

CONTENIDO

EL AUTOR.....	XXV
AGRADECIMIENTOS.....	XXVII
PRÓLOGO.....	XXIX
PARTE 1: PRINCIPIOS BÁSICOS DE LA SEGURIDAD INFORMÁTICA.....	1
CAPÍTULO 1: PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA.....	3
QUÉ SE ENTIENDE POR SEGURIDAD INFORMÁTICA.....	3
PRINCIPIO DE “DEFENSA EN PROFUNDIDAD”	6
OBJETIVOS DE LA SEGURIDAD INFORMÁTICA	7
SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN	9
CONSECUENCIAS DE LA FALTA DE SEGURIDAD.....	14
GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	18
REFERENCIAS DE INTERÉS	23
CAPÍTULO 2: POLÍTICAS, PLANES Y PROCEDIMIENTOS DE SEGURIDAD	25
CONCEPTOS BÁSICOS	25
CARACTERÍSTICAS DESEABLES DE LAS POLÍTICAS DE SEGURIDAD	27
DEFINICIÓN E IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD	30
INVENTARIO DE LOS RECURSOS Y DEFINICIÓN DE LOS SERVICIOS OFRECIDOS	34
REALIZACIÓN DE PRUEBAS Y AUDITORÍAS PERIÓDICAS	36
REFERENCIAS DE INTERÉS	37
CAPÍTULO 3: ELEMENTOS DE LAS POLÍTICAS DE SEGURIDAD.....	39

SEGURIDAD FRENTE AL PERSONAL	39
Alta de empleados.....	39
Baja de empleados	40
Funciones, obligaciones y derechos de los usuarios	40
Formación y sensibilización de los usuarios.....	41
ADQUISICIÓN DE PRODUCTOS.....	41
RELACIÓN CON PROVEEDORES	42
SEGURIDAD FÍSICA DE LAS INSTALACIONES	43
SISTEMAS DE PROTECCIÓN ELÉCTRICA.....	45
CONTROL DEL NIVEL DE EMISIONES ELECTROMAGNÉTICAS	46
VIGILANCIA DE LA RED Y DE LOS ELEMENTOS DE CONECTIVIDAD	48
PROTECCIÓN EN EL ACCESO Y CONFIGURACIÓN DE LOS SERVIDORES	48
PROTECCIÓN DE LOS EQUIPOS Y ESTACIONES DE TRABAJO	50
CONTROL DE LOS EQUIPOS QUE PUEDEN SALIR DE LA ORGANIZACIÓN	51
COPIAS DE SEGURIDAD	51
CONTROL DE LA SEGURIDAD DE IMPRESORAS Y OTROS DISPOSITIVOS PERIFÉRICOS	54
GESTIÓN DE SOPORTES INFORMÁTICOS	54
GESTIÓN DE CUENTAS DE USUARIOS	60
IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS	61
AUTORIZACIÓN Y CONTROL DE ACCESO (SEGURIDAD LÓGICA)	65
MONITORIZACIÓN DE SERVIDORES Y DISPOSITIVOS DE LA RED	66
PROTECCIÓN DE DATOS Y DOCUMENTOS SENSIBLES.....	67
SEGURIDAD EN LAS CONEXIONES REMOTAS	70
DETECCIÓN Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD	72
OTROS ASPECTOS A CONSIDERAR.....	73
Seguridad en el desarrollo, implantación y mantenimiento de aplicaciones informáticas	73
Seguridad en las operaciones de administración y mantenimiento de la red y de los equipos.....	73
Creación, manejo y almacenamiento de documentos relacionados con la seguridad del sistema informático.....	74
Cumplimiento de la legislación vigente.....	74
Actualización y revisión de las medidas de seguridad.....	74
AUDITORÍA DE LA GESTIÓN DE LA SEGURIDAD.....	75
REFERENCIAS DE INTERÉS	76

