

PERITAJE INFORMÁTICO Y TECNOLÓGICO

Rafael López Rivera

***Perito Informático y Tecnológico
Mediador Civil y Mercantil***

ÍNDICE DEL DOCUMENTO

1 *** GENERALIDADES DEL PERITAJE ***	17
1.1 Objetivo de este bloque temático	18
2 Introducción	19
2.1 ¿Qué es un perito informático y tecnológico?.....	19
2.2 ¿Qué debe ser un perito?	21
2.3 ¿Qué debe conocer un perito?	22
2.4 Clasificación.....	23
2.5 Ámbitos de Actuación.....	29
2.6 Principios Generales a considerar en las actuaciones.	33
2.7 Proceso Global del Peritaje	38
3 *** TIPOLOGÍAS DEL PERITAJE ***	45
3.1 Objetivo de este bloque temático	46
4 El Perito Forense Informático y Tecnológico	47
4.1 El Peritaje Forense Informático y Tecnológico	47
4.2 Proceso de “Actuación” en un Peritaje Forense Informático y Tecnológico	50
5 Perito de Gestión o de Management.....	58
5.1 El Peritaje Tecnológico de Gestión o de Management	58
5.2 Estándares en el Peritaje de Gestión	61
5.3 El proceso de “Actuación” en un Peritaje de Gestión.....	68
5.4 El Peritaje de Gestión como Auditoría y Normativa.	79
6 Perito Mediador Tecnológico	82
6.1 La Mediación	82
6.2 Herramientas de la Mediación	88
6.3 El Mediador.....	90
6.4 El Proceso de la Mediación.....	93
6.5 Métodos de Mediación.....	99
7 Perito Tasador	100
7.1 La Tasación	100
7.2 Ámbitos de aplicación de la Tasación Tecnológica.....	101
7.3 El Perito Tasador Informático o Tecnológico	102
7.4 Métodos de Valoración	105

8 * NORMATIVA LEGAL DEL PERITAJE *** 107**

- 8.1 Objetivo de este bloque temático 108
- 8.2 Sobre la Legislación y los artículos 108
- 8.3 Las Leyes referenciadas 109

9 Contexto General..... 110

- 9.1 La razón de ser de los Peritos y sus Informes 110
- 9.2 Intervención de los Peritos 112
- 9.3 El Principio de Oportunidad - Contexto y aplicación 112
- 9.4 Principios técnicos derivados 113

10 Sobre la Prueba 114

- 10.1 Introducción 114
- 10.2 ¿Qué es un medio de prueba? 115
- 10.3 Derechos concernientes a la Prueba 117
- 10.4 ¿Cómo se consideran los diferentes Medios de Prueba? 121

11 Sobre los Peritos 124

- 11.1 ¿Qué es un perito? 124
- 11.2 ¿Qué debe ser un perito? 124
- 11.3 La acreditación del perito como persona entendida 125
- 11.4 De la abstención, la recusación y las tachas 126
- 11.5 Proceso de Actuación del Perito Judicial 129
- 11.6 Derechos y deberes de los peritos 132
- 11.7 Responsabilidades del perito 137

12 Sobre el Procedimiento Probatorio 145

- 12.1 Principios del Procedimiento Probatorio 145
- 12.2 Etapas del Procedimiento Probatorio 148
- 12.3 El Informe o Dictamen Pericial 151

13 Extensión sobre los delitos de carácter tecnológicos... 156

- 13.1 Delitos informáticos o tecnológicos 156
- 13.2 Equiparación de los delitos virtuales a los delitos reales 159
- 13.3 Regulaciones específicas sobre Informática e Internet 161
- 13.4 El “peso” del testimonio del Perito Tecnológico 161
- 13.5 Delitos de menores (los tres ING’s) y el Phishing 162

