

# Contenido

## CAPÍTULO 1

<b>Delitos y usuarios informáticos .....</b>	<b>1</b>
<b>1.1 ¿Qué es un delito informático? ..</b>	<b>2</b>
1.1.1 Propuesta de definición para un delito informático .....	3
1.2 Tipos de delitos informáticos .....	4
1.3 Tipos de usuarios en sistemas informáticos .....	17
1.4 Peritajes psicológicos y su relación con la informática forense .....	21

## CAPÍTULO 2

### **Fundamentos De La Informática Forense**

.....	25
<b>2.1 Fundamentos de los sistemas operativos Windows .....</b>	<b>25</b>
2.1.1 Sistemas de archivos NTFS .....	25
2.1.2 Sistema de jerarquía de archivos en sistemas NTFS .....	26
2.1.3 Procesos en los sistemas operativos Windows .....	27
2.1.4 Servicios en los sistemas operativos Windows .....	28
2.1.5 Registros en los sistemas operativos Windows .....	29
2.1.6 Eventos en los sistemas de archivos NTFS .....	30
<b>2.2 Fundamentos de los sistemas operativos GNU/Linux .....</b>	<b>31</b>
2.2.1 Sistemas de archivos Ext4 .....	31
2.2.2 Jerarquía de archivos en sistemas Ext4 .....	32
2.2.3 Demonios en sistemas de archivos Ext4 .....	34

<b>2.2.4 Usuarios en los sistemas operativos GNU/Linux .....</b>	<b>35</b>
2.2.5 Contraseñas de usuarios en GNU/Linux .....	37
2.2.6 Grupos de usuarios en GNU/Linux .....	37
<b>2.3 Fundamentos de los sistemas operativos MacOS .....</b>	<b>38</b>
2.3.1 Sistema de archivos APFS .....	38
2.3.2 Estructura de los sistemas de archivos APFS .....	41
<b>2.4 Fundamentos de los sistemas operativos iOS .....</b>	<b>42</b>
2.4.1 Estructura de capas del sistema operativo iOS .....	42
2.4.2 Cifrado de los sistemas operativos iOS .....	45
<b>2.5 Fundamentos de los sistemas operativos Android .....</b>	<b>46</b>
2.5.1 Arquitectura de los sistemas Android .....	47
2.5.2 Particiones de los sistemas operativos Android .....	50
2.5.3 Modelo de permiso .....	51
<b>2.6 Particiones en discos duros .....</b>	<b>51</b>
<b>2.7 Máquinas virtuales .....</b>	<b>52</b>
2.7.1 VMWare Workstation Pro .....	54
2.7.1.1 Instalaciones en entorno Windows .....	55
2.7.1.2 Instalación en entorno GNU/Linux .....	65
2.7.2 Oracle Virtual Box .....	70
2.7.2.1 Instalaciones en entorno Windows .....	70