CAPÍTULO 4: LA IMPORTANCIA DEL FACTOR HUMANO EN LA SEGURIDAD	77
EL FACTOR HUMANO EN LA SEGURIDAD INFORMÁTICA	77
FUNCIONES Y RESPONSABILIDADES DE LOS EMPLEADOS Y DIRECTIVOS	80
INGENIERÍA SOCIAL.....	86
FORMACIÓN DE LOS USUARIOS.....	88
EL CONTROL Y SUPERVISIÓN DE LOS EMPLEADOS	90
El uso de los servicios de Internet en el trabajo.....	90
Herramientas para el control y vigilancia del acceso a los servicios de Internet	92
REFERENCIAS DE INTERÉS.....	98
PARTE 2: PROBLEMAS DE SEGURIDAD EN LAS REDES Y SISTEMAS INFORMÁTICOS.....	99
CAPÍTULO 5: VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS	101
INCIDENTES DE SEGURIDAD EN LAS REDES.....	101
CAUSAS DE LAS VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS	102
Debilidad en el diseño de los protocolos utilizados en las redes.....	102
Errores de programación.....	103
Configuración inadecuada de los sistemas informáticos.....	104
Políticas de Seguridad deficientes o inexistentes.....	105
Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.....	107
Disponibilidad de herramientas que facilitan los ataques	107
Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías.....	108
Existencia de “puertas traseras” en los sistemas informáticos	109
Descuido de los fabricantes	110
TIPOS DE VULNERABILIDADES.....	110
Vulnerabilidades que afectan a equipos.....	112
ROUTERS Y CABLE-MÓDEMS	112
CÁMARAS WEB Y SERVIDORES DE VÍDEO	112
VULNERABILIDADES EN OTROS EQUIPOS CONECTADOS A UNA RED: IMPRESORAS, ESCÁNERES, FAXES, FOTOCOPIADORAS.....	113
TELÉFONOS MÓVILES	114
AGENDAS ELECTRÓNICAS.....	114
Vulnerabilidades que afectan a programas y aplicaciones informáticas	115

SISTEMAS OPERATIVOS, SERVIDORES Y BASES DE DATOS	115
NAVEGADORES	115
APLICACIONES OFIMÁTICAS COMO WORD O EXCEL	116
OTRAS UTILIDADES Y APLICACIONES INFORMÁTICAS	117
RESPONSABILIDADES DE LOS DESARROLLADORES DE SOFTWARE	118
HERRAMIENTAS PARA LA EVALUACIÓN DE VULNERABILIDADES	118
Análisis y evaluación de vulnerabilidades	118
Ejecución de Tests de Penetración en el Sistema	121
REFERENCIAS DE INTERÉS	122
CAPÍTULO 6: AMENAZAS A LA SEGURIDAD INFORMÁTICA	125
CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES	125
<i>Hackers</i>	125
<i>Crackers</i> (“ <i>blackhats</i> ”)	126
<i>Sniffers</i>	126
<i>Phreakers</i>	126
<i>Spammers</i>	127
Piratas informáticos	127
Creadores de virus y programas dañinos	127
<i>Lamers</i> (“ <i>wannabes</i> ”): “ <i>Script-kiddies</i> ” o “ <i>Click-kiddies</i> ”	128
Amenazas del personal interno	128
Ex-empleados	128
Intrusos remunerados	128
Algunos “ <i>hackers</i> ”, “ <i>crackers</i> ” y “ <i>phreakers</i> ” famosos	129
JOHN DRAPER, “CAPITÁN CRUNCH”	129
VLADIMIR LEVIN	129
KEVIN POULSON	130
KEVIN MITNICK	130
MOTIVACIONES DE LOS ATACANTES	131
FASES DE UN ATAQUE INFORMÁTICO	132
TIPOS DE ATAQUES INFORMÁTICOS	134
1. Actividades de reconocimiento de sistemas	134
2. Detección de vulnerabilidades en los sistemas	134
3. Robo de información mediante la interceptación de mensajes	135
4. Modificación del contenido y secuencia de los mensajes transmitidos	135
5. Análisis del tráfico	135

