaciones y servicios puede estar a cargo de la misma organización o de un tercero. La infraestructura asociada puede estar dentro de la organización o fuera de ella. Ejemplo: Cualquier servicio de nube propio de la organización o contratado a un proveedor pero cuyos recursos sean exclusivos para dicha organización.

Nube Comunitaria: Es aquel modelo donde la infraestructura es compartida por diversas organizaciones y su principal objetivo es soportar a una comunidad específica que posea un conjunto de preocupaciones similares (misión, requisitos de seguridad o de cumplimiento normativo, etc.). Al igual que la Nube Privada, puede ser gestionada por las organizaciones o bien por un tercero y la infraestructura puede estar en las instalaciones propias o fuera de ellas. Ejemplo: El servicio app.goc (www.apps.gov) del gobierno de EEUU, el cual provee servicios de cloudcomputing a las dependencias gubernamentales.

Nube Híbrida: Es aquel modelo donde se combinan dos o más tipos de Nubes (Pública, Privada o Comunitaria) que se mantienen como entidades separadas pero que están unidas por tecnologías estandarizadas o propietarias, que permiten la portabilidad de datos y aplicaciones.

RECOMENDACIONES PARA LA ADOPCIÓN DEL CLOUD COMPUTING.

A continuación compartimos una serie de recomendaciones que sería importante que se tengan en cuenta al momento de evaluar una solución de servicio basado en Cloud Computing:

Llevar a cabo la evaluación de riesgos en el marco de un proyecto integral de la Empresa, involucrando a los referentes claves de las distintas áreas que estén involucradas.

Incluir los aspectos legales y regulatorios que apliquen al momento de evaluar los riesgos en el marco del proyecto de Cloud Computing. Por ej.: Datos Personales, Datos Sensibles (de acuerdo a lo establecido en la Ley).

Tener en cuenta los requerimientos de seguridad de la información involucrada en el marco del proyecto de Cloud Computing.

Considerarlo un proyecto de la Empresa y no únicamente de IT o Tecnología.

Incluir las responsabilidades y requisitos de seguridad de la información en el contrato de servicios de Cloud Computing o Service Leve Agreement (SLA) involucrado.

Definir los requisitos de seguridad que debe implementar el proveedor de Cloud Computing al momento de gestionar los incidentes de seguridad, en un todo de acuerdo con el proceso de gestión de incidentes de la Empresa.

Analizar los términos y condiciones, ofreciendo propuestas sobre aquellos puntos en los que no haya acuerdo. Si los términos y condiciones no cubren los requisitos, no se deberían aceptar, aunque ello signifique no utilizar el servicio.

Verificar que existan cláusulas al momento de finalizar el servicio, relacionadas con la seguridad de la información involucrada y los requisitos establecidos para su disposición. Por ej: borrado seguro, devolución, etc.

Una buena herramienta para ayudar selección de un proveedor de Cloud Computing es el ConsensusAssessmentsInitiative (CAI) de la Cloud Security Alliance (CSA). Consiste en un cuestionario que, a

través de las distintas respuestas, permite identificar la gestión de la seguridad por parte del proveedor de Servicios de Cloud.

Verificar si el proveedor de Cloud Computing se encuentra registrado en el proyecto Security, Trust, and Assurance (STAR) de Cloud Security Alliance (CSA), en el mismo se pueden conocer distintos aspectos de seguridad implementados en el servicio de Cloud Computing.

Tener en cuenta que aunque se seleccione un determinado proveedor de Cloud Computing, seguimos siendo los responsables por el cuidado de la información.

Mantener los controles de seguridad propios que sean adecuados, aunque se seleccione un servicio de Cloud Computing. Por ej: Respaldo de la Información.

Estar al tanto de los incidentes de seguridad que se presenten e involucren al proveedor de Cloud Computing seleccionado.*Referencias: Cloud Security Alliance: http://www.cloudsecurityalliance.org ;Cloud Security Alliance Chapter Argentina http://chapters.cloudsecurityalliance.org/argentina/ ;NIST SP800-145: The NIST Definition of Cloud Computing http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf; Infografía sobre Modelos de Implementación de Cloud Computing: http://wikibon.org/blog/wp-content/uploads/2010/12/cloud-computing-landscape-full.html; Guía para la Seguridad en Áreas Críticas de atención en Cloud Computing (CSG): https://cloudsecurityalliance.org/research/security-guidance/ ; Cloud AssessmentInitiative (CAI): https://cloudsecurityalliance.org/research/cai/ ; Security, Trust &Assurance (STAR): https://cloudsecurityalliance.org/research/initiatives/star-registry/ ; Riesgos y Amenazas del Cloud Computing: http://cert.inteco.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

Técnica digital forense cuántica.

Una nueva perspectiva, lo que denominamos prospectiva tecnología es el de la computación cuántica, o informática cuántica, que descansa

en la física cuántica sacando partido de algunas propiedades físicas de los átomos o de los núcleos que permiten trabajar conjuntamente con bits cuánticos (en el procesador y en la memoria del ordenador. Interactuando unos con otros estandoaislados de un ambiente externo los bits cuánticos pueden ejecutar cálculos exponenciales mucho más rápidamente que los ordenadores convencionales.

Mientras que los computadores tradicionales codifican información usando números binarios (0, 1) y pueden hacer solo cálculos de un conjunto de números de una sola vez cada uno, las computadoras u ordenadores cuánticos codifican información como serie de estados mecánicos cuánticos tales como direcciones de los electrones o las orientaciones de la polarización de un fotón representando un número que expresaba que el estado del bit cuántico está en alguna parte entre 1 y 0, o una superposición de muchos diversos números de forma que se realizan diversos cálculos simultáneamente.

En resumen, hablamos de computadores u ordenadores cuyo comportamiento es determinado de forma importante por leyes de la mecánica cuántica. El sistema descrito está formado por bits cuánticos (quantum bits) o qubits, y pueden ser por ejemplo: núcleos, puntos cuánticos semiconductores y similares.

Algunos visionan computadoras cuánticas que utilizan este tipo de estado sólido, qubits (quantum dots), es decir un material nanoestructurado preciso que se podría considerar como un arsenal de qubits. Pero la producción de ese arsenal ordenado qubits a nanoescala aislado del exterior puede ser una tarea tecnológica absolutamente exigente y compleja.

El primer computador cuantico, ya se fabrica y está disponible a un valor de quince millones de dólares, se basa en puntos cuánticos que son es una estructura cristalina a nanoescala que puede transformar la luz. El punto cuántico se considera que tiene una mayor flexibilidad que otros materiales fluorescentes, lo que lo hace apropiado para utilizarlo en construcciones a nanoescala de aplicaciones computacionales donde la luz es utilizada para procesar la información.

Los puntos cuánticos están hechos de una variedad de diferentes componentes, tales como cadmio selenio (cadmiumselenide). La firma Quantum DotsCorp controla un número de patentes para la producción de puntos cuánticos (quantum dots).

El punto cuántico (Quantum dot) es llamado en ocasiones transistor de un solo electrón (single-electron-transistor), bit cuántico (quantum bit), o "qubit"; se podría definir como una partícula de materia tan pequeña que la adición de un único electrón produce cambios en sus propiedades.

El atributo cuántico sirve para recordar que el comportamiento del electrón en tales estructuras debe ser descrito en términos de la teoría cuántica. Los átomos son ejemplos de puntos cuánticos. Estructuras hechas de unos pocos cientos de átomos también son puntos cuánticos (cadmiumselenideo, nanocristales de galliumarsenide, clusters), por sus características se trabaja a a escala nanométrica. La presencia e un único electrón en tales estructuras puede ser utilizada para almacenar información (esta es la explicación de unos de los nombres alternativos: qubits).

D-Wave Dos ™ Sistema.

El primer ordenador cuántico comercial.

El Quantum Computer Explota efectos de la mecánica cuántica Construido alrededor de "qubits" en lugar de "bits" Opera en un ambiente extremo Permite algoritmos cuánticos para resolver problemas muy duros.

Energía y refrigeración "La Nevera" es una dilución refrigerador de ciclo cerrado El procesador superconductor no genera calor Se enfrió hasta 150x más frío que el espacio interestelar (0,02 grados Kelvin).

La computación cuántica, tal como se aplica en el D-Wave sistema, se describe por una simple pero en gran medida desconocida modelo de programación. El uso de un simple mapa coloración problema

este documento describe el conjunto completo de transformaciones necesarias para encontrar soluciones mediante la ejecución de una instrucción de máquina cuántica única (QMI) dentro de este modelo de programación. Este "incrustación directa" es una de varias maneras de programar el ordenador cuántico D-Wave.

Así como el mundo de la informática clásica necesitaba un ecosistema de software para impulsar el uso y el desarrollo, las computadoras cuánticas también lo hacen. En D-Wave estamos empezando a desarrollar las capas de "software de sistema" que hará que sea fácil para los clientes y colaboradores a utilizar el sistema y explotar sus puntos fuertes.

Arquitectura de Software

La arquitectura de software D-Wave está en las primeras etapas de desarrollo. Esta imagen representa la arquitectura, con artículos futuros indicados en cursiva.

Programación de un ordenador cuántico es diferente a la programación de un ordenador tradicional. Para programar el sistema, el usuario asigna un problema en la búsqueda de la "punto más bajo en un vasto paisaje", que se corresponde con el mejor resultado posible. El procesador considera todas las posibilidades simultáneamente para determinar la energía más baja requerida para formar esas relaciones.

Debido a que una computadora cuántica es probabilística y no determinista, el equipo vuelve muchas muy buenas respuestas en un corto período de tiempo - 10.000 respuestas en un segundo. Esto le da al usuario no sólo la solución óptima o una única respuesta, sino también otras alternativas para elegir.

Para utilizar el ordenador cuántico que el usuario asigna su problema a una ecuación cuyo objetivo es devolver los valores mínimos (las soluciones óptimas). Hay dos valores que deben ser proporcionados - los "pesos" de los qubits y los "puntos fuertes" de la interacción entre ellos. Hasta alrededor de 500 y alrededor de 1.500 pesos fuertes

puede ser especificado, lo que refleja el número de qubits y el número de conexiones en el procesador actual qubit D-Wave 512. Además, el usuario también puede especificar el número de soluciones que quieren el sistema para volver.

Estos valores son enviadas al sistema, que entonces ejecuta una sola instrucción Quantum de la máquina ("QMI") para el procesamiento y devuelve el número especificado de resultados al usuario.

Hay múltiples maneras de involucrar el sistema:

Directamente programar el sistema mediante el uso de Quantum Máquina Idioma para emitir la Instrucción Quantum Máquina.

Utilice un programa de nivel superior en C, C ++, Fortran o Python para crear y ejecutar una instrucción de máquina cuántica .Usa un intérprete matemático híbrido (MATLAB) para expresar el problema como una serie de expresiones algebraicas que luego se convierten en una instrucción de máquina cuántica y ejecutados. Esto es adecuado para un clásico iterativo - proceso de la computación cuántica.

Utilice la herramienta de D-Wave QSage acelerador cuántico en un cuanto híbrido - modelo de computación convencional, se describe a continuación.

Las nuevas herramientas de software que permitirán a los usuarios de "hablar" en el idioma de su dominio del problema y luego automáticamente generar la instrucción de máquina cuántica están en desarrollo.

Descargar este libro blanco para obtener más información sobre el modelo de programación para un sistema de D-Wave.

Arquitectura de Software Información general.

A partir de la parte inferior, aquí hay una breve descripción de cada capa de la arquitectura:

Instrucción Máquina Cuántica (QMI): Este es el bloque de construcción básico sobre el que todo el software está construido. Una sola QMI es ejecutado por el procesador cuántico en respuesta a la exposición el problema del usuario. Un usuario puede programar directamente el sistema a este nivel o utilizar una de las lenguas o las herramientas de más alto nivel compatibles.

Quantum Meta-Máquina * (* en desarrollo): El Meta-máquina cuántica es una capa de abstracción que hace el código de usuario independiente de la topología específica de un procesador cuántico particular. Esto hace que sea más fácil para el código escrito por encima de esta capa a ser utilizado en nuestro sistema.

Interfaces a un nivel superior Idiomas: Para aquellos que deseen desarrollar aplicaciones, esta capa de abstracción de software suele ser el punto de partida más natural. Esta capa proporciona la capacidad de utilizar los lenguajes de programación de alto nivel estándar para acceder a las partes subyacentes del sistema de software. Se permite que los programas escritos en C, C ++, Fortran y Python para crear una instrucción de máquina cuántica que se ejecuta en el procesador.

