

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 cibercriminalidad	290
Clasificación de delitos informáticos Naciones Unidas	291
RED 24/7.	292
Commonwealth Cybercrime Initiative.	297
Iniciativa de la Mancomunidad para la Cibercriminalidad.	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