6. Ataques de suplantación de la identidad	136
<i>IP SPOOFING</i>	136
<i>DNS SPOOFING</i>	137
CAMBIOS EN EL REGISTRO DE NOMBRES DE DOMINIO DE INTERNIC	140
<i>SMTP SPOOFING</i>	140
CAPTURA DE CUENTAS DE USUARIO Y CONTRASEÑAS.....	141
7. Modificaciones del tráfico y de las tablas de enrutamiento	142
8. Conexión no autorizada a equipos y servidores.....	142
9. Consecuencias de las conexiones no autorizadas a los sistemas informáticos....	143
10. Introducción en el sistema de “ <i>malware</i> ” (código malicioso)	144
VIRUS INFORMÁTICOS, TROYANOS Y GUSANOS.....	144
ATAQUES DE “ <i>CROSS-SITE SCRIPTING</i> ” (XSS).....	145
ATAQUES DE INYECCIÓN DE CÓDIGO SQL.....	146
11. Ataques contra los sistemas criptográficos	148
12. Fraudes, engaños y extorsiones.....	148
13. Denegación del Servicio (Ataques DoS – <i>Denial of Service</i>).....	150
14. Ataques de Denegación de Servicio Distribuidos (DDoS)	154
15. Marcadores telefónicos (“ <i>dialers</i> ”).....	155
CREACIÓN DE ORGANISMOS ESPECIALIZADOS.....	155
CERT/CC (<i>Computer Emergency Response Team/Coordination Center</i>).....	155
ESCERT (Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas).....	156
Agencia Europea de Seguridad de las Redes y de la Información.....	156
CSRC (<i>Computer Security Resource Center</i>).....	156
CIAC (<i>Computer Incident Advisory Capability</i>)	156
FIRST (<i>Forum of Incident Response and Security Teams</i>).....	156
FedCIRC (<i>Federal Computer Incident Response Center</i>)	157
Otros centros de seguridad y respuesta a incidentes	157
Bases de datos de ataques e incidentes de seguridad	157
REFERENCIAS DE INTERÉS	159
CAPÍTULO 7: VIRUS INFORMÁTICOS Y OTROS CÓDIGOS DAÑINOS.....	163
CARACTERÍSTICAS GENERALES DE LOS VIRUS INFORMÁTICOS	163
TIPOS DE VIRUS Y OTROS PROGRAMAS DAÑINOS	165
Virus de <i>Boot</i> (sector de arranque)	166

Virus de ficheros ejecutables	167
VIRUS DE MS-DOS	168
VIRUS DE WIN32 (VIRUS DE WINDOWS)	168
Virus del lenguaje Java	170
Virus de macros	170
Troyanos	171
<i>Rootkits</i>	174
Gusanos (<i>Worms</i>).....	176
Bacterias	176
Bombas lógicas	177
“ <i>Hoaxes</i> ” (Bulos).....	177
“ <i>Jokes</i> ” (Bromas).....	178
Programas que permiten construir virus	178
DAÑOS OCASIONADOS POR LOS VIRUS INFORMÁTICOS	179
Posibles síntomas de una infección por código malicioso	179
Daños directos: ejecución de las propias rutinas del virus	180
Daños indirectos	180
Estimación del coste de los daños de los virus	181
TÉCNICAS DE “INGENIERÍA SOCIAL” PARA FACILITAR LA PROPAGACIÓN DE LOS VIRUS....	181
LA POLÉMICA DE LOS “PROGRAMAS ESPÍA” (“ <i>SPYWARE</i> ”).....	185
ÚLTIMAS TENDENCIAS EN EL MUNDO DE LOS VIRUS.....	191
CÓMO COMBATIR LA AMENAZA DE LOS VIRUS Y OTROS CÓDIGOS DAÑINOS	194
UTILIZACIÓN DE UN PROGRAMA ANTIVIRUS	199
REFERENCIAS DE INTERÉS	201
CAPÍTULO 8: CIBERTERRORISMO Y ESPIONAJE EN LAS REDES DE ORDENADORES.....	203
LA AMENAZA DEL CIBERTERRORISMO Y DE LAS GUERRAS INFORMÁTICAS.....	203
CONSECUENCIAS DE LOS FALLOS Y ATAQUES EN LAS EMPRESAS	205
EL ESPIONAJE EN LAS REDES DE ORDENADORES	206
El polémico chip “Clipper” y el papel de la NSA.....	206
ECHELON.....	207
ENFOPOL (<i>Enforcement Police</i>).....	209
CARNIVORE	210
REFERENCIAS DE INTERÉS	210