Intérprete Matemática híbrido: Esto permite a un usuario especificar un problema como una serie de expresiones algebraicas utilizando MATLAB u otras herramientas Mathematica® similares. Las expresiones se convierten entonces en una instrucción de máquina cuántica y ejecutadas en el procesador.

Herramientas de software

QSage acelerador cuántico: Un sistema de D-Wave trabaja en conjunto con un ordenador convencional, que actúa como un co-procesador o del acelerador. Esta división permite que los sistemas híbridos que se construirán de que puede hacer frente a enormes cantidades de datos y funciones de generación extremadamente complejas.

Este modelo de programación híbrido separa la evaluación de la función de generación y el proceso de la generación de soluciones potenciales. La evaluación de la función ocurre en un sistema

informático convencional, ya que implica una gran cantidad de cálculo de la especie sistemas informáticos convencionales sobresalen en. La generación de soluciones que sucede en el sistema de D-Wave, el uso de los resultados obtenidos por el sistema informático convencional para poner a punto rápidamente en soluciones cada vez mejores. Software convencional también puede realizar estos tipos de cálculos de función de generación de iterativo (por ejemplo, usando el algoritmo de Tabu), pero la D-Wave se aprovecha de la propiedad especial de volver muchas soluciones posibles a la vez, lo que permite el salto a una ubicación más óptima en el espacio de la solución a ser más eficaz. Esto reduce el coste total (tiempo) para llegar a la solución.

El flujo de información entre los dos es de bajo ancho de banda y se limita a cadenas de bits que representan las posibles soluciones que fluyen desde el sistema de D-Wave con el sistema convencional, y los números reales que representan los valores de la función de generación evaluado para aquellas conjeturas que fluyen desde el sistema convencional a la sistema de D-Wave.

El uso de la optimización del diseño como un ejemplo, así es como un ordenador convencional y un ordenador cuántico puede trabajar juntos:

El uso de este sistema híbrido es simple. El desarrollador proporciona la función generadora, inicia el cómputo, y luego el sistema se inicia 'pensamiento' acerca de la función de generación de la siguiente, de forma iterativa:

1 - Una serie de soluciones aleatorias son generadas por el sistema informático convencional.
2 - La calidad de estas conjeturas se evalúa pasándolos en la función de generación.
3 - Los números reales que caracterizan a la idoneidad de las soluciones se envían al sistema de D-Wave.
4 - El sistema D-Wave se ajusta automáticamente sobre la base de esta información, y genera una nueva serie de parámetros, basándose en los resultados recibidos.

5 - Estos nuevos parámetros se envían de vuelta al sistema convencional, en el que se evalúan.
6 - Pasos 3-5 se repiten hasta que se cumplan los criterios de salida.

Intérprete Quantum: Una nueva herramienta está en desarrollo en D-Wave que proporciona mecanismos sencillos para que los usuarios representen sus partes de sus problemas de cálculo como una serie de afirmaciones sobre la naturaleza de los parámetros en su dominio. El software permite al usuario seleccionar mediante programación todas o algunas de las afirmaciones, y traducir sus intenciones en un QMI que luego se pasa directamente a la D-Wave, que devuelven la solución (energía más baja) óptima. Este vector solución se devolvió al usuario.

(Ver Anexo 56)

La pericia digital forense.....una actividad del futuro?

GLOSARIO FORENSE

ANEXOS

- Línea del tiempo de la historia de la ciencia Forense

- Manual cadena de custodia. (Policía Nacional del Ecuador)

- Manual de manejo de evidencias digitales y entornos informáticos 2.0. (Fiscalía General del Estado- Ecuador).

- Convenio sobre cibercriminalidad de Budapest

- Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en materia de Ciberdelincuencia

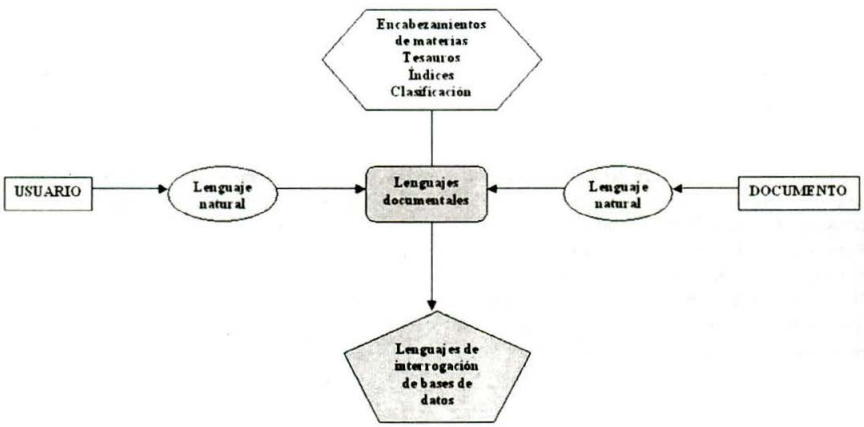
- Recomendación de COMJIB relativa a la Tipificación y Sanción de la Ciberdelincuencia

BIBLIOGRAFÍA.

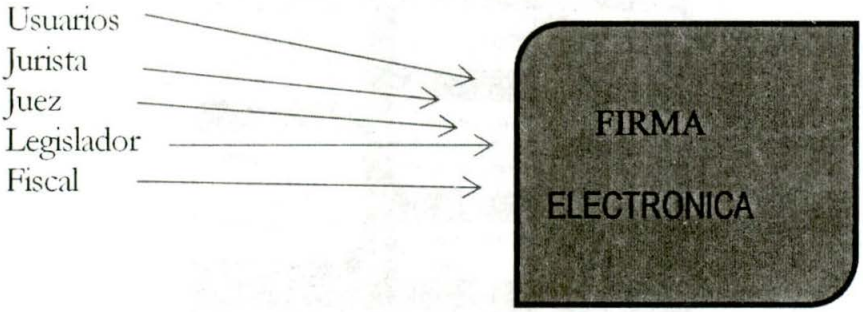
ANEXOS

Anexo 1

Anexo 2

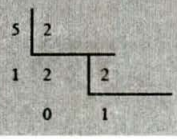


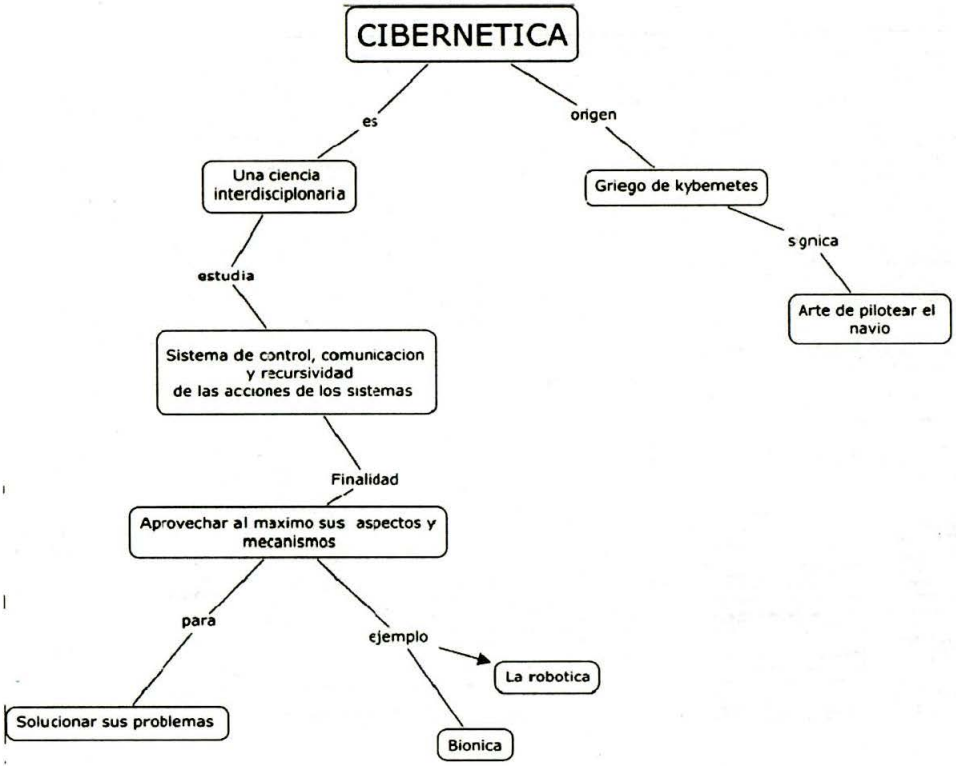
Anexo 3



Anexo 4

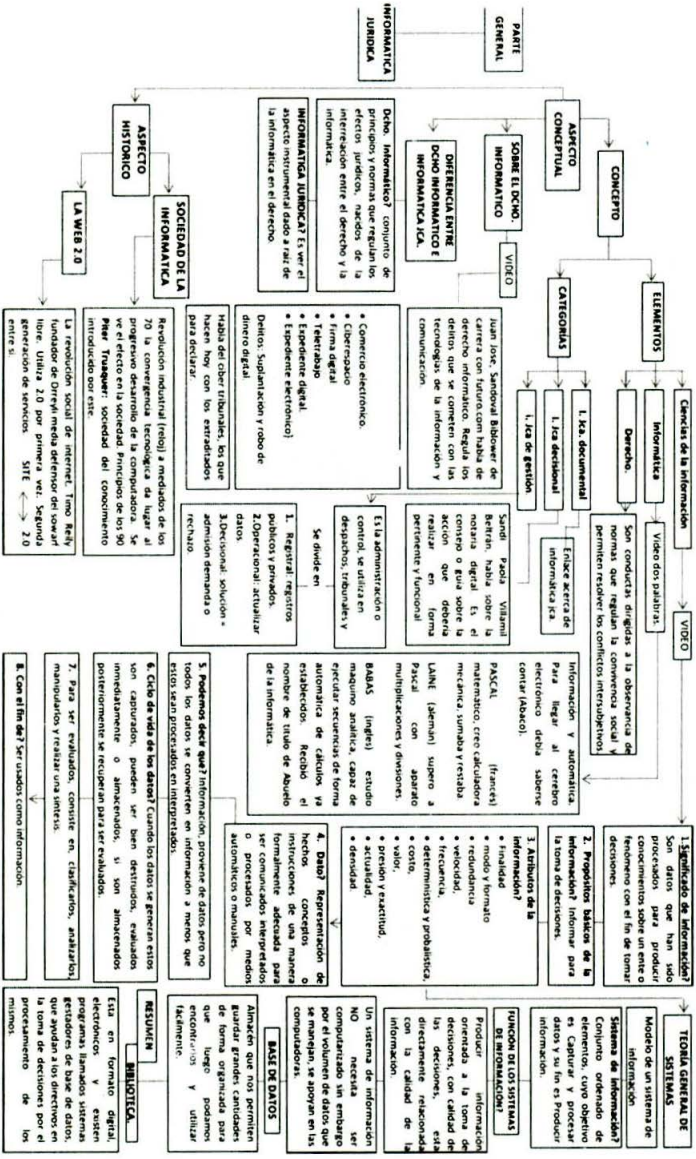
[15] La traducción de una cifra del sistema decimal al lenguaje binario es relativamente sencilla. Veamos un par de ejemplos. La cifra 5, como cualquier otra, según el sistema decimal, se descompone en una ecuación de segundo grado [$ax^2 + bx + c = 0$], es decir, $5 = 1 \cdot 2^2 + 0 \cdot 2 + 1 = 4 + 0 + 1$. Para convertir la cifra 5 al lenguaje binario se procede a la división adjunta, de modo que 5= 101= 100 + 0 + 1 [centenas, decenas y unidades]= 4 [porque en el sistema binario 100 es el número que representa la cifra 4] + 0 + 1= $1 \cdot 2^2 + 0 \cdot 2 + 1 = 5$

