

ÍNDICE

PREÁMBULO. Basilio Ramírez	19
INTRODUCCIÓN. Raúl Guillén	47
CAPÍTULO I. LA CIBERSEGURIDAD EN LA ÉPOCA DE LA AI Y EL MUNDO HIPERCONECTADO. Raúl Guillén	55
1. ¿QUÉ ES LA IA?	57
2. ¿POR QUÉ ES IMPORTANTE LA IA?	57
3. ¿QUÉ TIPOS DE IA EXISTEN?	57
4. ¿DÓNDE NOS ENCONTRAMOS IA EN EL DÍA A DÍA?	59
5. ¿QUÉ AMENAZAS Y DESAFÍOS TRAE LA IA?	61
6. CIBERSEGURIDAD, ¿POR DÓNDE EMPIEZO?	63
7. ¿QUÉ ES LA CIBERSEGURIDAD?	64
8. ¿POR QUÉ ES IMPORTANTE LA CIBERSEGURIDAD?	64
9. ¿QUÉ ES UNA VULNERABILIDAD INFORMÁTICA?	65
10. ¿QUÉ ES UN CIBERATAQUE?	66
11. ¿QUÉ BENEFICIOS PROPORCIONA LA CIBERSEGURIDAD? ..	66
12. ¿CUÁLES SON LOS TIPOS DE ATAQUE MÁS COMUNES? ...	73
13. ¿CUÁLES SON LOS COMPONENTES DE UNA ESTRATEGIA DE CIBERSEGURIDAD?	87
14. EL ROL DEL CISO.	88
15. ¿CUÁLES SON ENTONCES LAS PRINCIPALES FUNCIONES DE UN CISO?	89
16. ¿QUÉ REQUISITOS DEBE TENER UN CISO?	90
17. ¿CUÁLES SON LOS TIPOS DE CIBERSEGURIDAD?	90
17.1. Ciberseguridad de la infraestructura crítica	90

17.2.	Seguridad de la red	95
17.3.	Seguridad de los Endpoint: EPP, EDR & XDR	99
17.4.	Seguridad en el correo electrónico	103
17.5.	Seguridad en la nube	106
17.6.	Seguridad de <i>IoT</i>	111
17.7.	Seguridad de los datos	113
17.8.	Seguridad de las aplicaciones	116
17.9.	Planificación de la recuperación de desastres y continuidad del negocio.	120
17.10.	Detección y respuesta a Incidentes	123
18.	EL ESQUEMA NACIONAL DE SEGURIDAD (ENS)	128
19.	EDUCACIÓN DEL USUARIO FINAL	129
20.	CONTEXTO DE CIBERSEGURIDAD EN LA ERA DE LA IA	130
21.	PRINCIPALES INCIDENTES DE CIBERSEGURIDAD DE LA HISTORIA	132
22.	CIFRAS E IMPACTO ECONÓMICO DEL CIBERCRIMEN.	137
23.	CIBERDELITOS TIPIFICADOS EN EL CÓDIGO PENAL.	138
24.	ABUSOS DE LA IA, IA EN LA DARK WEB	139
25.	USOS CONSTRUCTIVOS Y VALOR DE LA IA EN LA CIBERSEGURIDAD	146
26.	REFERENCIAS.	153
 CAPÍTULO II. LA INGENIERÍA SOCIAL. Ana Isabel Corral García .		155
1.	INTRODUCCIÓN.	157
2.	¿QUÉ ES LA INGENIERÍA SOCIAL?.	158
2.1.	Historia de la ingeniería social	163
2.2.	La evolución de las técnicas de ingeniería social: del «timo de la estampita» al «fraude del CEO»	165
3.	PRINCIPIOS DE LA INGENIERÍA SOCIAL.	166
4.	ATAQUES DE INGENIERÍA SOCIAL.	175
4.1.	Phishing, Spear Phishing y Smishing.	175
4.2.	Vishing	183
4.3.	Pretexting	186
4.4.	Baiting	188