CAPÍTULO 9: RESPUESTA A INCIDENTES DE SEGURIDAD Y PLANES PARA LA CONTINUIDAD DEL NEGOCIO	213
INCIDENTES DE SEGURIDAD	213
PLAN DE RESPUESTA A INCIDENTES	214
Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT).....	214
Procedimientos y actividades a realizar	215
Detección de un Incidente de Seguridad	215
Análisis de un Incidente de Seguridad	217
Contención, Erradicación y Recuperación	219
Identificación del atacante y posibles actuaciones legales.....	220
Comunicación con terceros y Relaciones Públicas	222
Documentación del Incidente de Seguridad.....	223
Análisis y revisión “a posteriori” del incidente.....	224
PRÁCTICAS RECOMENDADAS POR EL CERT/CC.....	225
Preparación de la respuesta ante incidentes de seguridad	225
Gestión del incidente de seguridad	226
Seguimiento del incidente de seguridad.....	227
OBLIGACIÓN LEGAL DE NOTIFICACIÓN DE ATAQUES E INCIDENCIAS	227
INFORMÁTICA FORENSE	228
Fundamentos de la Informática Forense	228
Etapas en el análisis forense de un incidente informático.....	229
CAPTURA DE LAS EVIDENCIAS	229
PRESERVACIÓN DE LAS EVIDENCIAS DIGITALES	232
ANÁLISIS DE LAS EVIDENCIAS OBTENIDAS.....	232
Herramientas de análisis forense.....	234
Organismos y medios especializados en Informática Forense.....	235
PLAN DE RECUPERACIÓN DEL NEGOCIO.....	236
REFERENCIAS DE INTERÉS	239
PARTE 3: IDENTIFICACIÓN DE USUARIOS Y SISTEMAS BIOMÉTRICOS	241
CAPÍTULO 10: AUTENTICACIÓN, AUTORIZACIÓN Y REGISTRO DE USUARIOS	243
MODELO DE SEGURIDAD AAA.....	243
CONTROL DE ACCESO (SEGURIDAD LÓGICA)	244

IDENTIFICACIÓN DE USUARIOS	245
VERIFICACIÓN DE CONTRASEÑAS	246
Principios básicos	246
Protocolos de Desafío/Respuesta (<i>Challenge/Response</i>)	249
Otras alternativas para la gestión de contraseñas	250
LISTA DE CONTRASEÑAS (OTP: <i>ONE TIME PASSWORD</i>)	250
CONTRASEÑA VARIABLE	250
LAS IMÁGENES COMO CONTRASEÑAS	250
TARJETAS DE AUTENTICACIÓN (“ <i>AUTHENTICATION TOKENS</i> ”)	250
AUTENTICACIÓN BASADA EN CERTIFICADOS DIGITALES	251
IDENTIFICACIÓN DE LOS USUARIOS REMOTOS	251
SERVIDORES DE AUTENTICACIÓN	252
El papel de los Servidores de Autenticación	252
INICIO DE SESIÓN ÚNICO (“ <i>SINGLE SIGN-ON</i> ”)	254
GESTORES DE CONTRASEÑAS	254
REFERENCIAS DE INTERÉS	255
CAPÍTULO 11: SISTEMAS BIOMÉTRICOS.....	257
CARACTERÍSTICAS DE LOS SISTEMAS BIOMÉTRICOS	257
TIPOS DE SISTEMAS BIOMÉTRICOS	259
Reconocimiento de voz	259
Reconocimiento de firmas manuscritas	260
Huellas dactilares	261
Patrones basados en la geometría de las manos	264
Patrones faciales	265
Análisis del fondo del ojo	266
Análisis del iris	267
Otros sistemas biométricos	269
IMPLANTACIÓN DE LOS SISTEMAS BIOMÉTRICOS	270
IMPLANTACIÓN DE MICROCHIPS EN LAS PERSONAS	273
REFERENCIAS DE INTERÉS	275
PARTE 4: FUNDAMENTOS Y APLICACIONES DE LA CRIPTOGRAFÍA.....	277
CAPÍTULO 12: FUNDAMENTOS DE CRIPTOGRAFÍA.....	279
CRIPTOGRAFÍA, CRIPTOANÁLISIS Y CRIPTOLOGÍA	279