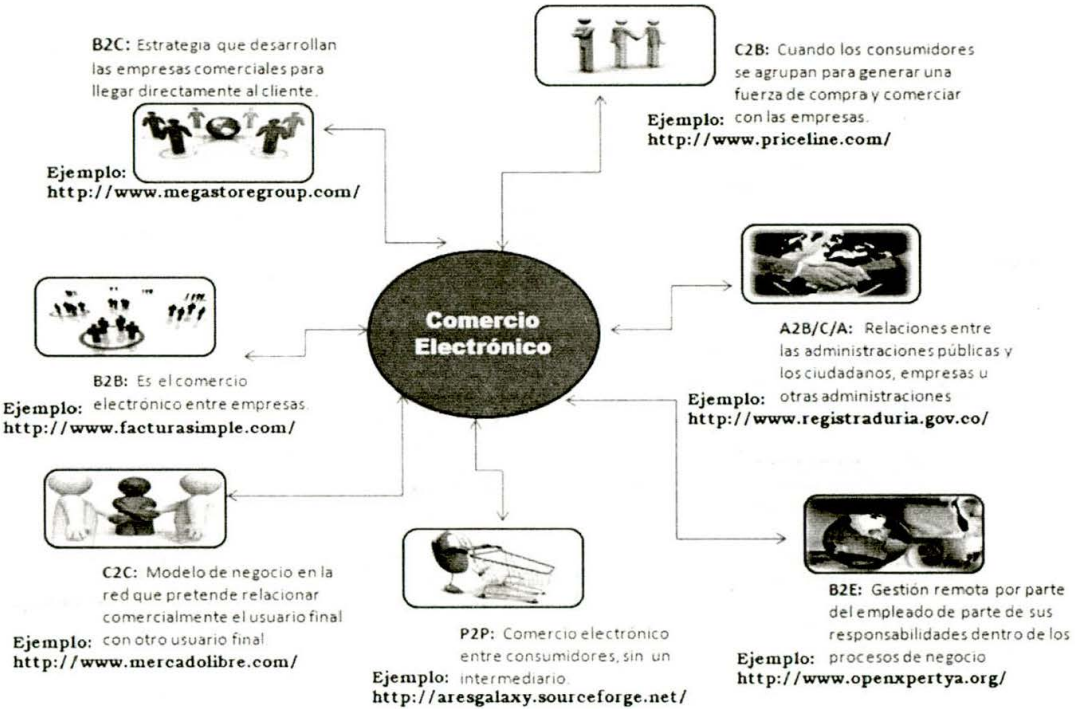



CIBERNETICA
es
origen
Una ciencia interdisciplonaria
Griego de kybemetes
sgnica
Arte de pilotear el navio
estudia
Sistema de control, comunicacion y recursividad de las acciones de los sistemas
Finalidad
Aprovechar al maximo sus aspectos y mecanismos
para
ejemplo
La robotica
Solucionar sus problemas
Bionica

Anexo 5

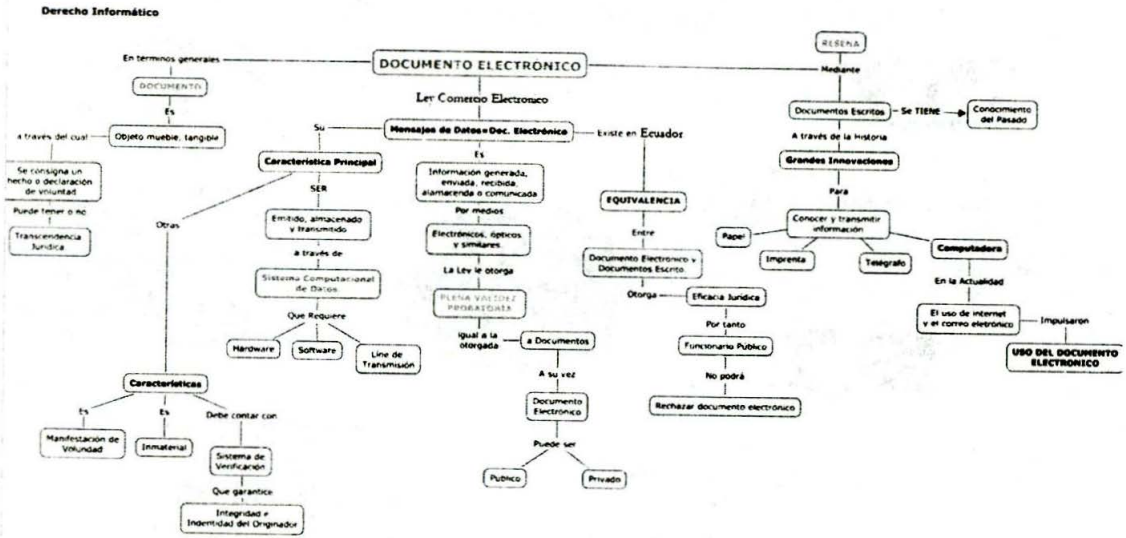
Anexo 6


PARTE GENERAL
INFORMATICA JURIDICA
ASPECTO CONCEPTUAL
SOBRE EL DCHO. INFORMATICO
VIDEO
DIFERENCIA ENTRE DCHO INFORMATICO E INFORMATICA JCA.
Dcho. Informático? conjunto de principios y normas que regulan los efectos jurídicos, nacidos de la interrelación entre el derecho y la informática.
INFORMATICA JURIDICA? Es ver el aspecto instrumental dado a raíz de la informática en el derecho.
Juan Jose, Sandoval Bibiover de carrera con futuro.com habla de derecho informático. Regula los delitos que se cometen con las tecnologías de la información y comunicación.
• Comercio electrónico.
• Ciberespacio
• Firma digital
• Teletrabajo
• Expediente digital.
• Expediente electrónico)
Delitos: Suplantación y robo de dinero digital
Habla del cíber tribunales, los que hacen hoy con los extraditados para declarar
CONCEPTO
CATEGORIAS
I. Jca. de gestión
I. Jca. decisional
I. Jca. documental
Sandi Paola Villamil Beltran, habla sobre la notaria digital. Es el consejo o guía sobre la acción que debería realizar en forma pertinente y funcional
Es la administración o control, se utiliza en despachos, tribunales y
Se divide en
1. Registral: registros públicos y privados.
2.Operacional: actualizar datos
3.Decisional: solución + admisión demanda o rechazo
Enlace acerca de informática jca.
Información y automática. Para llegar al cerebro electrónico debía saberse contar (ábaco).
PASCAL (francés) matemático, creo calculadora mecánica, sumaba y restaba
LAINE (alemán) superó a Pascal con aparato multiplicaciones y divisiones.
BABAS (inglés) estudio maquino analítica, capaz de ejecutar secuencias de forma automática de cálculos ya establecidos. Recibió el nombre de título de Abuelo de la informática.
ELEMENTOS
Informática
Derecho.
Ciencias de la información
Video dos palabras.
Son conductas dirigidas a la observancia de normas que regulan la convivencia social y permiten resolver los conflictos intersubjetivos.
VIDEO
1.Significado de información? Son datos que han sido procesados para producir conocimientos sobre un ente o fenómeno con el fin de tomar decisiones.
2. Propósitos básicos de la información? Informar para la toma de decisiones.
3. Atributos de la información?
• Finalidad
• modo y formato
• redundancia
• velocidad,
• frecuencia,
• determinística y probabilística,
• costo,
• valor,
• precisión y exactitud,
• actualidad,
• densidad
4. Dato? Representación de hechos conceptos o instrucciones de una manera formalmente adecuada para ser comunicados interpretados o procesados por medios automáticos o manuales.
SOCIEDAD DE LA INFORMATICA
ASPECTO HISTORICO
LA WEB 2.0
Revolución industrial (reloj) a mediados de los 70 la convergencia tecnológica da lugar al progresivo desarrollo de la computadora. Se ve el efecto en la sociedad Principios de los 90 Peter Truaquer: sociedad del conocimiento introducido por este.
La revolución social de internet. Timo Rely fundador de Dirrejk media defensor del software libre. Utiliza 2.0 por primera vez. Segunda generación de servicios SITE ⟷ 2.0 entre sí.
5. Podemos decir que? Información, proviene de datos pero no todos los datos se convierten en información a menos que estos sean procesados en interpretados.
6. Ciclo de vida de los datos? Cuando los datos se generan estos son capturados, pueden ser bien destruidos, evaluados inmediatamente o almacenados, si son almacenados posteriormente se recuperan para ser evaluados.
7. Para ser evaluados, consiste en, clasificarlos, analizarlos, manipularlos y realizar una síntesis.
8. Con el fin de? Ser usados como información
TEORÍA GENERAL DE SISTEMAS
Modelo de un sistema de información
Sistema de información? Conjunto ordenado de elementos, cuyo objetivo es Capturar y procesar datos y su fin es Producir información.
FUNCION DE LOS SISTEMAS DE INFORMACIÓN?
Producir información orientada a la toma de decisiones, con calidad de las decisiones, está directamente relacionada con la calidad de la información.
Un sistema de información NO necesita ser computarizado sin embargo por el volumen de datos que se manejan, se apoyan en las computadoras.
BASE DE DATOS
Almacen que nos permiten guardar grandes cantidades de forma organizada para que luego podamos encontrarlos y utilizar fácilmente.
RESUMEN
BIBLIOTECA
Esta en formato digital, electrónicos y existen programas llamados sistemas gestadores de base de datos, que ayudan a los directivos en la toma de decisiones por el procesamiento de los mismos.


Comercio Electrónico
B2C: Estrategia que desarrollan las empresas comerciales para llegar directamente al cliente.
Ejemplo: http://www.megastoregroup.com/
C2B: Cuando los consumidores se agrupan para generar una fuerza de compra y comerciar con las empresas.
Ejemplo: http://www.priceline.com/
B2B: Es el comercio electrónico entre empresas.
Ejemplo: http://www.facturasimple.com/
A2B/C/A: Relaciones entre las administraciones públicas y los ciudadanos, empresas u otras administraciones
Ejemplo: http://www.registraduria.gov.co/
C2C: Modelo de negocio en la red que pretende relacionar comercialmente el usuario final con otro usuario final.
Ejemplo: http://www.mercadolibre.com/
P2P: Comercio electrónico entre consumidores, sin un intermediario.
Ejemplo: http://aresgalaxy.sourceforge.net/
B2E: Gestión remota por parte del empleado de parte de sus responsabilidades dentro de los procesos de negocio
Ejemplo: http://www.openxpertya.org/

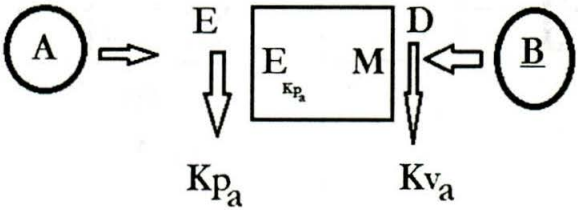
Anexo 7

Anexo 8


Derecho Informático
DOCUMENTO ELECTRONICO
En terminos generales
DOCUMENTO
Es
Objeto mueble, tangible
a través del cual
Se consigna un hecho o declaración de voluntad
Puede tener o no
Transcendencia Jurídica
Otras
Características
Es
Manifestación de Voluntad
Es
Inmaterial
Debe contar con
Sistema de Verificación
Que garantice
Integridad e Indemidad del Originador
Ley Comercio Electronico
Su
Mensajes de Datos=Doc. Electrónica
Existe en Ecuador
Es
Información generada, enviada, recibida, alamacenda o comunicada
Por medios
Electrónicos, ópticos y similares
La Ley le otorga
PLENA VALIDEZ PROBATORIA
igual a la otorgada
a Documentos
A su vez
Documento Electrónico
Puede ser
Público
Privado
Característica Principal
SER
Emitido, almacenado y transmitido
a través de
Sistema Computacional de Datos
Que Requiere
Hardware
Software
Line de Transmisión
EQUIVALENCIA
Entre
Documento Electrónico y Documentos Escrito
Otorga
Eficacia Jurídica
Por tanto
Funcionario Público
No podrá
Rechazar documento electrónico
RESEÑA
Mediante
Documentos Escritos
Se TIENE
Conocimiento del Pasado
A través de la Historia
Grandes Innovaciones
Para
Conocer y transmitir información
Papel
Imprenta
Telégrafo
Computadora
En la Actualidad
El uso de internet y el correo eletrónico
Impulsaron
USO DEL DOCUMENTO ELECTRONICO

