

Índice

Agradecimientos	V
Prólogo	XVII

CAPÍTULO I: LA CIBERSEGURIDAD

1. Introducción	1
2. Definición de ciberseguridad	2
2.1. Presencia, importancia y concepciones de la ciberseguridad	4
2.2. La ciberseguridad y su influencia en los derechos humanos	6
2.3. Los ciberataques	10
2.4. Phishing	11
2.4.1. Ataques de malware	11
2.4.2. Ransomware o secuestro de datos	12
2.5. Descargas automáticas	12
2.5.1. Troyano	12
2.5.2. Ataques a la Web	13
2.5.3. Inyección SQL	13
2.5.4. XSS o Cross Site Scripting	13
2.6. Tipos de seguridad informática	13
2.6.1. Seguridad de hardware	13
2.6.2. Seguridad de software	14
2.6.3. Seguridad en la red	14
2.7. Importancia de la ciberseguridad en la empresa	14

CAPÍTULO II: AMENAZAS, DESAFÍOS Y ATAQUES EN EL MUNDO ACTUAL

1. El alcance de la responsabilidad jurídica por daños causados por la inteligencia artificial	21
2. Menores de edad. La protección de su derecho a la intimidad en la era digital	21
3. Medios de comunicación social y el derecho al olvido	27

CAPÍTULO III: DESAFÍOS EN EL MUNDO DIGITAL ACTUAL DESDE LA PERSPECTIVA DEL DERECHO

1. Privacidad en riesgo	31
2. Ciberseguridad y protección de datos	32
3. Propiedad intelectual en la era digital	33
4. Responsabilidad legal de las plataformas en línea	33
5. Jurisdicción transfronteriza	33
6. Regulación de la inteligencia artificial	34

CAPÍTULO IV: HISTORIA DE LA CIBERSEGURIDAD

1. Introducción	37
2. Desarrollo	38
2.1. Surgimiento de las redes de computadoras	39
2.2. Desarrollo de la criptografía moderna	39
2.3. Nacimiento de los virus informático	39
2.4. Concientización y desarrollo de políticas de seguridad	39
2.5. Primeros pasos hacia la ciberseguridad empresarial	40
2.6. Ciberataques	42
2.6.1. Iloveyou	43
2.6.2. Conficker	44
2.6.3. Stuxnet	45
2.6.4. Petya	47
2.6.5. Wannacry	49
2.6.6. Aparición de Anonymous	50
3. Actualidad en la prevención	52
4. Inteligencia artificial	53

CAPÍTULO V: PRINCIPIOS Y FUNDAMENTOS DE LA CYBERSEGURIDAD

1. Principios	60
1.1. Confidencialidad	60
1.2. Integridad	60
1.3. Disponibilidad	61
1.4. Autenticación	62
1.5. Autorización	63

1.6. Auditabilidad	63
2. Fundamentos	64
2.1. Firewalls y protección de redes	65
2.2. Antivirus y antimalware	65
2.3. Cifrado de datos	66
2.4. Gestión de accesos	67
2.5. Actualizaciones de seguridad	68
2.6. Concientización del usuario	69
2.7. Monitorización y respuesta rápida	69

CAPÍTULO VI: TRIÁNGULO DE LA SEGURIDAD: CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

1. Conceptos básicos	73
1.1. Informática	73
1.2. Redes	74
1.3. Seguridad informática	75
1.4. Confidencialidad	79
1.5. Integridad	80
1.6. Disponibilidad	80
2. Interrelación del triangulo	81
3. Intersección del triangulo	82
3.1. Confidencialidad	82
3.2. Integridad	82
3.3. Disponibilidad	83
4. Aplicación en redes	83

CAPÍTULO VII: TIPOS DE ATAQUES CIBERNÉTICOS EN LOS ÚLTIMOS AÑOS

1. Principales tipos de ataques informáticos	87
1.1. ¿Por qué los hackers y los ciberdelincuentes usan malware?	89
1.2. ¿Cómo protegerse de los ataques de malware?	89
2. Phishing	90
2.1. Tipos de ataques de phishing:	91
3. Ransomware	92
3.1. ¿Cuántas clases diferentes de ransomware existen?	93
3.2. ¿Cómo protegerse contra el ransomware?	94

4. Inyección SQL	94
4.1. DDoS	95
5. Caza de ballenas	95
5.1. Spear Phishing	95

CAPÍTULO VIII: TENDENCIAS Y AVANCES EN LA CIBERSEGURIDAD

1. Ciberseguridad en la nube y virtualización	99
2. Ciberseguridad en la virtualización	100
3. Internet de las cosas y su impacto en la seguridad	101
4. Normativa y regulación de la ciberseguridad	103
4.1. Normativa internacional	104
4.2. Normativa nacional	104
4.2.1. Constitución del Ecuador	105
4.2.2. Ley Orgánica de Protección de Datos	105
4.2.3. Ley Orgánica de Telecomunicaciones	106
4.2.4. Código Orgánico Integral Penal	106

CAPÍTULO IX: LA CIBERSEGURIDAD: HERRAMIENTAS DE ATAQUE Y MÉTODOS DE DEFENSA

1. Desafíos para la regulación legal	114
2. La necesidad de una regulación global coordinada	117
3. Diferencia entre Contrato electrónico y Contrato informático	120

CAPÍTULO X: TRATAMIENTO INTERNACIONAL DEL DELITO INFORMÁTICO – EUROPA – LA UNIÓN EUROPEA

1. Tratamiento internacional del delito informático	123
1.2. Europa. La Unión Europea	123
2. Tratado de Ámsterdam	124
3. Convenio de Budapest	127
4. Centro europeo de ciberdelincuencia	129
5. Directiva sobre las redes y sistemas de información	132
6. Reglamento de Ciberresistencia	133