FUNCIONAMIENTO DE UN SISTEMA CRIPTOGRÁFICO.....	280
HISTORIA DE LOS SISTEMAS CRIPTOGRÁFICOS.....	283
CRIPTOANÁLISIS	285
Tipos de ataques contra un sistema criptográfico	286
Técnicas de criptoanálisis	286
CLASIFICACIÓN DE LOS SISTEMAS CRIPTOGRÁFICOS	287
SISTEMAS CRIPTOGRÁFICOS SIMÉTRICOS	290
Fundamentos de los sistemas simétricos.....	290
SISTEMAS CRIPTOGRÁFICOS ASIMÉTRICOS	291
AUTENTICACIÓN MEDIANTE LOS SISTEMAS CRIPTOGRÁFICOS ASIMÉTRICOS	295
ALGORITMOS DE DIGESTIÓN DE MENSAJES. CONCEPTO DE “HUELLA DIGITAL”	295
DE QUÉ DEPENDE LA SEGURIDAD DE LOS SISTEMAS CRIPTOGRÁFICOS	297
Robustez del esquema de encriptación diseñado	297
Adecuada gestión de las claves	300
IMPLEMENTACIÓN PRÁCTICA DE LOS ALGORITMOS	301
Hardware especializado vs Software	301
Utilización en protocolos de comunicaciones para redes de ordenadores.....	303
Encriptación de datos para su almacenamiento en un soporte informático.....	305
GESTIÓN DE CLAVES	305
La problemática de la gestión de claves.....	305
Generación y cambio de las claves	306
Transmisión de las claves a los distintos usuarios	307
Activación y utilización de las claves	308
Almacenamiento de las claves	308
Destrucción de las claves	309
Servidor para la distribución de claves	310
Algoritmos de intercambio seguro de claves	311
REFERENCIAS DE INTERÉS	311

CAPÍTULO 13: ESTEGANOGRAFÍA Y MARCAS DE AGUA (“WATERMARKS”)..... 315

ESTEGANOGRAFÍA.....	315
Los orígenes de la Esteganografía	315
Funcionamiento de las técnicas esteganográficas modernas.....	316
Programas informáticos para la esteganografía	318

TECNOLOGÍA DE MARCAS DE AGUA ('WATERMARKS')	320
Aplicaciones de las marcas de agua digitales	320
Propiedades de las marcas de agua digitales.....	321
Soluciones comerciales para las marcas de agua	322
Comparación entre la esteganografía y las marcas de agua	324
REFERENCIAS DE INTERÉS	324
CAPÍTULO 14: FIRMA ELECTRÓNICA.....	325
QUÉ ES LA FIRMA ELECTRÓNICA	325
CARACTERÍSTICAS DE LA FIRMA ELECTRÓNICA	327
AUTORIDADES DE CERTIFICACIÓN.....	328
Funciones de una Autoridad de Certificación.....	329
Infraestructura de Clave Pública.....	331
Autoridades de Certificación en España y a nivel internacional.....	332
Redes o anillos de confianza.....	333
CERTIFICADOS DIGITALES.....	333
Tipos de certificados digitales	336
CERTIFICADOS DE USUARIO FINAL.....	336
CERTIFICADOS DE FIRMA DE SOFTWARE O DE UN COMPONENTE INFORMÁTICO....	337
CERTIFICADOS DE SERVIDOR SSL.....	337
Clases de certificados digitales de usuario final	337
Certificados de atributos para el control de accesos	338
SERVICIOS BASADOS EN LA FIGURA DEL "TERCERO DE CONFIANZA".....	339
El sellado temporal de mensajes.....	339
Otros servicios de valor añadido.....	341
UTILIZACIÓN PRÁCTICA DE LA FIRMA ELECTRÓNICA	342
Firma electrónica y autenticación de documentos	342
Estándares en la Tecnología de Clave Pública: PKCS.....	343
Seguridad de los sistemas basados en la firma electrónica	344
Dispositivos personales de firma electrónica.....	346
Utilización de un servidor de firma electrónica.....	347
DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO	349
REFERENCIAS DE INTERÉS	353
CAPÍTULO 15: PROTOCOLOS CRIPTOGRÁFICOS	355
REQUISITOS DE SEGURIDAD EN LAS TRANSACCIONES ELECTRÓNICAS	355