4.5.	Tailgating	188
4.6.	Quid pro quo	189
4.7.	Dumpster Diving	189
5.	¿CÓMO PODEMOS DEFENDERNOS DE LA INGENIERÍA SOCIAL?	190
6.	¿CÓMO PUEDE AFECTAR A LAS EMPRESAS UN ATAQUE DE INGENIERÍA SOCIAL?	193
7.	CASOS REALES DE ATAQUES POR INGENIERÍA SOCIAL	195
7.1.	2gether	195
7.2.	Ayuntamiento de Barcelona – Instituto Municipal de Informática (IMI)	196
7.3.	Grupo Zendal	196
7.4.	Empresa Municipal de Transportes (EMT) de Valencia	197
7.5.	Ayuntamiento de Granada	198
8.	CONCLUSIONES	198
CAPÍTULO III. LOS 3 ATAQUES MÁS USADOS CONTRA LAS EMPRESAS. Fernando Mairata		201
1.	LOS 3 ATAQUES MÁS USADOS CONTRA LAS EMPRESAS	203
1.1.	Ransomware	208
1.1.1.	Para prevenir el ransomware debemos tener en cuenta	212
1.1.2.	Ataques famosos de ransomware	213
1.2.	Phishing	216
1.2.1.	Para prevenir el phishing, es esencial	219
1.2.2.	Otras variedades de phishing	219
1.2.3.	Ataques famosos de phishing	221
1.3.	Wifi Hacking	226
1.3.1.	Casos famosos phishing	232
1.3.2.	Casos famosos fraude al CEO	235
2.	BIBLIOGRAFÍA	243

CAPÍTULO IV. LA PREVENCIÓN EN LAS PYMES Y GRANDES EMPRESAS. Juan Carlos Galindo	245
1. PREVENCIÓN DE ESTAFAS Y FRAUDES EN EL ENTORNO PERSONAL Y EMPRESARIAL	247
1.1. Cómo evitar una estafa	250
1.2. Cómo intentar reducir los peligros en la red (a nivel global)	252
1.3. Cómo prevenir los fraudes informáticos	258
1.4. Cómo evitar el phishing	262
1.5. Glosario de términos de ciberseguridad	264
1.6. Recomendaciones para prevenir el Man In The Middle	266
1.7. Recomendaciones para evitar el fraude del CEO	268
1.8. Cómo identificar los fraudes relacionados con las criptomonedas	271
2. LUCHA CONTRA LAS ESTAFAS Y FRAUDES	272
2.1. Qué hacer si ha sufrido una estafa	272
2.2. Cómo actuar tras ser objeto de un fraude informático	273
2.3. Delitos en la legislación complementaria	276
3. TEORÍAS (CIBER)CRIMINOLÓGICAS DEL CIBERDELITO	277
3.1. Teorías criminológicas explicativas de la ciberdelincuencia	279
3.2. Perfilado criminal	286
4. LA SEGURIDAD FÍSICA Y LÓGICA	289
4.1. La lógica	289
4.2. Aspectos sobre seguridad informática en general	289
4.3. La física	291
4.4. Seguridad frente a posibles accidentes	292
5. LAS 25 RECOMENDACIONES DEL FORO NACIONAL DE SEGURIDAD	292
6. CONCLUSIONES	296