14 * LA RECOPIACIÓN DE EVIDENCIAS *** 171**

14.1 Objetivo de este bloque temático 172

15 La Actuación Pericial 173

15.1 La Evidencia Informática o Telemática 174

15.2 La Cadena de Custodia 177

15.3 Proceso de Identificación y Registro en la actuación pericial 179

15.4 Los pasos a seguir en la Actuación Pericial 180

15.5 Intervención del Fedatario Público en la Cadena de Custodia 183

16 Lo esencial de las Directrices RFC 3227 186

16.1 Las Actuaciones Básicas 186

16.2 Conceptos 187

17 Contenido de las Directrices - RFC 3227 190

17.1 Cap. 0 - Resumen 190

17.2 Cap. 1 - Introducción 190

17.3 Cap. 2 - Principios Guía en la Recopilación de Evidencias .. 192

17.4 Cap. 3 - El procedimiento de recopilación 195

17.5 Cap. 4 - Procedimiento de archivo (almacenamiento) 196

17.6 Cap. 5 - Herramientas que se necesitarán 196

17.7 Cap. 6 - Referencias 197

17.8 Cap. 7 – Agradecimientos 197

17.9 Cap. 8 – Consideraciones de Seguridad 197

17.10 Cap. 9 - Direcciones de los autores 198

17.11 Cap. 10 – Acuerdo completo de Copyright 198

18 Lo esencial de la ISO/IEC 27037 199

18.1 Introducción 199

18.2 Alcance 199

18.3 Los principios básicos en los que se basa la norma 200

18.4 Procesos en los que se dividen las Actuaciones 201

18.5 El Análisis 202

19 Contenido Directrices – ISO/IEC 27037 203

19.1	Introducción	203
19.2	Cap. 7 - La Cadena de Custodia.....	204
19.3	Cap. 10 – Acciones Iniciales.....	204
19.4	Cap. 11 - Prioridad de recolección, Orden de Volatilidad	205
19.5	Cap. 12 - Equipos, medios y dispositivos periféricos.	206
19.6	Cap. 13 – Ordenadores y dispositivos en red.....	211
19.7	Cap. 14 – Dispositivos móviles.....	213

20 * LA ELABORACIÓN DE UN INFORME PERICIAL *** .. 217**

20.1	Objetivo de esta Guía de Elaboración	218
20.2	Objetivos derivados.....	218
20.3	Informe o Dictamen	218
20.4	Estructura de la guía de elaboración de informes	219

21 El Informe 220

21.1	Contexto Sistemático	220
21.2	Requisitos Generales.....	221
21.3	Título.....	221
21.4	Documento	222
21.5	Visado y Normativa	224
21.6	Confidencialidad	225
21.7	Uso no autorizado	226
21.8	Firma y anulación de espacios vacíos	227
21.9	Paginación – Cabecera y Pie de página	228

22 Identificación o Encargo 229

22.1	Objetivo de la Identificación.....	229
22.2	Título y su código de referencia o de identificación.....	229
22.3	Destinatario y Peticionario.....	230
22.4	El Profesional (el Perito).....	231
22.5	Localización Temporal	232
22.6	Localización Espacial	232

23 Declaraciones	234
23.1 Generalidades y contenido	234
23.2 Declaración de Abstención y Tachas	234
23.3 Declaración de Juramento o de Promesa	236
24 Índice del Informe	237
24.1 Generalidades y contenido	237
25 Cuerpo del Informe.....	238
25.1 Generalidades y contenido	238
25.2 Objeto.....	241
25.3 Alcance.....	244
25.4 Antecedentes	245
25.5 Consideraciones	247
25.6 Documentos de Referencia	249
25.7 Terminología y Abreviaturas	250
25.8 Actuaciones.....	251
25.9 Análisis y Dictamen.....	255
25.10 Conclusiones	258
25.11 Contenido mínimo imprescindible de un informe pericial	262
26 Visado de los informes periciales.....	263
26.1 Introducción	263
26.2 Documentos que componen el Visado.....	265
27 *** LA SEGURIDAD INFORMÁTICA ***	269
27.1 Objetivo de este bloque temático	270
27.2 La Seguridad Informática.....	271
27.3 ¿De qué protege la Seguridad Informática?	275
28 ¿Qué medios dispone la Seguridad Informática?	277
28.1 Las Políticas de Seguridad Informática.....	277
28.2 Los Sistemas de Detección de Intrusos (SDI).....	278
28.3 Las Auditorías de Seguridad Informática	280
28.4 Los test en búsqueda de vulnerabilidades. Pentest.....	282
28.5 Los Firewalls.....	284
28.6 Los Antivirus.....	285

29 Incidentes Informáticos	286
29.1 Tipología y clasificación de los incidentes informáticos	286
29.2 ¿Cómo protegerse de los Incidentes Informáticos?	291
29.3 El proceso de “Respuesta ante un Incidente de Seguridad”... ..	292
30 ISO/IEC 17799 Buenas Prácticas de Seguridad de la Información.....	299
30.1 ISO/IEC 17799 origen y objetivo	299
30.2 Estructura básica	299
31 ISO/IEC 15408 Un estándar para Seguridad.....	301
31.1 Reglamentación Española de Certificación, Orden PRE/2740/2007	301
31.2 Norma ISO/IEC 15408, Common Criteria	302
31.3 Norma ISO/IEC 18045, Methodology for IT Evaluation	309
32 ENS - Esquema Nacional de Seguridad	311
33 LOPD – Ley Orgánica de Protección de Datos	313