PROTOCOLOS CRIPTOGRÁFICOS.....	356
Los protocolos SSL (<i>Secure Sockets Layer</i>) y TLS	357
Protocolo S-HTTP (<i>Secure Hypertext Transport Protocol</i>).....	359
El protocolo SET (<i>Secure Electronic Transaction</i>)	360
Comparación entre SSL y SET	363
Protocolo SSH.....	363
REFERENCIAS DE INTERÉS	365

PARTE 5: ASPECTOS TÉCNICOS DE LA SEGURIDAD EN LAS REDES DE ORDENADORES367

CAPÍTULO 16: HERRAMIENTAS PARA LA SEGURIDAD EN REDES DE ORDENADORES..... 369

EL PROBLEMA DE LA SEGURIDAD EN LA CONEXIÓN A INTERNET	369
LA SEGURIDAD EN LA RED INTERNA DE LA ORGANIZACIÓN.....	373
EL PAPEL DE LOS SERVIDORES “ <i>PROXY</i> ”	374
Características de un servidor <i>proxy</i>	374
Servicio de <i>proxy</i> inverso.....	378
EL PAPEL DE LOS CORTAFUEGOS (“ <i>FIREWALLS</i> ”)... ..	379
Características básicas de un cortafuegos	379
Servicios de protección ofrecidos por un cortafuegos	382
Tipos de cortafuegos.....	384
Configuración típica de una red protegida por un cortafuegos	385
Recomendaciones para la configuración de un cortafuegos	387
Limitaciones de los cortafuegos.....	390
Cortafuegos personales	391
ANÁLISIS DE LOS REGISTROS DE ACTIVIDAD (“ <i>LOGS</i> ”)	393
SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS).....	396
Características básicas de los IDS.....	396
Tipos de IDS	399
HIDS (“ <i>HOST IDS</i> ”)	399
MHIDS (“ <i>MULTIHOST IDS</i> ”)	400
NIDS (“ <i>NETWORK IDS</i> ”)	400
IPS (“ <i>INTRUSION PREVENTION SYSTEMS</i> ”).....	401
Arquitecturas de los IDS	402
LOS “ <i>HONEYPOTS</i> ” Y LAS “ <i>HONEYNETS</i> ” (SEÑUELOS)	403

OTRAS HERRAMIENTAS Y APLICACIONES DE UTILIDAD	407
REFERENCIAS DE INTERÉS	409
CAPÍTULO 17: SEGURIDAD EN REDES WINDOWS	413
VULNERABILIDADES DE LOS SISTEMAS WINDOWS	413
RECOMENDACIONES DE SEGURIDAD	413
Recomendaciones de seguridad de Microsoft.....	414
Recomendaciones generales de seguridad	415
REFERENCIAS DE INTERÉS	420
CAPÍTULO 18: SEGURIDAD EN REDES PRIVADAS VIRTUALES. 421	
EL PAPEL DE LAS REDES PRIVADAS VIRTUALES	421
PROTOCOLOS PARA REDES PRIVADAS VIRTUALES	424
PPTP, L2F y L2TP.....	424
IPSec	425
Redes privadas virtuales basadas en SSL.....	428
Otras consideraciones	429
REFERENCIAS DE INTERÉS	430
CAPÍTULO 19: SEGURIDAD EN LAS REDES INALÁMBRICAS..... 431	
SEGURIDAD TRADICIONAL EN LAS REDES INALÁMBRICAS	431
POSIBLES ATAQUES CONTRA REDES INALÁMBRICAS	433
Conexión no autorizada a la red inalámbrica.....	433
Análisis del tráfico y sustracción de información confidencial	433
Instalación de un Punto de Acceso falso.....	435
Instalación de Puntos de Acceso no autorizados.....	436
Interferencias electromagnéticas (“jamming”).....	436
Descubriendo redes inalámbricas desde redes cableadas.....	436
Ataques contra los terminales de usuarios de redes inalámbricas.....	436
“WarDriving” y “WarChalking”	437
EL PROTOCOLO WEP	438
ESTÁNDARES PROPUESTOS PARA MEJORAR LA SEGURIDAD DE LAS REDES WiFi	441
Protocolo WPA – Wi-Fi Protected Access	441
Autenticación robusta en redes inalámbricas: estándar 802.1x.....	442
El nuevo estándar RSN (<i>Robust Security Network</i>).....	444
RECOMENDACIONES PARA REFORZAR LA SEGURIDAD.....	445