CAPÍTULO V. LA INVESTIGACIÓN DEL DELITO TECNOLÓGICO.	Manuel Huerta de la Morena	299
1.	INTRODUCCIÓN.	301
1.1.	Definiciones clásicas de delincuencia, crimen y seguridad.	302
2.	CLASIFICACIÓN DE CIBERDELITOS Y CIBERDELINCIENTES.	305
2.1.	Grupo I: Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.	306
2.2.	Grupo II: Delitos informáticos.	306
2.3.	Grupo III: Delitos relacionados con el contenido	306
2.4.	Grupo IV: Delitos relacionados con infracciones de la propiedad intelectual y derechos afines	307
2.5.	Ataques contra el Derecho a la Intimidad.	307
2.6.	Fraudes Informáticos.	307
2.7.	Infracciones a la Propiedad Intelectual (Derechos de Autor)	307
2.7.1.	Amenazas	307
2.7.2.	Falsedades	307
2.7.3.	Calumnias e Injurias	307
2.7.4.	Sabotajes Informáticos	308
2.7.5.	Pornografía Infantil	308
2.8.	Introducción a través de Ejemplos	308
2.8.1.	Ataque a Cuentas de Usuarios: El Caso de Yahoo!	308
2.8.2.	Primero: ataque perpetrado por un actor avanzado, estado nación	309
2.8.3.	Segundo: aspecto técnico del ataque	309
2.8.4.	Tercero: impacto muy significativo del ataque	309
2.8.5.	Guerra cibernética: la red eléctrica de Ucrania	310
2.8.6.	Pensar en las amenazas y las infraestructuras críticas.	311

2.8.7.	Pensar en la resiliencia y la importancia de la capacidad de recuperación	311
2.8.8.	Defensa activa	311
3.	CLASIFICACIÓN DE DELINCUENCIA	312
3.1.	Delincuencia Organizada	313
3.2.	Tipos Adicionales de Delincuencia y su Relevancia en el Contexto Cibernético	313
3.3.	Motivaciones de los Ciberdelincuentes y su Relevancia para la Seguridad Cibernética	314
3.3.1.	Ganancia Financiera	315
3.3.2.	Desafío Intelectual	315
3.3.3.	Activismo Político o Social (Hacktivismo)	315
3.3.4.	Espionaje	315
3.3.5.	Venganza o Reputación	315
3.3.6.	Curiosidad y Aprendizaje	315
3.3.7.	Trastornos Psicológicos	315
3.4.	Tipos de Motivaciones de los Ciberdelincuentes y sus Implicaciones	316
3.4.1.	Enriquecimiento, Beneficio Financiero	316
3.4.2.	Emociones Fuertes	316
3.4.3.	Creencias Políticas e Ideología	316
3.4.4.	Diversión	316
3.5.	Implicaciones para la Seguridad Cibernética	317
3.6.	Perfiles más Comunes en Ciberdelincuencia y sus Implicaciones	317
3.6.1.	Ciberactivistas	317
3.6.2.	Implicaciones para la Seguridad	317
3.7.	Ciberdelincuencia Circunstancial	318
3.7.1.	Características	318
3.7.2.	Implicaciones para la Seguridad	318
3.8.	Ciberdelincuencia Organizada	318
3.8.1.	Características	318
3.8.2.	Implicaciones para la Seguridad	318
3.9.	Ciberdelincuencia Instrumental	318
3.9.1.	Características	318

3.9.2.	Implicaciones para la Seguridad	319
4.	PRESENTACIÓN INVESTIGACIÓN DEL DELITO TECNOLÓGICO	319
4.1.	El procedimiento forense	320
4.2.	La prueba o evidencia digital	321
5.	EL PROCEDIMIENTO DE INVESTIGACIÓN FORENSE DE EVIDENCIAS DIGITALES	323
5.1.	Tareas de la investigación forense: qué se hace	324
5.2.	Identificación del incidente y obtención de la información	326
5.3.	Recopilación de las evidencias	326
5.3.1.	Preservación de las evidencias obtenidas	327
5.3.2.	Análisis de evidencias digitales	327
5.3.3.	Documentación y resultados	327
5.4.	Ratificación en juicio	328
5.5.	Tareas del análisis forense: quién lo hace	328
5.6.	Coordinación y gestión	329
5.7.	Trabajo de campo	330
5.8.	Trabajo de laboratorio	330
5.9.	Redacción de informes	331
5.10.	Ratificación en juicio y soporte a letrados y FYCSE en ratificaciones	331
6.	TAREAS DEL ANÁLISIS FORENSE: CÓMO SE HACE	331
6.1.	Trabajo de campo	332
6.2.	Trabajo con dispositivo en «caliente»	333
6.3.	Trabajo con dispositivo en «frío» o estáticos	334
6.4.	Formularios de Adquisición de Evidencias	336
6.5.	Trabajo de laboratorio	336
6.6.	Coordinación y gestión	337
6.6.1.	Redacción de informes y soporte a letrados en ratificaciones	337
7.	INVESTIGACIÓN DE DELITOS CIBERNÉTICOS	338
7.1.	Estrategia y Evidencia en la Investigación	339
7.1.1.	Estrategia Técnica	339
7.1.2.	Importancia de la Evidencia	339