Anexo 9

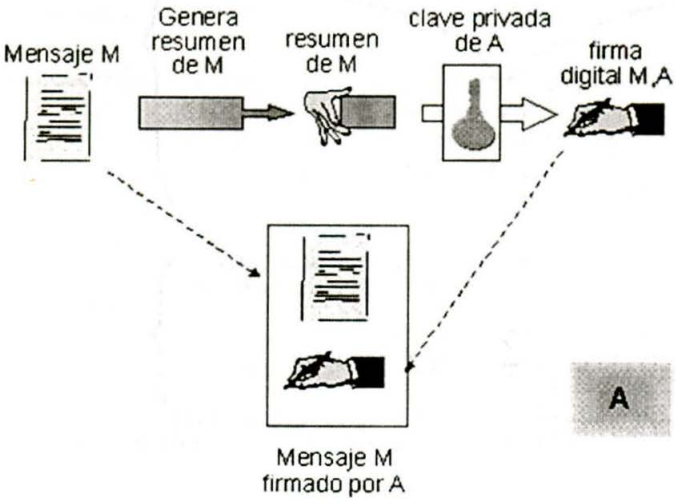
FORMULA FIRMA DIGITAL



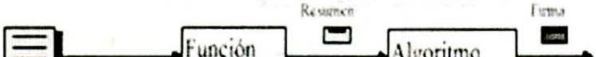
A usuario
B usuario
E encriptar
D desencriptar
Kpa encriptacionclave privada
Kva encriptacion clave publica
M mensaje

A-M-EKpa-M-DKva-M-B

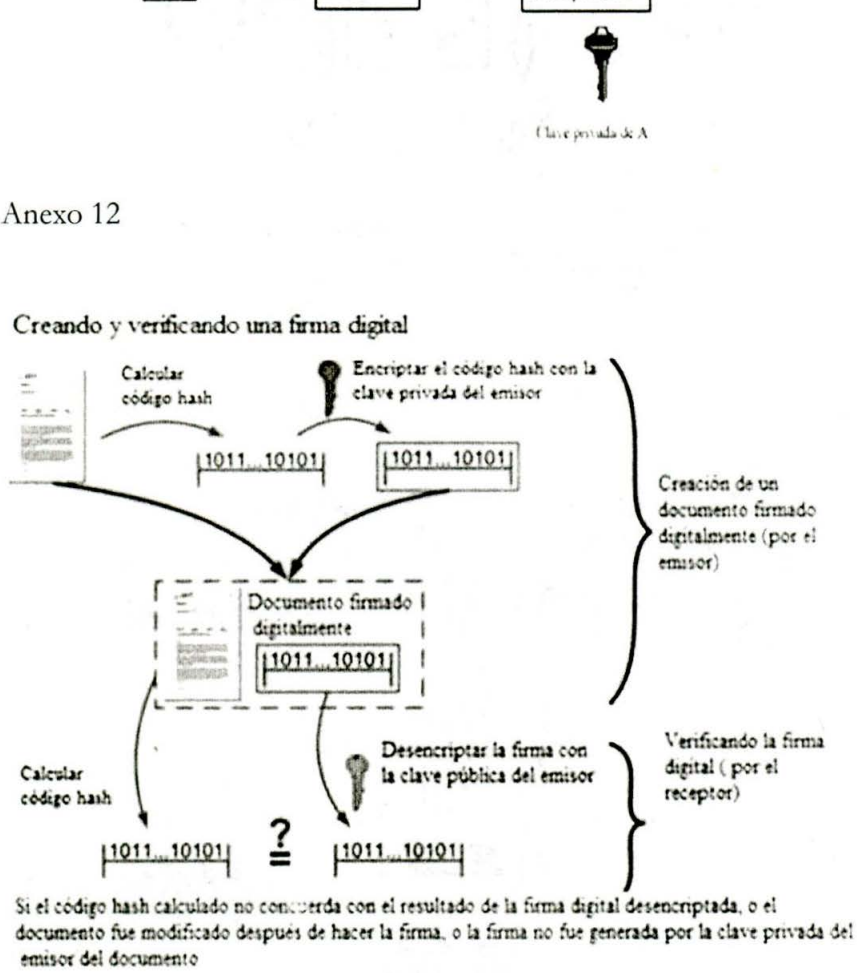
Anexo 10



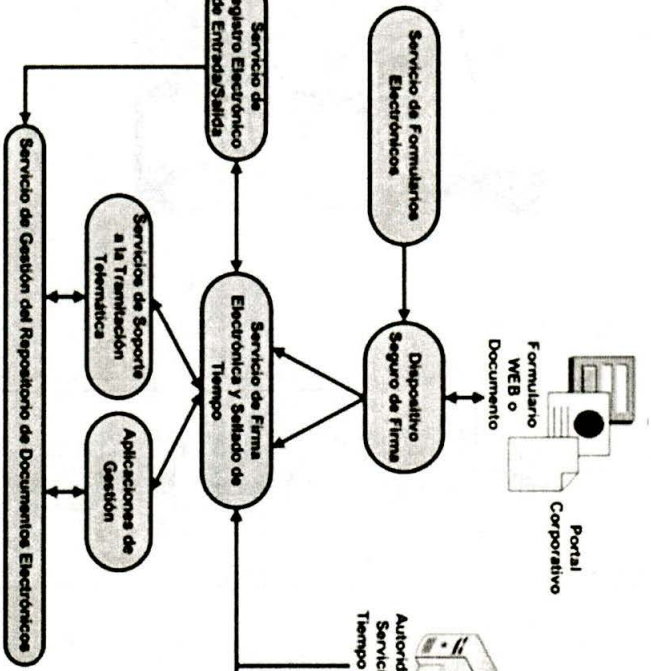
Anexo 11



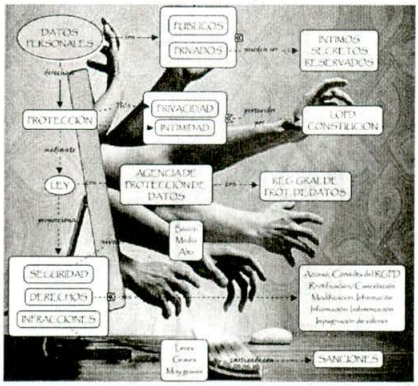
Anexo 12



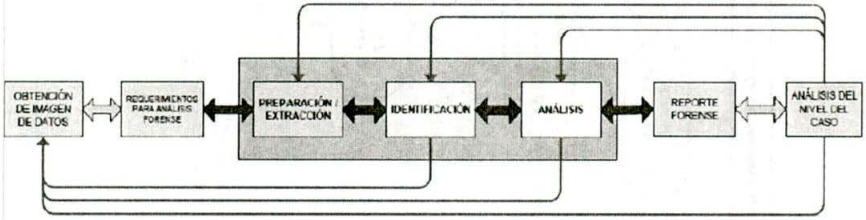
Anexo 13


Portal Corporativo
Formulario WEB o Documento
Servicio de Formularios Electrónicos
Dispositivo Seguro de Firma
Servicio de Registro Electrónico de Entrada/Salida
Servicio de Firma Electrónica y Sellado de Tiempo
Autoridad de Servicio de Tiempo (TSA)
Entidad Certificadora
Servicios de Soporte a la Tramitación Telemática
Aplicaciones de Gestión
Servicio de Gestión del Repositorio de Documentos Electrónicos

Anexo 14

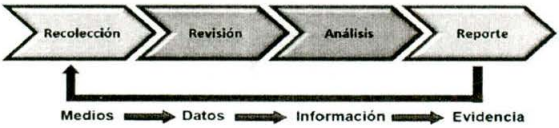


Anexo 15



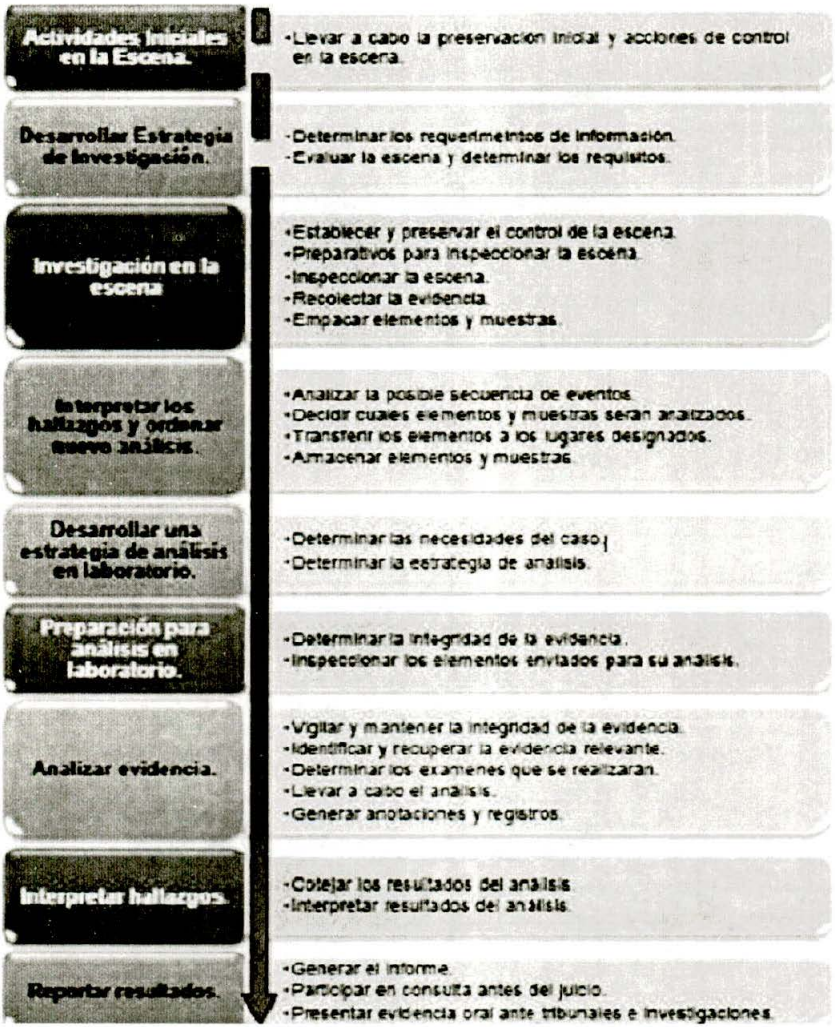
Fuente: Metodología Forense del Departamento de Justicia de los EE.UU.
http://www.justice.gov/criminal/cybercrime/

Anexo 16



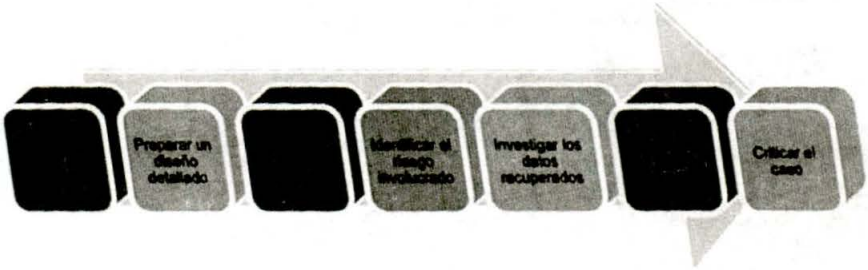
Fuente: Proceso Forense del NIST

Anexo 17



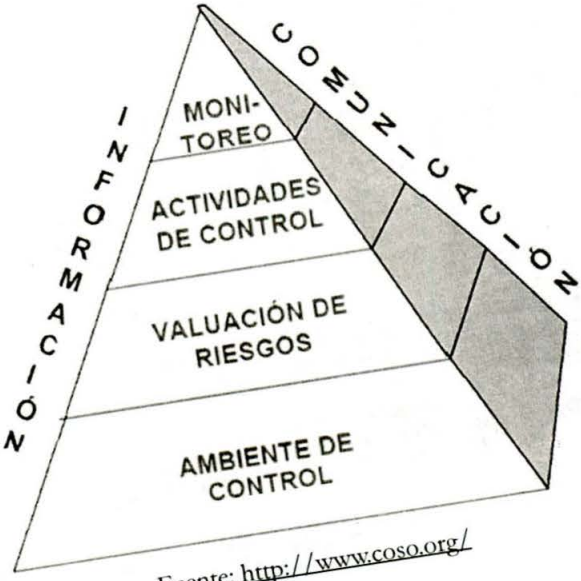
Fuente: http://www.enfsi.eu/about-enfsi/structure/working-groups/information-technology