**CAPÍTULO XI: TRATAMIENTO DEL DELITO
INFORMÁTICO: ASIA**

1. Asia	137
2. Brechas internacionales	138
3. Convenio de Budapest	140
4. La ASEAN	140
5. Legislación Japonesa	141
6. Legislación China	142
7. Legislación de Corea del Sur	143
8. Legislación de Tailandia	144
9. Legislación Rusa	144
10. Legislación Turca	145
11. Legislación de Emiratos Árabes Unidos	146

**CAPÍTULO XII: TRATAMIENTO INTERNACIONAL
DEL DELITO INFORMÁTICO: OCEANÍA**

1. Oceanía	151
2. Oceanía comparado a otros países en el ciberdelito	152
3. Marco legal internacional y regional en la lucha contra el delito informático en Oceanía	154
4. Cooperación internacional frente al delito informático en Oceanía	155
5. Caso: "Operación Aurora en Australia"	156

**CAPÍTULO XIII: ANÁLISIS COMPARATIVO
DEL TRATAMIENTO INTERNACIONAL DEL DELITO
INFORMÁTICO: AMÉRICA Y ÁFRICA**

1. América y África	161
1.1. Marco Legal y Normativo	162
2. Capacidades tecnológicas y recursos	164
2.1. América	164
2.2. África	164
3. Enfoques preventivos en América	165
4. Enfoques Preventivos en África	166
5. Las políticas de seguridad informática	166
6. Falencias del delito informático	167

CAPÍTULO XIV: INTELIGENCIA ARTIFICIAL Y APRENDIZAJE AUTOMÁTICO EN CIBERSEGURIDAD

1. La ciberseguridad: tendencias y avances en la ciberseguridad	171
1.1. Inteligencia artificial y aprendizaje automático en ciberseguridad	171
2. Machine Learning	172
2.1. Definición	172
2.2. Funcionamiento del machine learning	173
2.3. Métodos de machine learning	174
2.4. Algoritmos comunes de machine learning	175
2.5. Casos de uso de machine learning en el mundo real	176
3. Deep Learning	176
3.1. Definición	177
3.2. Red neuronal artificial	177
3.3. Capas de la red de aprendizaje profundo	178
3.4. Aplicación del Deep learning en la vida cotidiana	178
3.5. Deep learning y el procesamiento del lenguaje natural	179

CAPÍTULO XV: EVIDENCIA DIGITAL

1. Introducción	183
2. Desarrollo	184
2.1. Informática Forense	184
3. Evidencia digital	186
3.1. Características de la evidencia digital	186
3.2. Medios de la evidencia digital	187
3.2.1. Internet	188
3.2.2. Ordenadores	188
3.2.3. Dispositivos móviles	188
3.3. Tipos de evidencia digital	189
3.3.1. Según el tipo de elemento:	189
3.3.2. Según el tipo de sistema	189
3.3.3. Según la fuente:	189
3.4. Admisibilidad de la evidencia digital	189
3.4.1. Autenticidad	190

3.4.2. Confiabilidad	190
3.4.3. Suficiencia	191
3.4.4. Conformidad con las leyes y reglas de la administración de justicia	191

CAPÍTULO XVI: INVESTIGACIÓN Y CRIMINALÍSTICA

1. Introducción	199
2. Investigación forense	200
2.1. Etapas de la investigación forense	200
2.2. Herramientas de la investigación forense	205
3. Roles en la investigación	206
4. Criminalística	207
4.1. Definición de criminalística	207
4.2. Objetos de estudio de la criminalística	208
4.3. Métodos y técnicas de la criminalística	208
5. Aplicaciones de la criminalística	209
5.1. La informática forense en la criminalística	209
5.2. Ámbitos de aplicación	210
5.3. Importancia de la informática forense	211
6. Conclusiones	211

CAPÍTULO XVII: CADENA DE CUSTODIA Y PRINCIPIOS PROCESALES

1. Introducción	215
2. Desarrollo:	217
2.1. Principios de la prueba penal	217
2.2. Principios de la prueba penal	218
2.3. La cadena de custodia	221
2.4. Teoría del árbol envenenado	223
2.5. Relación entre los principios procesales y la cadena de custodia	223
2.6. Relación entre la informática y la cadena de custodia	224
3. Conclusión	225

CAPÍTULO XVIII: DIFICULTADES PROBATORIAS Y DELITOS TRANSNACIONALES

1. Introducción	229
2. Desarrollo	230
2.1. Delitos Transaccionales	233
2.2. Delitos contra la propiedad intelectual como componente de Delitos Transnacionales	235
3. Conclusión	236

CAPÍTULO XIX: TIPOS DE PRUEBA Y SU VALOR O EFICACIA JURÍDICA

1. Introducción	241
2. La prueba digital	241
3. Tipos de prueba digital según la doctrina	242
4. Requisitos de eficacia de la prueba digital	243
5. Sistema de valoración de la prueba digital	244
6. La prueba digital en el derecho penal	245
7. Comunicaciones por medios de correos	246
8. Llamadas telefónicas	247
9. Conclusión	249

CAPÍTULO XX: EL PERITO

1. Introducción	251
2. El perito informático	252
3. El peritaje informático	253
4. Conclusiones	257

CAPÍTULO XXI: CARGA DE LA PRUEBA INFORMÁTICA

1. Carga probatoria de la prueba informática	261
2. Ilícitud de la prueba digital	264
3. Valoración de la prueba digital	267
4. Conclusiones	270

Referencias bibliográficas	273
---	------------