7.1.3.	Factores a Considerar	339
7.2.	El Escenario de Adquisición en la Investigación de Delitos Cibernéticos	340
7.3.	Disponibilidad de Evidencia	340
7.3.1.	Identificación de Información Importante	340
7.3.2.	Técnicas de Extracción	340
7.3.3.	Desafíos en la Era del Cloud Computing	341
7.4.	Las Fuentes de Información	341
7.4.1.	La Importancia de la Identificación Correcta	342
7.4.2.	Desafíos en la Verificación de Fuentes Múltiples	343
7.4.3.	Localización de Datos Específicos	344
7.4.4.	Barreras de Acceso	345
7.4.5.	Aspectos Legales de Romper Barreras de Seguridad	345
7.4.6.	Procedimientos Técnicos para la Adquisición de Evidencia	345
7.5.	Procesos de Adquisición	346
7.5.1.	Adquisición de Evidencia Física	346
7.5.2.	El Concepto de Colisiones	346
7.5.3.	Longitud del Algoritmo y Reducción de Colisiones	346
7.5.4.	Adquisición de Fuentes Diversas y Evolución de Algoritmos	346
7.5.5.	Implicaciones Legales y Éticas	347
7.5.6.	Consentimiento y Privacidad	347
7.5.7.	Jurisdicción y Ley Aplicable	348
7.5.8.	Manejo de Datos Sensibles	348
7.5.9.	Transparencia y Responsabilidad	348
7.5.10.	Consecuencias de la Mala Praxis	348
7.5.11.	Evolución de Algoritmos de Adquisición	348
7.5.12.	Recomendaciones para Algoritmos Seguros	349
7.6.	Inalterabilidad de la Evidencia Introducción	349
7.6.1.	Mantenimiento del Estado Original	349
7.6.2.	Desafíos en Entornos Virtuales y en la Nube	349

7.6.3.	Implicaciones Jurídicas	349
7.6.4.	Análisis de Interpretaciones	350
8.	EPILOGO	350
CAPÍTULO VI. LA RECUPERACIÓN DE ACTIVOS. Claudio Chifa .		353
1.	INTRODUCCIÓN.	356
1.1.	Importancia de la recuperación de datos en investigaciones digitales	356
1.2.	Diferenciación entre evidencia volátil y no volátil	356
2.	FUNDAMENTOS DE LA EVIDENCIA DIGITAL.	358
2.1.	Concepto de evidencia digital y su relevancia legal	358
2.2.	Cadena de custodia y su aplicación en la recuperación de datos	359
3.	EVIDENCIA VOLÁTIL: DEFINICIÓN Y CARACTERÍSTICAS	360
3.1.	La naturaleza volátil de la evidencia.	360
3.2.	Ejemplos de Evidencia Volátil y su Significado en Investigaciones Digitales	361
4.	EVIDENCIA NO VOLÁTIL: DEFINICIÓN Y TIPOS	363
4.1.	Comprender la persistencia de la evidencia no volátil y sus categorías.	363
4.2.	Herramientas y Técnicas para la Recuperación de Datos en Medios Digitales.	381
5.	CASOS PRÁCTICOS.	382
5.1.	Disco duros, pendrives y otros soportes digitales	382
5.2.	Recuperación de datos	388
5.3.	Captura de evidencias dinámicas	393
5.4.	Otros casos.	397
5.4.1.	Contraseñas	397
5.4.2.	Historial web	399
5.4.3.	Recuperación de historial online.	401
6.	NOTAS FINALES	407