nexo 18



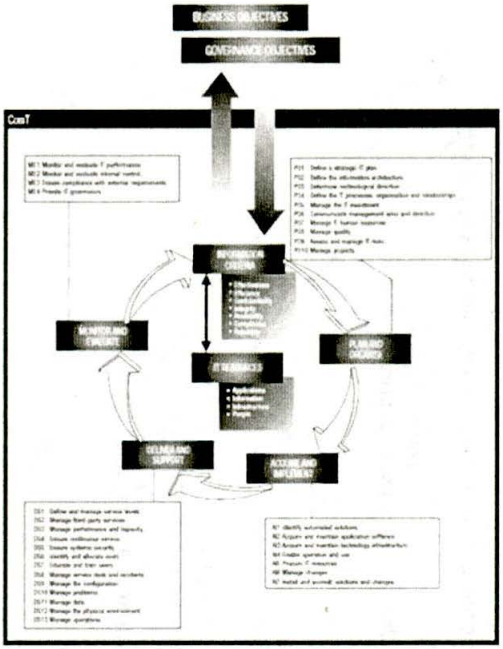
Fuente: http://www.eccouncil.org/

Anexo 19



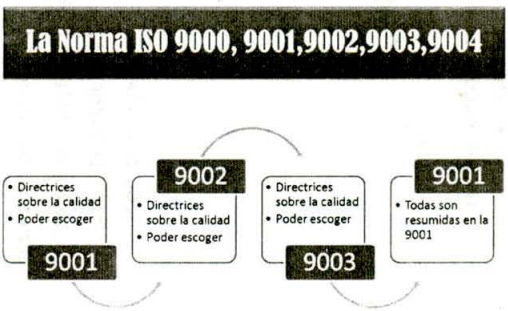
Fuente: http://www.coso.org/

Anexo 20



Fuente: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

Anexo 21



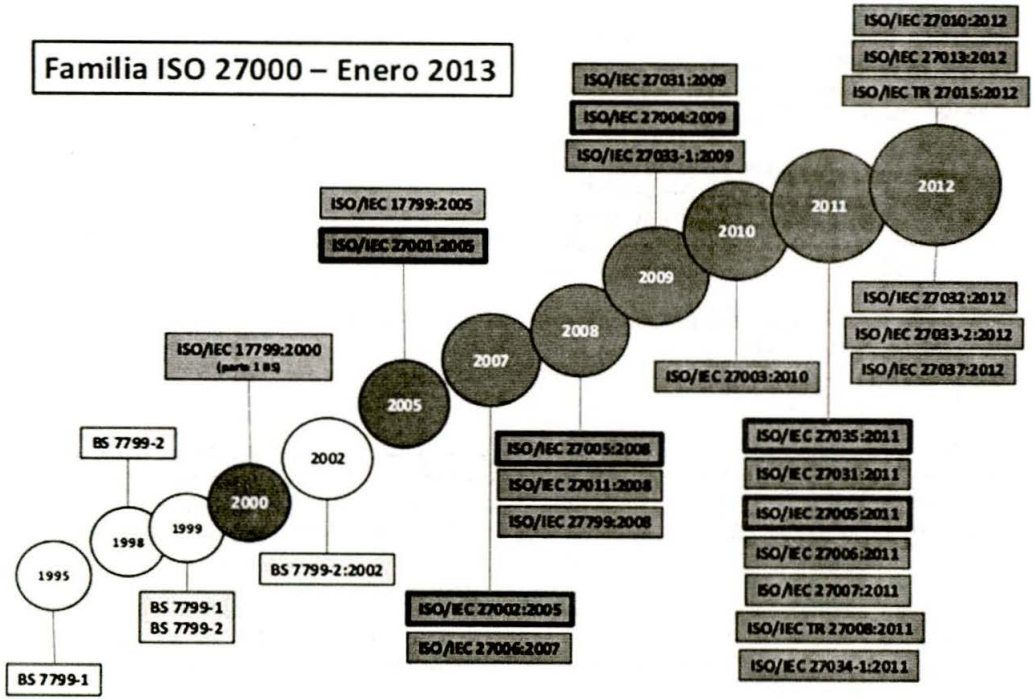
Fuente: www.iso.org

Obra: CI 25 Derechos y Nuevas Tecnologías Fecha: 15-ene-2015 Nro Placa: 15 Impresión de blanco

Fuente: www.iso.org

Anexo 22

Anexo 23



Fuente: http://www.iso.org/iso/home.html

Gerar: 5: 20 Derechos y Nuevas Tecnologías Fecha: 19-ene-2015 Nro Hoja: 12 Impresión de blanco

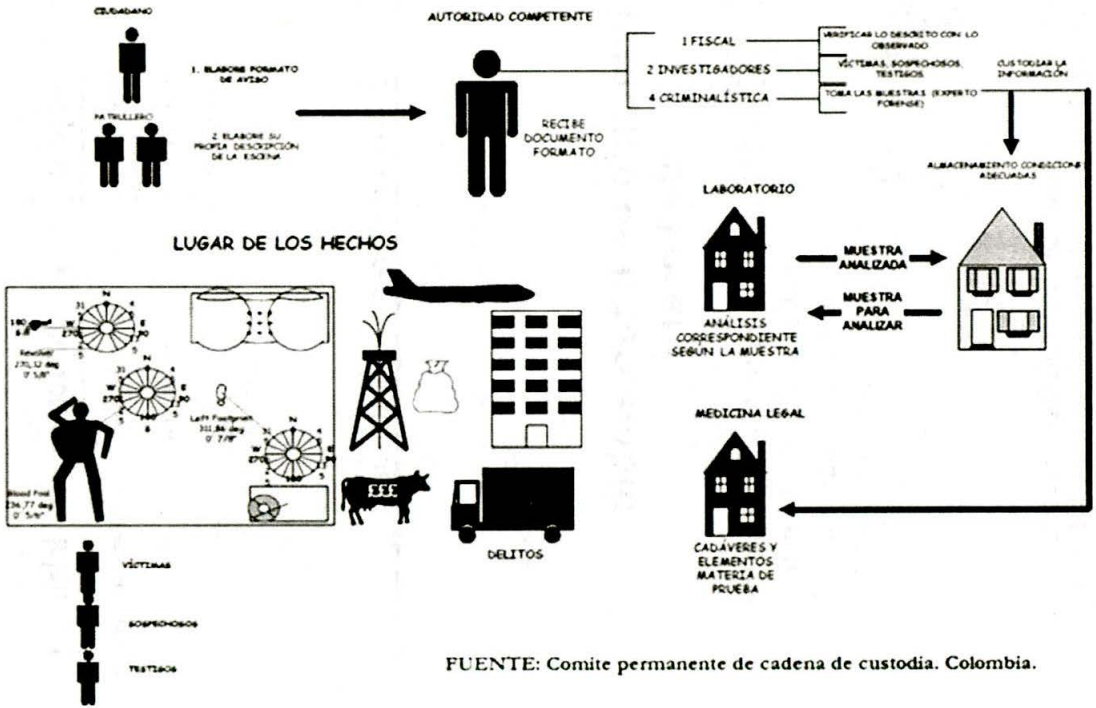
Documento Normativo Internacional	Documento Normativo Nacional
ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*	No existe documento nacional normativo correspondiente.
ISO/IEC 27000, *Information technology — Security techniques — Sistemas de gestión de seguridad de información – Information security management systems — Overview and vocabulary*	NTE INEN ISO/IEC 27000:2012, *Tecnología de la información — Técnicas de seguridad — Sistema de gestión de seguridad de la información — Descripción general y vocabulario*
ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*	NTE INEN-ISO/IEC 27001:2011, *Tecnología de la información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información (SGSI). Requisitos*
ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security management*	NTE INEN-ISO/IEC 27002:2009, *Tecnología de la información — Técnicas de la seguridad — Código de práctica para la gestión de la seguridad de la información.*
ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*	NTE INEN ISO/IEC 27005:2012, *Tecnología de información – Técnicas de seguridad – Gestión del riesgo en la seguridad de información*

Fuente: www.normalizacion.gob.ec

INEN - ECUADOR

Anexo 24

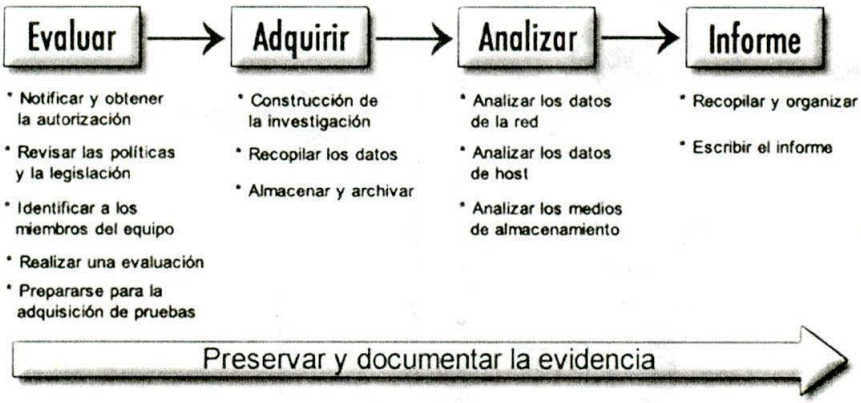
DIAGRAMA PICTORICO DEL SISTEMA DE CADENA DE CUSTODIA



FUENTE: Comite permanente de cadena de custodia. Colombia.

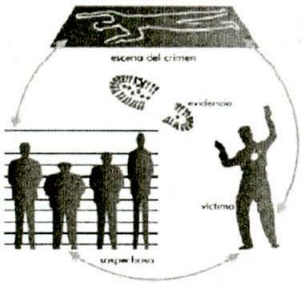
Anexo 25

Anexo 26



Anexo 27

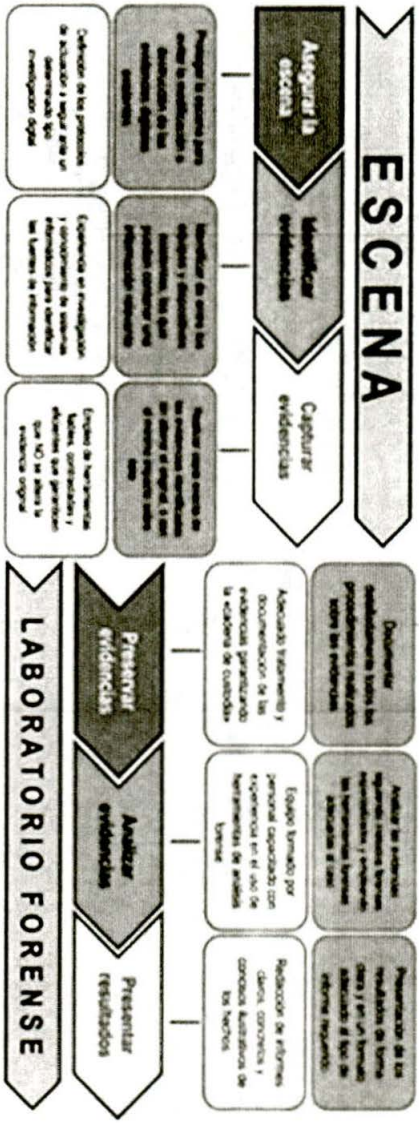
Principio de Intercambio de Locard



"Siempre que dos objetos entran en contacto estos transfieren parte del material que incorporan al otro objeto"

Fuente: http://razonalo.com/index.php?option=com_k2&view=item&id=277:principio-de-intercambio-de-locard&Itemid=73

Anexo 28


ESCENA
Asegurar la escena
Identificar evidencias
Capturar evidencias
Documentar exhaustivamente todos los procedimientos realizados sobre las evidencias
Analizar las evidencias aplicando técnicas forenses, herramientas y metodologías, y emitir las hipótesis técnicas de cada caso
Presentación de los resultados de forma clara y en un formato adecuado al tipo de informe requerido
Asegurar la escena para evitar la modificación o destrucción de las evidencias digitales existentes
Identificar de entre las digitales y dispositivos existentes, los que pueden contener una información relevante
Realizar copia exacta de los primeros dispositivos de interés y original, y con el mismo respecto sobre las
Adecuado tratamiento y documentación de las evidencias garantizando la cadena de custodia
Equipo formado por personal capacitado con experiencia en el uso de herramientas de análisis forense
Redacción de informes claros, concretos y concisos ajustándose a los hechos
Definición de los protocolos de actuación y legal ante un determinado tipo investigación digital
Experiencia en investigación y conocimiento de materiales y dispositivos para identificar las barreras de información
Empleo de herramientas fiables, contrastadas y eficientes que garanticen que NO se altera la evidencia original
Preservar evidencias
Analizar evidencias
Presentar resultados
LABORATORIO FORENSE