REFERENCIAS DE INTERÉS	447
CAPÍTULO 20: DESARROLLO SEGURO DE APLICACIONES EN INTERNET	449
LOS PROBLEMAS DE SEGURIDAD EN LAS APLICACIONES WEB	449
EL MODELO DE DESARROLLO DE APLICACIONES BASADAS EN EL WEB	456
DESARROLLO DE APLICACIONES WEB SEGURAS	457
Principios fundamentales y recomendaciones básicas de seguridad	457
Actividades para el desarrollo seguro de aplicaciones.....	459
PROTECCIÓN DE LA INFORMACIÓN TRANSMITIDA	459
AUTENTICACIÓN DEL USUARIO	461
GESTIÓN DE SESIONES DE USUARIO	463
VALIDACIÓN DE ENTRADAS Y SALIDAS DE DATOS EN LAS APLICACIONES.....	465
INTERACCIÓN ENTRE EL CLIENTE Y EL SERVIDOR WEB.....	468
OTRAS CUESTIONES A CONSIDERAR	471
INICIATIVAS PARA MEJORAR LA SEGURIDAD DE LAS APLICACIONES.....	473
REFERENCIAS DE INTERÉS.....	474
PARTE 6: SEGURIDAD EN EL USO DE LOS SERVICIOS DE INTERNET.....	475
CAPÍTULO 21: LA NAVEGACIÓN SEGURA EN EL WORLD WIDE WEB.....	477
EL SERVICIO WORLD WIDE WEB	477
PROBLEMAS DE SEGURIDAD EN EL WORLD WIDE WEB.....	481
RECOMENDACIONES DE SEGURIDAD	482
REFERENCIAS DE INTERÉS	492
CAPÍTULO 22: UTILIZACIÓN SEGURA DEL CORREO ELECTRÓNICO	493
CARACTERÍSTICAS DEL CORREO ELECTRÓNICO.....	493
PROBLEMAS DE SEGURIDAD QUE AFECTAN AL CORREO ELECTRÓNICO.....	495
RECOMENDACIONES PARA MEJORAR LA SEGURIDAD DEL CORREO ELECTRÓNICO	497
Evitar la ejecución de código dañino asociado al correo electrónico.....	497
Garantizar la confidencialidad, integridad y autenticidad de los mensajes y de los usuarios	499
S/MIME.....	500
PGP (<i>PRETTY GOOD PRIVACY</i>).....	501
Configuración más segura de la red de la organización para el servicio de correo electrónico.....	504

SERVICIOS DE CORREO ELECTRÓNICO AVANZADOS.....	505
Nuevos servicios de seguridad previstos.....	505
Clasificación y respuesta automática del correo electrónico.....	506
EL USO DEL CORREO ELECTRÓNICO POR PARTE DE LOS EMPLEADOS	507
Normas de utilización para los usuarios del correo.....	507
Privacidad de los mensajes de correo de los empleados	508
REFERENCIAS DE INTERÉS	508
CAPÍTULO 23: LA LUCHA CONTRA EL “SPAM”	511
QUÉ ES EL “SPAM”	511
PROBLEMAS OCASIONADOS POR EL SPAM.....	515
PRÁCTICAS HABITUALES DE LOS SPAMMERS	516
NUEVAS FORMAS DE SPAM	518
CÓMO COMBATIR EL SPAM	520
Recomendaciones a los usuarios de los servicios de Internet	520
Tecnologías y herramientas para luchar contra el spam	521
UTILIZACIÓN DE SISTEMAS DE FILTRADO.....	521
TÉCNICA DE DESAFÍO/RESPUESTA (“CHALLENGE/RESPONSE”)	524
CONFIGURACIÓN MÁS ROBUSTA DE LOS SERVIDORES DE CORREO	524
ALTERNATIVAS PARA MEJORAR LA AUTENTICIDAD DE LOS MENSAJES.....	525
Protocolo SPF (“Senders Policy Framework”)	525
Sender ID Framework (SIDF).....	525
Domain Keys Identified Email (DKIM)	525
UTILIZACIÓN DE PROTOCOLOS CRIPTOGRÁFICOS Y DE LA FIRMA ELECTRÓNICA... 525	
OTRAS ASPECTOS A TENER EN CUENTA	526
RECOMENDACIONES DE LA UNIÓN EUROPEA CONTRA EL SPAM.....	526
LEGISLACIÓN CONTRA EL SPAM.....	528
ACTUACIONES DESTACADAS CONTRA EL SPAM	530
REFERENCIAS DE INTERÉS	531
CAPÍTULO 24: EL “PHISHING” Y LAS ESTAFAS EN INTERNET..	533
QUÉ ES EL PHISHING	533
EJEMPLOS DE CASOS DE “PHISHING” EN LA BANCA ELECTRONICA.....	539
OPERACIONES POLICIALES CONTRA EL FRAUDE EN INTERNET.....	543
RECOMENDACIONES DE SEGURIDAD PARA COMBATIR EL “PHISHING”	544
REFERENCIAS DE INTERÉS	547

