

DR. SANTIAGO ACURIO DEL PINO

*PROFESOR DE DERECHO INFORMÁTICO DE LA PUCE
PROFESOR DE MARCO JURÍDICO DE LA SEGURIDAD DE
LA ESPOL
JUEZ DE LA CORTE PROVINCIAL DE PICHINCHA – SALA
PENAL*

Primera Parte Derecho e Informática

1.- La Informática	1
1.1.- Qué es la Informática	1
1.2.- Invasión de la Informática en los últimos tiempos	3
2.- Relaciones entre la Informática y el Derecho	5
2.1.- Informática Jurídica	5
2.1.1.- Clasificación de la Informática Jurídica	6
2.2.- Derecho Informático	7
2.2.1.- Características del Derecho Informático	9
2.2.2.- Contenido del Derecho Informático	10

Segunda Parte Aspectos legales del Comercio Telemático

1.- Introducción al Comercio Telemático	15
2.- Aspectos Preliminares	16
2.1.- La Revolución Digital	16
2.2.- Concepto	19
2.3.- Clases de Comercio Telemático	22
2.4.- Principios Reguladores del Comercio Telemático	23
2.5.- Características del Comercio Telemático	26
2.6.- Proceso de promoción del Comercio Telemático	26
2.7.- Ventajas del comercio telemático	27
3.- Contenido de la Ley de Comercio Electrónico del Ecuador	29
3.1.- Introducción y ámbito de aplicación	29
3.2.- Los mensajes de datos	30

3.3.- De las firmas electrónicas, certificados de firma electrónica, entidades de certificación y organismo de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas	31
3.4.- De los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios e instrumentos públicos	36
3.5.- De la prueba y notificaciones electrónicas	37
3.6.- De las Infracciones Informáticas	38
3.7.- Disposiciones generales	38

Tercera Parte Generalidades de los Delitos Informáticos

1.- Delimitación del Fenómeno de la Delincuencia Informática	39
1.1.- Generalidades	39
1.2.- Campo de acción de la criminalidad informática	40
1.2.1.- Delincuencia informática y Abuso Informático	42
1.2.2.- Criminalidad informática	42
1.3.- Definición y el concepto de Delitos Informáticos	43
1.4.- Factor Criminógeno y Proliferación de esta clase de ilícitos	50
1.4.1.- Desconocimiento de los nuevos sistemas de tratamiento de información	51
1.4.2.- La inexistencia y precariedad de los sistemas de seguridad	52
1.4.3.- La Falta de leyes y normativas especiales	52
1.5.- Porque es atractivo el Delito Informático	53
2.- Sujetos del Delito Informático	54
2.1.- Sujeto Activo	54
2.1.1.- Conociendo al Enemigo	59
2.1.2.- Los hackers y los Crackers	60
2.1.2.1.- Anonimous del Ciberactivismo al Hactivismo	67
2.1.3.- Motivaciones de los Delincuentes Informáticos	72
2.1.4.- Triángulo de la Intrusión	73
2.1.5.- Casos de Referencia	74
2.1.5.1.- Mark Abene “PHIBER OPTIK”	74
2.1.5.2.- Wladimir Levin	75
2.1.5.3.- Kevin Mitnick	75
2.1.5.4.- Robert T. Morris	76

2.1.5.4.-Kevin Poulson	77
2.1.5.5.- CHEN ING-HAU	77
2.1.5.6.- Jérôme Karviel	78
2.1.5.7.- Gary McKinnon	79
2.1.5.8.- Albert González	80
2.1.5.9.- David Kernell, alias “RUBICO”	81
2.1.5.10.- Christopher Chaney “El Hakeraczi”	81
2.2 - Sujeto Pasivo	82
3.- Bien Jurídico Protegido	84
3.1.- Los Bienes Jurídicos Protegidos por los Delito Informáticos	85
4.- Tipos de Delitos informáticos	88
4.1.- - Los fraudes	89
4.1.1.- Noción de Fraude y Defraudación	90
4.1.2.- En cuanto al carácter “Informático” del Fraude	92
4.1.3.- Tipos de Fraudes	93
4.4.- - El robo de servicios	104
4.5.- - El acceso no autorizado a servicios informáticos	104
5.- Situación Internacional	106
5.1.- Organización de Estados Americanos	112
5.2.- La Convención de las Naciones Unidas contra la Delin- cuencia Organizada Transnacional	115
5.3.- Convenio de Cibercriminalidad de la Unión Europea	117
5.4.-Nuevos retos en materia de seguridad	121
5.5.- Seguridad Informática y Normativa	123
6.- El Delito Informático y su realidad penal en el Ecuador	126
6.1.- Tipos de Delitos Informáticos existentes en el Código Pe- nal anterior	130
6.1.1.- Delitos contra la Información Protegida Violación de claves o sistemas de seguridad	130
6.1.2.- Delitos contra la Información Protegida Destrucción o supresión de documentos, programas	132
6.1.3.- Falsificación Electrónica	133
6.1.4.- Daños Informáticos	134
6.1.5.- Fraude Informático	135
6.1.6.- Violaciones al Derecho a la Intimidad (Contraven- ción)	136
6.1.7.- Pornografía Infantil	136