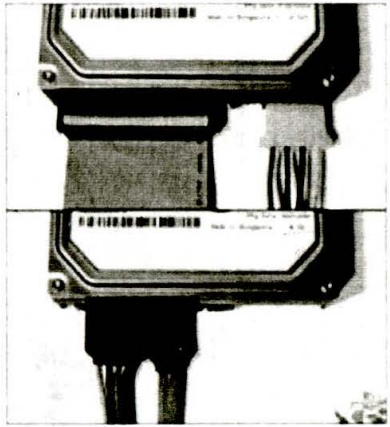
Servicios	EnCase	ForensicToolkit FTK
Clonación de discos	X	X
Validación de la integridad criptográfica de las evidencias	X	X
Información del sistema	X	X
Adquisición de imágenes en vivo	X	X
Recuperación de contraseñas	X	X
Recuperación de archivos borrados	X	X
Recuperación de correos borrados	X	X
Análisis Forense en Red	X	
Análisis Forense en Navegadores	X	X
Análisis de Dispositivos Móviles	X	
Análisis de documentos firmados electrónicamente	X	
Búsqueda de archivos	X	X
Reportes automáticos	X	X
Adquisición de evidencia de la RAM	X	
Herramientas de automatización	X	
Análisis de discos IDE y Serial ATA	X	X
Análisis de discos RAID y SCSI	X	
Reparación de sectores de disco defectuosos	X	X
Reparación de particiones dañadas	X	X
Recuperación de información eliminada por virus	X	X
Recuperación de imágenes ocultas (esteganografía)	X	X

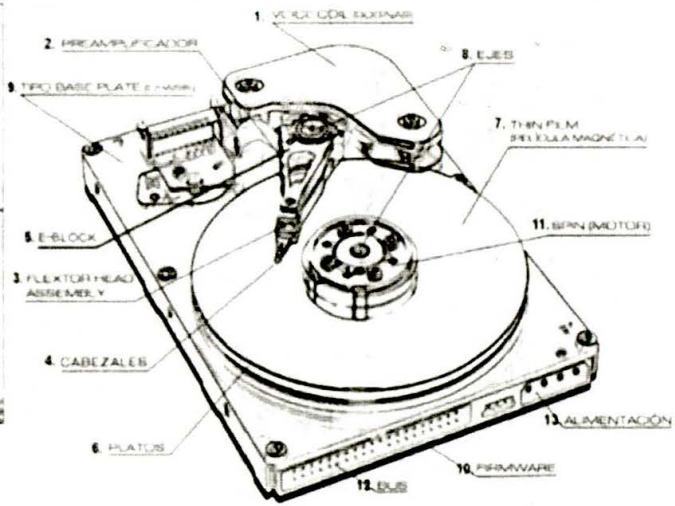
Fuente: www.encase.org

Anexo 29

ESTRUCTURA FISICA DE UN DISCO DURO

CONEXIONES DE UN DISCO DURO IDE/SATA. (SCSI)

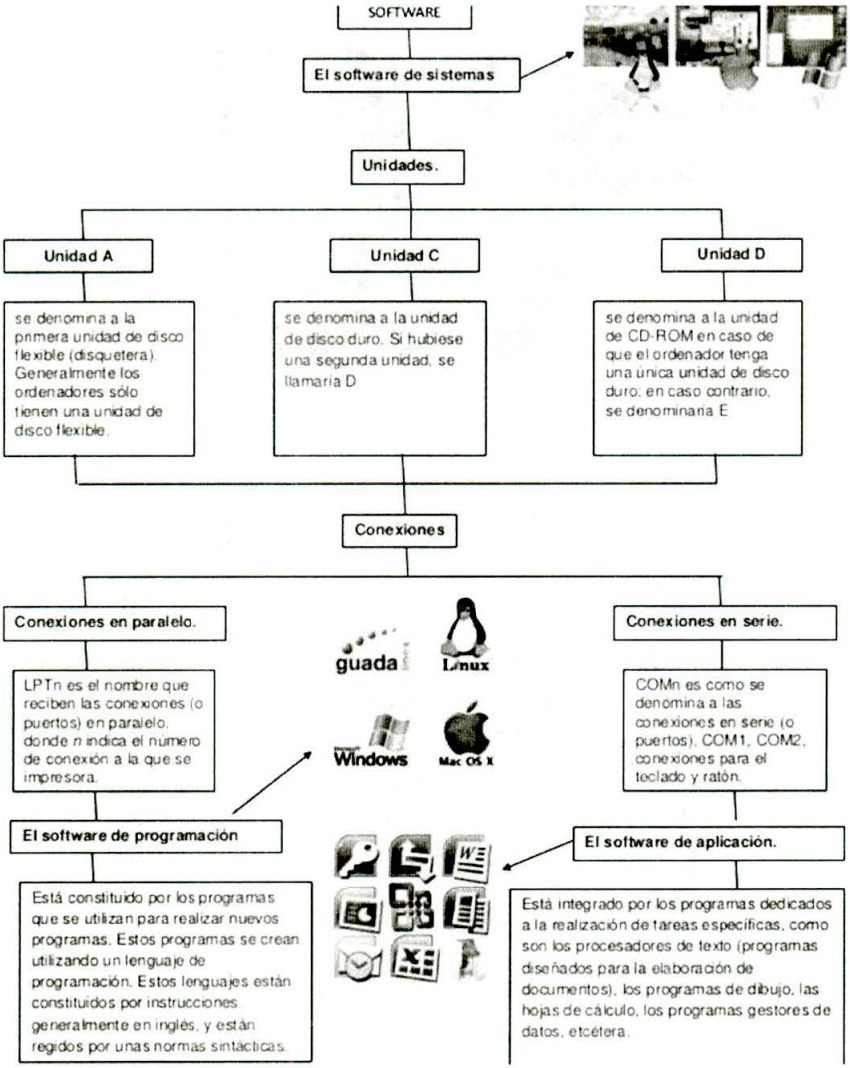




Fuente: www.cetid.abogados.ec

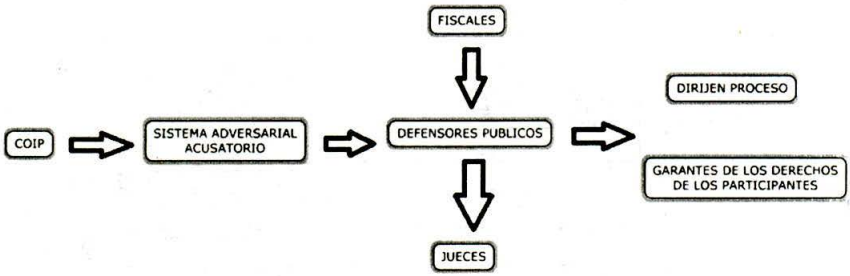
Anexo 30

Anexo 31

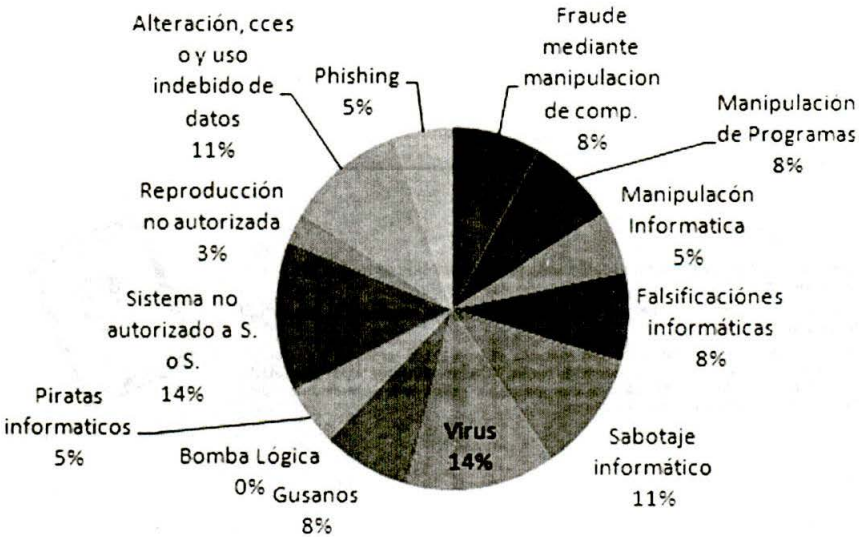


Fuente: www.wikipedia.org

Anexo 32



Anexo 33



Anexo 34

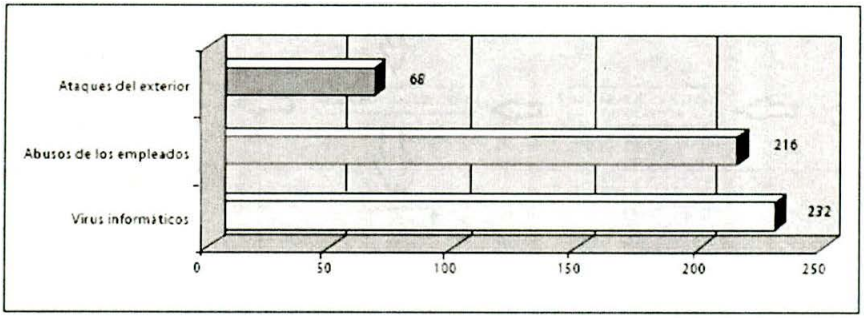


Figura 1. Frecuencia de ataques informáticos a las organizaciones.
Fuente: Cisco.

Anexo 35

EL COSTO

- El **costo del cibercrimen** para la economía mundial se sitúa entre los **375 y 575 billones de dólares**
- **En Estados Unidos** se pierden anualmente **200.000 empleos a causa del cibercrimen**
- Algunas víctimas de ciberataques durante el año 2013 incluyen Facebook, WhatsApp, Twitter, Apple, The New York Times, The Washington Post, Target, JP Morgan Chase, Citigroup, Barclays, e innumerables sitios web gubernamentales de países desarrollados y en desarrollo

*Fuentes en seccion de Documentos de Referencia

Anexo 36

Delitos informáticos según "CONVENIO CIBER DELINCUENCIA 1 de Nov. 2001

1. Contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
   - Acceso ilícito a sistemas informáticos.
   - Interceptación ilícita de datos informáticos.
   - Interferencia en el funcionamiento de un sistema informático.
   - Abuso de dispositivos que faciliten la comisión de delitos.

     Ejemplos: el robo de identidades, la conexión a redes no autorizadas y la utilización de spyware y de keylogger

2. Delitos informáticos
   - Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
   - Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

     Ejemplo:

     El borrado fraudulento de datos o la corrupción de ficheros.

3. Delitos relacionados con el contenido
   - Producción, oferta, difusión, adquisición de contenidos de pornografía infantil, por medio de un sistema informático o posesión de dichos contenidos en un sistema informático o medio de almacenamiento de datos.