CAPÍTULO 3

**Introducción a la Informática forense** 75

3.1 Fases de una investigación en informática forense ..... 77

3.2 Evidencia digital ..... 81

3.2.1 Características de las evidencias digitales ..... 82

3.3 Información volátil y no volátil ... 84

3.4 Incidentes de ciberseguridad y su respuesta ..... 85

3.4.1 Equipos de respuesta a incidentes ..... 88

3.4.2 Estándares internacionales .... 91

3.5 Equipos de seguridad informática 93

3.5.1 Blue Team ..... 93

3.5.2 Red Team ..... 94

3.5.3 Purple Team ..... 94

3.6 Funciones hash ..... 95

3.7 Números mágicos ..... 97

3.8 Metadatos ..... 98

3.8.1 Ciclo de vida de los metadatos 99

3.9 Criptografía y esteganografía ....100

3.9.1 Criptografía simétrica .....101

3.9.2 Criptografía asimétrica .....101

3.10 Análisis de riesgos .....103

3.11 Marco de trabajo OSINT .....108

3.12 Acuerdo de confidencialidad ....109

CAPÍTULO 4

**Formación de un perito en Informática forense** ..... 113

4.1 ¿Qué es un perito en informática forense? .....113

4.2 Tipos de peritos en informática .114

4.3 Formación requerida .....114

4.4 Perfil de un perito en informática119

4.5 Certificaciones internacionales ..121

CAPÍTULO 5

**Generación de ambientes controlados para la Investigación de delitos Informáticos** ..... 123

5.1 USB de arranque .....125

5.2 Herramientas no dependientes del sistema operativo .....126

5.3 Creación de ambientes controlados para el análisis forense en sistemas Windows ..... 129

5.3.1 Fase de adquisición de indicios 130

5.3.1.1 Adquisición de información

volátil ..... 130

5.3.1.2 Adquisición de información No volátil ..... 130

5.3.2 Fase de análisis de indicios y extracción de evidencias ..... 131

5.4 Creación de ambientes controlados para el análisis forense en sistemas GNU/Linux ..... 135

5.4.1 Fase de adquisición de indicios 137

5.4.1.1 Adquisición de información volátil ..... 137

5.4.1.2 Adquisición de información No volátil ..... 137

5.4.2 Fase de análisis de indicios y extracción de evidencias ..... 138

5.5 Creación de ambientes controlados para el análisis forense en sistemas MacOS e iOS ..... 142

5.5.1 Fase de adquisición de indicios 142

5.5.1.1 Adquisición de información volátil ..... 142

5.5.1.2 Adquisición de información No volátil ..... 143

5.5.2 Fase de análisis de indicios y extracción de evidencias ..... 143

5.6 Creación de ambientes controlados para el análisis forense en sistemas Android ..... 146

5.6.1 Fase de adquisición de indicios 147

5.6.2 Fase de análisis de indicios y extracción de evidencias ..... 148

5.6.3 Emuladores ..... 149

5.6.4 Distribuciones especializadas para análisis forense en dispositivos móviles ..... 152

CAPÍTULO 6

**Marco de trabajo para el análisis forense de delitos informáticos; EDAPREHD** 155

6.1 Generalidades del marco de trabajo EDAPREHD ..... 155

6.2 Fase 1: estudio del caso ..... 156

6.3 Fase 2: documentación de la escena del delito ..... 160

6.4 Fase 3: adquisición de indicios ..165

6.5 Fase 4: preservación y traslado de indicios ..... 201

6.6 Fase 5: análisis de indicios y extracción de evidencias ..... 208

6.6.1 Estándares internacionales ..... 208

6.6.2 Análisis de entornos Windows 213  
 6.6.3 Análisis de entornos  
 GNU/Linux ..... 232  
 6.6.4 Análisis de entornos MacOS ... 238  
 6.6.5 Análisis de dispositivos  
 móviles ..... 244  
 6.6.5.1 Análisis en sistemas iOS ..... 248  
 6.7 Fase 6: determinación y  
 documentación de hallazgos ..... 258  
 6.8 Fase 7: elaboración de dictamen  
 pericial y juicio experto ..... 259  
 6.9 Expectativas ..... 268

CAPÍTULO 7

**Implementación del marco de trabajo**

**EDAPREHD** ..... 269  
 7.1 Implementación del marco de trabajo  
 EDAPREHD en un escenario de  
 ransomware ..... 269  
 7.1.1 Contexto del escenario ..... 269  
 7.1.2 Estudio del caso ..... 270  
 7.1.3 Documentación de la escena del  
 delito ..... 271  
 7.1.4 Adquisición de indicios ..... 271  
 7.1.5 Preservación y traslado de  
 indicios ..... 272  
 7.1.6 Análisis de indicios y extracción de  
 evidencias ..... 273  
 7.1.7 Determinación de hallazgos ... 285  
 7.2 Implementación del marco de trabajo  
 EDAPREHD en escenario de accesos no  
 autorizados ..... 286  
 7.2.1 Contexto del escenario ..... 286  
 7.2.2 Estudio del caso ..... 286  
 7.2.3 Documentación de escena del  
 delito ..... 290  
 7.2.4 Adquisición de indicios ..... 290  
 7.2.5 Preservación y traslado de  
 indicios ..... 292  
 7.2.6 Análisis de indicios y extracción de  
 evidencias ..... 293  
 7.2.7 Determinación de hallazgos ... 302  
 7.3 Implementación del marco de trabajo  
 EDAPREHD en escenario de malware  
 para dispositivos móviles ..... 303  
 7.3.1 Contexto del escenario ..... 303  
 7.3.2 Estudio del caso ..... 304  
 7.3.3 Documentación de escena del  
 delito ..... 305  
 7.3.4 Adquisición de indicios ..... 305

7.3.5 Preservación y traslado de  
 indicios ..... 306  
 7.3.6 Análisis de indicios y extracción de  
 evidencias ..... 307  
 7.3.7 Determinación de hallazgos .... 318  
 7.4 Efectividad del marco de trabajo  
 EDAPREHD ..... 319

CAPÍTULO 8

**Legislaciones relacionadas a la**

**informática forense** ..... 321  
 8.1 marco legal en México ..... 321  
 8.2 propuesta a las legislaciones en  
 México ..... 324

Capítulo 9

**Información forense; actualidad y**

**proyección** ..... 327  
 9.1 Presente de la informática  
 forense ..... 327  
 9.2 La informática forense; su evolución  
 y futuro ..... 329  
 9.2.1 La inteligencia artificial en la  
 informática forense ..... 330  
 9.2.2 El aprendizaje automático en la  
 informática forense ..... 331  
 9.2.3 La informática forense en  
 la OT ..... 322  
 9.2.4 La informática forense en  
 el IoT ..... 333  
 9.2.5 La informática forense en  
 ambientes de nube ..... 335

**Glosario** ..... 337