

## Contenido

	Agradecimientos	9
	Prólogo a la primera edición	11
	Prólogo a la segunda edición	13
1	<b>Introducción: la informática forense, una disciplina técnico-legal</b>	
	Introducción	19
	Definiciones	19
	Evidencia digital	21
	Procedimientos	22
	Herramientas	24
	Retos	25
	Conclusiones	27
2	<b>La computación forense. una perspectiva de tres roles: el intruso, el administrador y el investigador</b>	
	Introducción	31
	2.1 Las evidencias tradicionales	31
	2.2 El informático forense	31
	2.3 La faceta del intruso	32
	2.3.1 Los roles del intruso	32
	2.4 El investigador	33
	<i>Resumen</i>	34
3	<b>El intruso y sus técnicas</b>	
	Introducción	39
	3.1 Breve historia de los hackers	39
	3.2 La mente de los intrusos	44
	3.2.1 Técnicas básicas de hacking	51
	3.2.2 Técnicas avanzadas de hacking	58
	3.3 Identificación de rastros de los ataques	63
	<i>Resumen</i>	69
	<b>PREGUNTAS Y EJERCICIOS</b>	70

## El administrador y la infraestructura de la seguridad informática

Introducción	73
4.1 Roles y responsabilidades del administrador de sistemas	73
4.2 Consideraciones de diseño de infraestructuras de seguridad	78
4.2.1 Inseguridad centralizada	78
4.2.2 Inseguridad descentralizada	80
4.2.3 Inseguridad en el Web	84
4.2.4 Inseguridad orientada a los servicios	86
4.2.5 Evolución de la inseguridad informática	88
4.3 Técnicas básicas para el diseño y la generación del rastro	90
4.4 Auditabilidad y trazabilidad	93
4.4.1 Auditabilidad	93
4.4.2 Trazabilidad	96
4.4.3 Niveles de trazabilidad	97
4.5 Consideraciones jurídicas y aspectos de los rastros en las plataformas tecnológicas	99
4.5.1 Autenticidad	100
4.5.2 Confiabilidad	101
4.5.3 Suficiencia	102
4.5.4 Conformidad con las leyes y las regulaciones de la administración de justicia	103
<i>Resumen</i>	104
<b>PREGUNTAS Y EJERCICIOS</b>	105

## El investigador y la criminalística digital

Introducción	109
5.1 Introducción a la criminalística digital	110
5.2 Roles y responsabilidades del investigador forense en informática	115
5.3 Modelos y procedimientos para adelantar investigaciones forenses en informática	118
5.3.1 Algunos modelos de investigaciones forenses en informática	119
5.4 Credenciales para los investigadores forenses en informática	124
5.4.1 IACIS	126
5.4.2 HTCEN	127
5.4.3 IISFA	128
5.4.4 ISFCE	128
5.4.5 SANS Institute	129
5.5 Informes de investigación y presentación de pruebas informáticas	133
5.5.1 Teoría básica de la preparación de informes	134
5.5.2 Consideraciones básicas sobre los informes periciales	136
5.5.3 Estructura base de un informe pericial	137
5.5.4 Estructura general	137
<i>Resumen</i>	140
<b>PREGUNTAS Y EJERCICIOS</b>	141

## 6 Retos y riesgos emergentes para la computación forense

Introducción	145
6.1 La formación de especialistas en informática forense	145
6.2 Confiabilidad de las herramientas forenses en informática	149
6.3 Técnicas antiforenses y sus implicaciones para las investigaciones actuales y futuras	152
6.3.1 Destrucción de la evidencia	155
6.4 Cibercrimen y ciberterrorismo: amenazas estratégicas y tácticas de las organizaciones modernas	156
6.4.1 Ciberterrorismo	157
6.4.2 Cibercrimen: viejos hábitos del mundo offline, nuevas armas en el mundo online	159
6.4.3 Retos tecnológicos para los investigadores forenses en informática	161
6.4.4 Archivos cifrados	161
6.4.5 Esteganografía en video	162
6.4.6 Rastros en ambientes virtuales	163
6.4.7 Información almacenada electrónicamente en memoria volátil	164
6.4.8 Análisis de sistemas en vivo	164
<i>Resumen</i>	165
<b>PREGUNTAS Y EJERCICIOS</b>	166

## 7 Análisis forense en entornos y tecnologías emergentes

Introducción	171
7.1 Análisis forense en un ecosistema tecnológico: redes sociales, tecnologías móviles y computación en la nube	172
7.1.1 Entendiendo la computación en la nube	173
7.1.2 Seguridad y control en la nube	176
7.1.3 Análisis forense en un ecosistema tecnológico: Consideraciones básicas	177
7.1.4 Modelo conceptual de análisis forense en un ecosistema tecnológico	181
<i>Reflexiones</i>	186
7.2 Forense en redes sociales	187
7.2.1 Reto forense en medios sociales digitales	188
7.2.2 Las cuatro “P”	189
7.2.3 El proceso forense digital estándar	190
7.2.4 Fuentes de información en los medios sociales digitales	192
<i>Reflexiones</i>	193
7.3 Unidades de estado sólido. El reto forense en el mundo de los semiconductores	194
7.3.1 Las memorias flash (TAL 2002)	195
7.3.2 Sistemas de archivos para memorias flash	197
7.3.3 Unidades de estado sólido	199
7.3.4 Retos de las unidades de estado sólido para la computación forense	201
<i>Reflexiones finales</i>	202
7.4 iPhone: un reto para la informática forense por Andrea Ariza, Juan Ruiz y Jeimy Cano	204

7.4.1	¿Qué es el iPhone?	205
7.4.2	Problemas de seguridad en el iPhone	207
7.4.3	Informática forense en teléfonos inteligentes	208
7.4.4	Guía metodológica para realizar análisis forense sobre dispositivos móviles (Caso de estudio: iPhone)	213
7.4.5	Evidencia relevante	220
	<i>Reflexiones</i>	220

8

## **Anexos**

8.1.	Tratamiento de la evidencia digital	229
8.2	Fuentes potenciales de evidencia digital	237
8.3	Evidencia digital en la práctica	239
8.4	Características para seleccionar un informático forense	240
8.5	Preguntas para llevar a la audiencia	243
8.6	Consejos prácticos para sustentar un reporte técnico en una audiencia	246
8.7	Reflexiones sobre la norma ISO/IEC 27037:2012	248
8.8	Formulario Actuación del primer respondiente	256
8.9	Formulario Documentación escena del crimen	257
8.10	Entrevista al propietario del dispositivo iPhone	258
8.11	Formulario Identificación del dispositivo vulnerado	259
8.12.	Formulario Documentación evidencia digital	260

9

## **Bibliografía**

261