CAPÍTULO VII. LOS RESPONSABLES DE LA CIBERSEGURIDAD.	Javier Martín Fernández y Basilio Ramírez Pascual	409
1.	INTRODUCCIÓN.	411
1.1.	Buen gobierno corporativo y ciberseguridad: roles y responsabilidades	411
1.2.	Las previsiones normativas	413
1.3.	Las aportaciones del Foro Nacional de Ciberseguridad	415
2.	LOS RESPONSABLES DE CIBERSEGURIDAD: SU CONFIGURACIÓN LEGAL	416
2.1.	Los responsables del Esquema Nacional de Seguridad	416
2.2.	El responsable de seguridad y enlace de las infraestructuras críticas	417
2.3.	El responsable de seguridad de la información	418
2.3.1.	Funciones	418
2.3.2.	Requisitos	420
2.4.	Las previsiones del Código de buen gobierno de la ciberseguridad.	420
2.4.1.	Objetivos	420
2.4.2.	Los responsables de la ciberseguridad.	421
3.	¿QUÉ ES LA CERTIFICACIÓN DE PERSONAS?	422
4.	EL ESQUEMA NACIONAL DE CERTIFICACIÓN DE RESPONSABLES DE CIBERSEGURIDAD	423
4.1.	Aspectos generales	423
4.2.	Descripción de las tareas	424
4.3.	Competencias requeridas	427
4.3.1.	Prevención y asesoramiento	427
4.3.2.	Supervisión	428
4.3.3.	Identificación	430
4.3.4.	Detección	430
4.3.5.	Respuesta y recuperación	430
4.3.6.	Coordinación y seguimiento	431
4.4.	Modos de acceso a la certificación	431
4.5.	Prerrequisitos	431

4.5.1.	Modo 1	431
4.5.2.	Modo 2	432
4.5.3.	Normas comunes	432
4.6.	Procedimiento de evaluación	433
4.6.1.	Modo 1	433
4.6.2.	Modo 2	433
	4.6.2.1. Las pruebas	433
	4.6.2.2. Temario	434
4.7.	Concesión del certificado	449
4.8.	Renovación	449
4.9.	Suspensión y retirada del certificado.	451
4.9.1.	Suspensión	451
	4.9.1.1. Suspensión temporal o voluntaria.	451
	4.9.1.2. Otros motivos de suspensión temporal.	451
4.9.2.	Retirada	452
4.10.	Derechos y obligaciones de las personas certificadas .	452
4.11.	Información sobre las personas certificadas	453

CAPÍTULO VIII. EL USO DE HERRAMIENTAS DE INTELIGENCIA ARTIFICIAL Y GEOLOCALIZACIÓN POR PARTE DE LA AGENCIA ESTATAL DE ADMINISTRACIÓN TRIBUTARIA (AEAT) EN ESPAÑA. Basilio Ramírez. 455

1.	AUTOMATIZACIÓN EN EL PROCESAMIENTO DE DATOS . . .	458
2.	DETECCIÓN DE PATRONES Y DETECCIÓN DEL FRAUDE . . .	459
3.	ASESORAMIENTO AUTOMATIZADO	459
4.	MEJORA EN LA LUCHA CONTRA EL FRAUDE INTERNACIONAL	459
5.	CONCLUSIÓN.	459

CAPÍTULO IX. TECNOLOGÍA BLOCKCHAIN. LA REVOLUCIÓN DE LOS SISTEMAS CONTABLES. Basilio Ramírez. 471

1.	VOCABULARIO BÁSICO	473
----	------------------------------	-----

2.	TECNOLOGÍA <i>BLOCKCHAIN</i> Y CONTABILIDAD	477
3.	OTRAS APLICACIONES EN LAS QUE SE TRABAJA	480
4.	CONCLUSIONES	484
5.	BIBLIOGRAFÍA	485
	EL FUTURO (VISIÓN CONJUNTA DE LOS AUTORES)	487