4. Delitos relacionados con infracciones de la propiedad intelectual y derechos afines

   Un ejemplo de este grupo de delitos es la copia y distribución de programas informáticos, o piratería informática

Anexo 37

DATOS BÁSICOS DE SEGURIDAD CIBERNÉTICA

El CONTEXTO - Siglo XXI

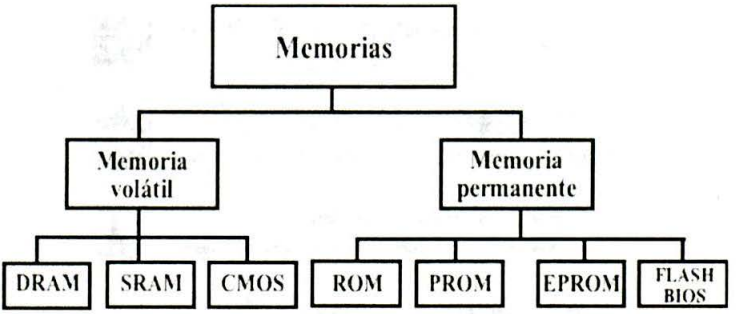
- Hoy en día hay casi **3 mil millones de usuarios** Internet alrededor del mundo
- Cada minuto se envían más de **200 millones de correos electrónicos**
- Cada minuto se crean **517 nuevos sitios web**
- El valor de las transacciones de comercio electrónico globales en el 2014 alcanzará **1,500 billones de dólares**
- **América Latina y el Caribe: 250 millones de usuarios** de internet (con la tasa de crecimiento anual para 2013 más alta a nivel mundial 12%)
- Los **latinoamericanos** pasan más tiempo en las **redes sociales** que ningún otro ciudadano del mundo, **8.67 horas por mes**
- A fines de **2015** habrá **20 mil millones de dispositivos conectados** y 50 mil millones para el año 2020
- **La infraestructura crítica** - incluyendo sistemas de purificación de agua, generación y distribución de energía, administración de sistemas de transporte, comunicación y manufactura - **depende de un acceso seguro a Internet y sistemas TIC** para su funcionamiento

Anexo 38

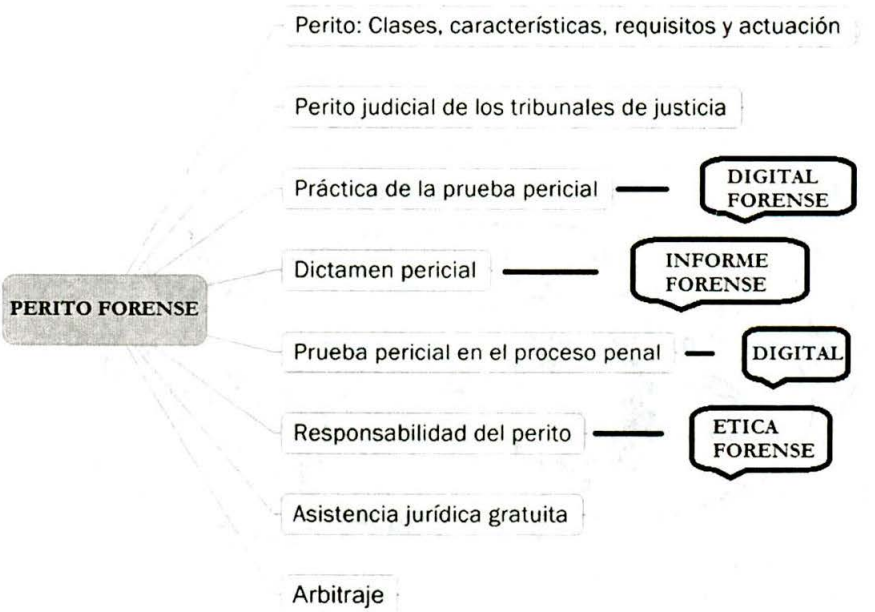
LA AMENAZA

- Más de **1,400 instituciones financieras** de 88 países fueron víctimas de **ciberataques** durante el año **2013**
- Durante el **2013 hubo 253 grandes fallos de seguridad** en el ciberespacio (un 62% más que al año anterior) que han dejado en manos de delincuentes los datos de casi 600 millones de personas
- **Cada día hay 568.000 ataques a sitios web** y más de 29 mil millones de correos electrónicos no deseados (spam)
- El **77% de los sitios web actualmente** operan con una vulnerabilidad conocida; y **1 de cada 8** tiene vulnerabilidades críticas
- El **16% de los ataques de suplantación de identidad** o spear phishing van **dirigidos a la administración pública**
- En la actualidad **existen al menos 20 grupos de cibercriminales** a nivel internacional que cuentan **con capacidades similares a las de un gobierno**

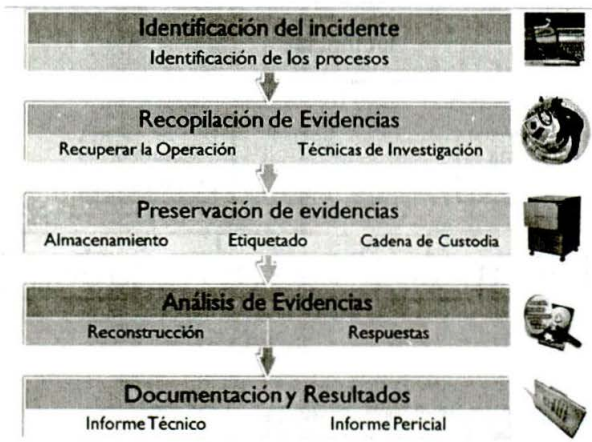
Anexo 39



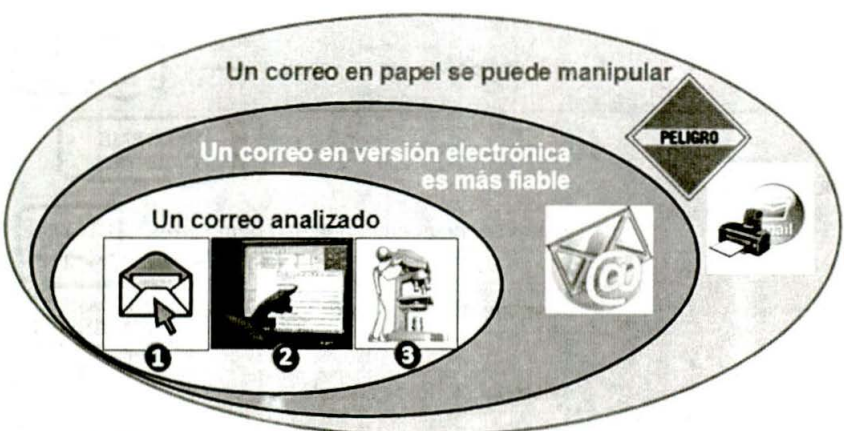
Anexo 40



Anexo 41



Anexo 42



1) Flujo
2) Mensaje
3) Contenido

CONEXIÓN INVERSA
Vulnerabilidades del equipo
- Sistemas Desactualizados o no protegidos.
- Puestos accesibles, vulnerabilidades del Sistema.
- Redes Wifis abiertas o protecciones WAP o WEP poco seguras.
- Malwares, Troyanos, backdoors, botnets, etc.
Delincuente cibernético (oculto)
Orden de Transacción Bancaria Fraudulenta
Orden de Transacción Bancaria Fraudulenta
MULERO
Presunto Delincuente 2
- Apropiación de la Comisión.
- Retirada del Dinero.
- Envío del resto al Extranjero.
Identificación Vía operador ISP
Perito IT
Presunto Delincuente 1
Indicios de posible No culpabilidad
- Ausencia de lucro personal en la operación.
- No posee conocimientos técnicos para obtener claves bancarias.
- No se encuentran indicios de la operación en el examen del equipo.

Anexo 43

NIVEL DE PUBLICIDAD

facebook

NIVEL DE RELACIÓN

Publicación visitada

Perito IT

USUARIO QUE VISUALIZA — RELACIÓN — **USUARIO QUE PUBLICA**

Cada usuario posee una relación con otro usuario y dependiendo de la misma posee un nivel de autorización para ver o participar en las publicaciones

Niveles de Relación:
Ninguna / Seguidores / Amigo de Amigo / Amigo

Toda publicación posee un nivel de "Alcance" de la Publicidad.
Niveles de Publicidad:
Público / Amigos de Amigos / Amigos / Personalizado / Sólo yo

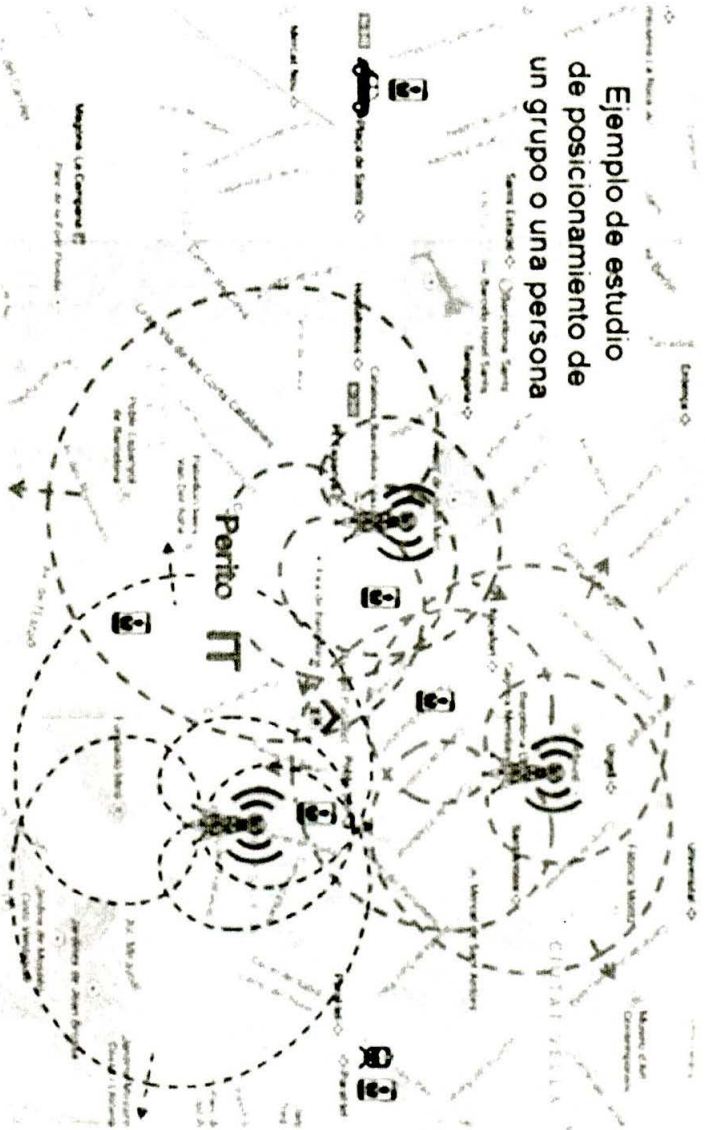
AUTORIZACIÓN

El nivel de Autorización esta formado por el nivel de Publicidad y el de Relación

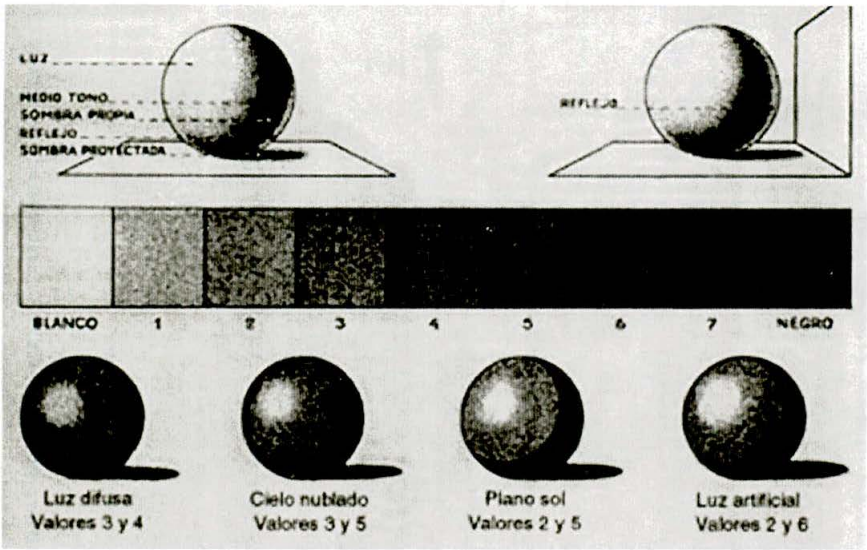
Publicidad	→ Relación
Público	→ Todos los niveles de relación
Amigos de Amigos	→ Amigos de Amigos / Amigos
Amigos	→ Amigos
Personalizado	→ Amigos
Sólo yo	→ El que publica