6.1.8.- Interceptación de comunicaciones	138
7.- Tipos Penales en el COIP	138
7.1.- Pornografía Infantil	138
7.2.- Acoso sexual “Grooming”	139
7.3.- Ofertas de servicios sexuales a través de medios electrónicos	140
7.4.- Delitos contra el derecho a la intimidad	141
7.5.- Estafa	141
7.6.- Aprovechamiento de servicios públicos	143
7.7.- Apropiación fraudulenta por medios electrónicos	144
7.8.- Delitos referentes a terminales móviles y su información de identificación	145
7.9.- Delitos contra la identidad	146
7.10.- Revelación ilegal de información en base de datos	147
7.11.- Interceptación ilegal de datos	148
7.12.- Fraude Informático y muleros	149
7.13.- Daños Informáticos, Malware, ataques de DoS y DDoS	150
7.14.- Delitos contra la información pública reservada	151
7.15.- Acceso no autorizado a sistemas informáticos, telemáticos o de telecomunicaciones	152
8.- Problemas de Persecución	153
8.1.- Problemática con la concepción tradicional de tiempo y espacio	153
8.1.1.- Principios de extraterritorialidad	156
A.- Principio de la nacionalidad o personalidad	156
B.- Principio de la defensa	157
C.- Principio de la universalidad y justicia mundial	157
8.2.- Anonimato del Sujeto Activo	158
9.- Temas Pendientes	159
9.1.- Proyecto de Reforma que se propuso para que fuera incluido en el COIP	159

Cuarta Parte Investigación, Informática Forense y Evidencia Digital

1.- Introducción	167
------------------	-----

2.- La Investigación y la Prueba de los Delitos Informáticos	171
2.1.- Investigación Penal	175
2.1.1.- Características de la Investigación Penal	176
2.1.2.- Extensión del término	178
2.2.- Rol del Sistema Informático en el ITER CRIMINIS	180
2.2.1.- Hardware o Elementos Físicos	181
2.2.2.- Información	181
3.- Las Ciencias Forenses	182
4.- La Informática Forense	183
5.- Evidencia Digital	185
5.1.- Fuentes de la Evidencia Digital	187
5.1.1.- Incautación de Equipos Informáticos o Electrónicos	190
5.1.1.1.- Derechos a tener en cuenta durante la incautación y registro de equipos tecnológicos	191
5.1.2.- Teléfonos Inalámbricos, Celulares, Smartfones, Cámaras Digitales	192
5.1.3.- Máquinas de Fax	194
5.1.4.- Dispositivos de Almacenamiento	194
5.2.- Evidencia Digital Constante y Volátil	195
5.3.- La Dinámica de la Evidencia	196
6.- Relevancia de la Evidencia Digital el Proceso Penal Ecuatoriano	200
6.1.- Entendimiento de la Evidencia Digital	200
6.2.- Relevancia y Admisibilidad de la Evidencia Digital	203
6.3.- Legislación Procesal	213
6.3.1.- Código de Procedimiento Penal	213
6.3.2.- Normas del Código Orgánico Integral Penal	215
6.4.- Valides de la Evidencia Digital (Código Integral Penal, Ley de Comercio Electrónico y Código Orgánico de la Función Judicial)	220
7.- Claves para hacer efectivo el Testimonio experto	222
7.1.- Primer paso Calibrar el nivel de conocimientos del Fiscal en temas de Delitos Informáticos	223
7.2.- Segundo Paso Discutir el caso con el Fiscal	224
7.3.- Tercer Paso Calibrar a la Defensa	225
7.4.- Cuarto Paso Revisar los Informes	226

7.5.- Quinto Paso Preséntese usted mismo como un testigo confiable	226
7.5.1.- Examinación Directa	227
7.5.2.- El contra examen	227
7.6.- Sexto Paso Que el árbol no les impida ver el bosque	228
7.7.- Corolario	229
8.- Roles en la Investigación	230
8.1.- Peritos Informáticos	233
9.- Incidentes de Seguridad	238
9.1.- Amenazas deliberadas a la seguridad de la información	241
9.2.- Ataques pasivos	243
9.3.- Ataques activos	244
10.- Procedimiento de Operaciones Estándar	245
10.1.- Investigación en la Escena del Delito	248
10.2.- Reconstrucción de la Escena del Delito	250
11.- Fases de la Investigación Forense	252
11.1.- Recolección	252
11.2.- Preservación	252
11.3.- Filtrado	252
11.4.- Presentación	253
12.- Metodología de búsqueda y resguardo de la Evidencia Digital	253
12.1.- Introducción	253
12.2.- Metodología de procesamiento de Evidencia	255
12.3.- Análisis en Profundo	258
12.3.1.- Identificación de los medios digitales	260
12.3.2.- Minimizar la escena priorizando los dispositivos de almacenamiento relevantes	260
12.3.3.- Recolectar todos los dispositivos de medios digitales	261
12.3.4.- Asegurar los dispositivos de medios digitales	261
12.3.5.- Se debe jalar el cable de poder o no se debe hacerlo	261
12.4.- Enfoque progresivo de búsqueda y recuperación de la evidencia digital	263
13.- Manual de Manejo de Evidencias Digitales y Entornos Informáticos	264
14.- Rastreo del Correo Electrónico	267
14.1.- ¿Por dónde va un correo electrónico?	269
14.2.- Encabezamientos del Correo Electrónico	270

14.2.1.- Direcciones IP y Nombres de Dominio	270
14.2.1.- Encabezado General	273
14.2.2.-Encabezado Técnico	274
14.3.- Para que puede ser usado el correo electrónico	275
14.3.1.- Como instrumento	276
14.3.2.-Como objeto del delito	276
14.3.3.- Como medio de prueba	276
15.- Glosario de Términos	277
16.- Bibliografía	283
ANEXOS	295