Anexo 44

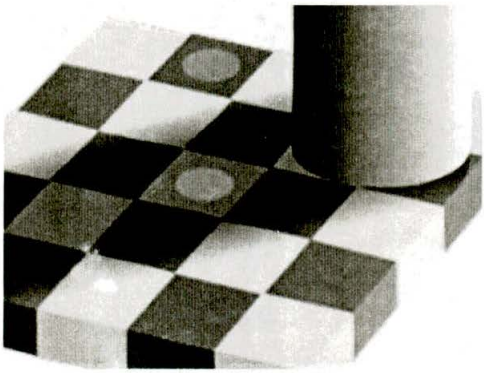
Anexo 45


Ejemplo de estudio
de posicionamiento de
un grupo o una persona
Perito
IT

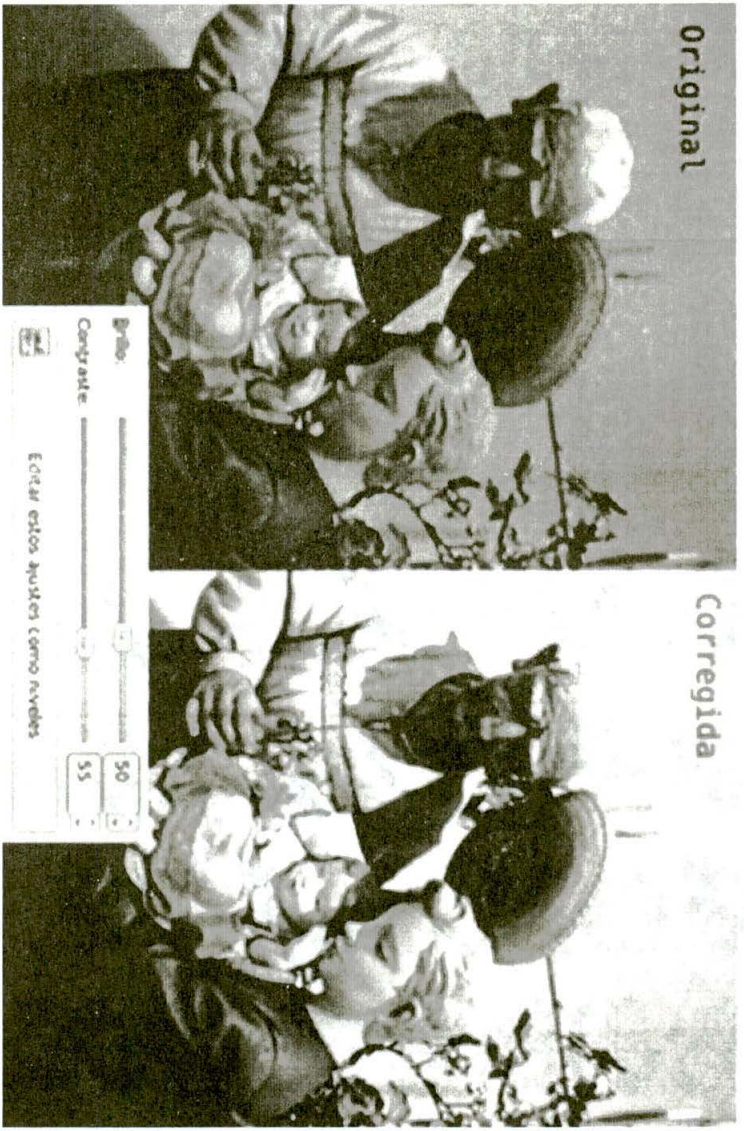
Anexo 46



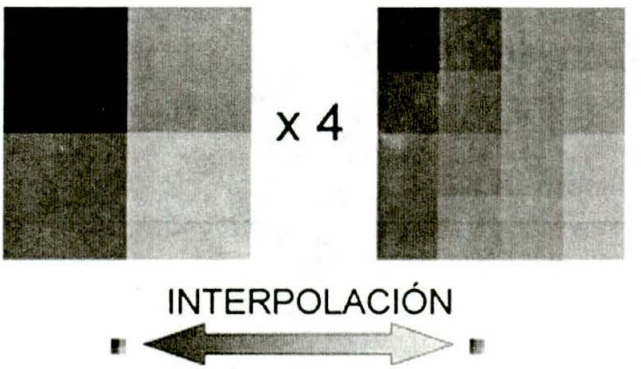
Anexo 47



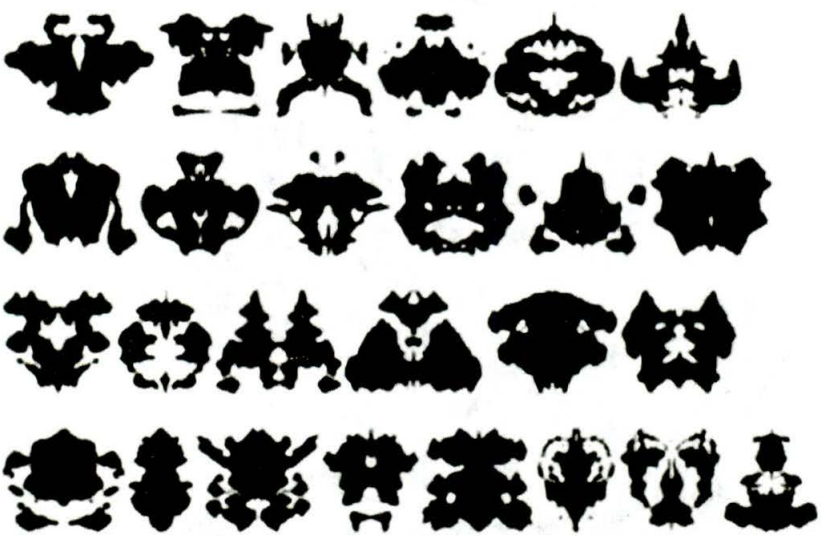
Anexo 48


Original
Corregida
Brillo:
50
Contraste:
55
Editar estos ajustes como niveles

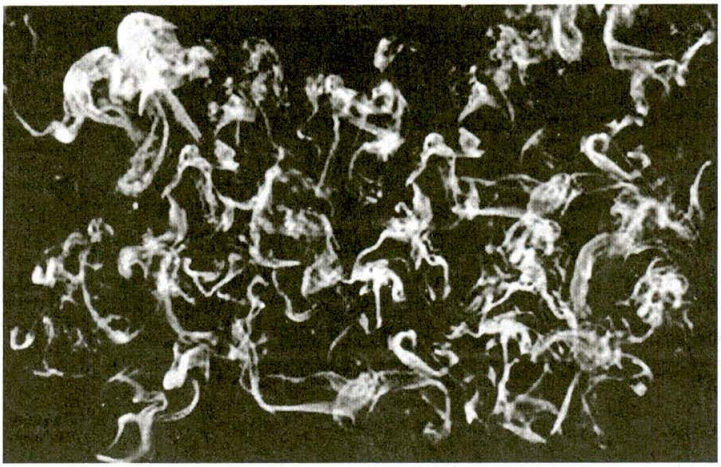
Anexo 49



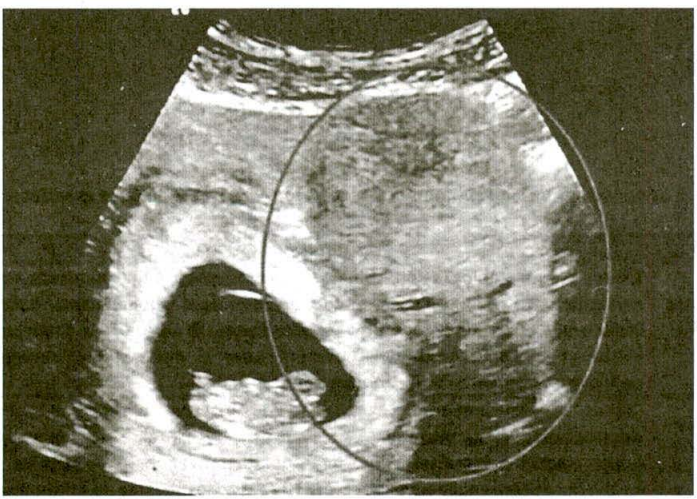
Anexo 50



Anexo 51



Anexo 52



Anexo 53

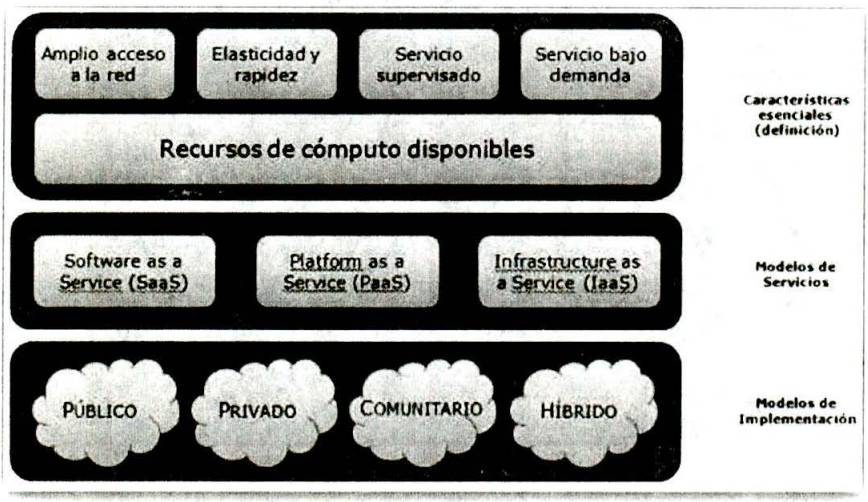


Figura 1 – Representación de la definición de Cloud Computing del NIST.

Anexo 54

Modelos de Servicios

La prestación de servicios de cloud computing puede asociarse a tres modelos específicos:

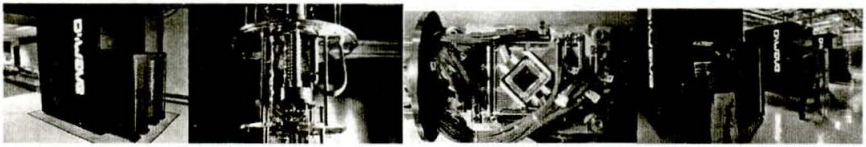
Modelo	Descripción
Infrastructure as a Service (IaaS)	Ofrece al consumidor la provisión de procesamiento, almacenamiento, redes y cualquier otro recurso de cómputo necesario para poder instalar software, incluyendo el sistema operativo y aplicaciones. El usuario no tiene control sobre el sistema de nube subyacente pero si del Sistema operativo y aplicaciones. *Ejemplo: Amazon Web Services EC2.*
Platform as a Service (PaaS)	Ofrece al consumidor la capacidad de ejecutar aplicaciones por éste desarrolladas o contratadas a terceros, a partir de los lenguajes de programación o interfaces provistas por el proveedor. El usuario no tiene control ni sobre el sistema subyacente ni sobre los recursos de Infraestructura

Anexo 55

	de nube. *Ejemplo: Microsoft Azure.*
Software as a Service (SaaS)	Ofrece al consumidor la capacidad de utilizar las aplicaciones del proveedor que se ejecutan sobre la infraestructura en la nube. Las aplicaciones son accedidas desde los dispositivos cliente a través de interfaces, por ejemplo un navegador web. En este caso, el usuario solo tiene acceso a una interfaz de configuración del software provisto. Ejemplo: SalesForce

Tabla 1 – Modelos de provisión de servicios de Cloud Computing.

Anexo 56



OI-29-6-ene-2015-AN

Derecho y Nuevas Tecnologías se trata de una nueva área de estudio que interrelaciona el Derecho con la tecnología, disciplina que generalmente se la ha denominado "Derecho Informático", "Derecho telemático", "Iuscibernética", "Derecho de Internet", también "Derecho tecnológico", "Derecho de las nuevas tecnologías de la información y comunicación - TICS", o "Derecho de la sociedad de la información", etc.

El presente texto aborda la temática de forma clara, con principios y preceptos fundamentales para conocer y aplicar el uso de las Nuevas Tecnologías, valiéndose de la informática jurídica, que goza en el campo del Derecho de su propia autonomía a través de una legislación que ha desarrollado su normativa específica, tanto a nivel mundial, como internamente en cada país, delimitando su ámbito de aplicación, la delincuencia informática, criminalidad informática, falsificación electrónica, etc. Permitiendo así desarrollar el interés de los estudiosos del Derecho, lo cual constituye un aporte al progreso, difusión y comprensión del mismo.

P.V.P $ 28.00 USD.

ISBN: 978-9942-10-247-8

9789942102478

cep
CORPORACIÓN
DE ESTUDIOS Y PUBLICACIONES

UIO Acuña E2-02 y Agama.
Telfs. (593-2) 2221-711 / 2232-693 / 2232-694 / 2232-696
Fax (593-2) 2226-256 Apartado 172100186

GYE Telf. (593-4) 2622-052

CUE Honorato Vásquez 794 y Luis Cordero
Telf. (593-7) 2837-281

www.cep.org.ec ▪ ventas@cep.org.ec

Paéz Rivadeneir
Juan José
1160754