PARTE 7: ASPECTOS LEGALES DE LA SEGURIDAD INFORMÁTICA.....	549
CAPÍTULO 25: DELITOS INFORMÁTICOS	551
LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS	551
CONVENIO SOBRE CIBERDELINCUENCIA DE LA UNIÓN EUROPEA.....	553
LEGISLACIÓN CONTRA LOS DELITOS INFORMÁTICOS	554
Tratamiento de los Delitos Informáticos en el Código Penal español.....	554
Estados Unidos	558
Alemania.....	559
China.....	559
CREACIÓN DE UNIDADES POLICIALES ESPECIALES.....	559
REFERENCIAS DE INTERÉS	563
CAPÍTULO 26: LA PROTECCIÓN DE DATOS PERSONALES	565
CÓMO GARANTIZAR LA PROTECCIÓN DE DATOS PERSONALES Y LA PRIVACIDAD.....	565
EL MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA	569
La aprobación y entrada en vigor de la LOPD.....	569
Ámbito de aplicación de la LOPD	570
Responsable del fichero	572
Principios de la protección de los datos	573
PRINCIPIO FUNDAMENTAL DE “ <i>HABEAS DATA</i> ”	573
CALIDAD DE LOS DATOS	574
SEGURIDAD DE LOS DATOS	574
DEBER DE SECRETO.....	574
INFORMACIÓN EN LA RECOPIACIÓN DE LOS DATOS.....	574
CONSENTIMIENTO DEL AFECTADO PARA EL TRATAMIENTO	575
COMUNICACIÓN O CESIÓN DE DATOS A TERCEROS	576
TRANSFERENCIAS DE DATOS PERSONALES A TERCEROS PAÍSES	577
DATOS ESPECIALMENTE PROTEGIDOS.....	578
DATOS RELATIVOS A LA SALUD DE LAS PERSONAS.....	578
Derechos de los ciudadanos	579
Agencia Española de Protección de Datos.....	581
Órganos de control autonómicos.....	583
Inscripción de ficheros con datos de carácter personal	585
Implantación de las medidas de seguridad sobre los ficheros.....	586
Infracciones y sanciones	592

La problemática de la adaptación de una empresa a la LOPD	594
Recomendaciones prácticas para cumplir con la LOPD	597
DECÁLOGO DE RECOMENDACIONES	597
IDENTIFICACIÓN E INSCRIPCIÓN DE FICHEROS	599
INFORMACIÓN Y PETICIÓN DE CONSENTIMIENTO	601
AUDITORÍAS PERIÓDICAS	602
REFERENCIAS DE INTERÉS	603
CAPÍTULO 27: CONTROL DE CONTENIDOS	605
LA DISTRIBUCIÓN DE CONTENIDOS DIGITALES A TRAVÉS DE INTERNET	605
El papel de Internet como nuevo medio de comunicación	605
Contenidos ilícitos y contenidos nocivos	606
Agentes involucrados en la difusión de contenidos	607
MEDIDAS LEGALES PARA COMBATIR LOS CONTENIDOS ILÍCITOS	607
Aspectos a tener en cuenta desde el punto de vista legal	607
Entorno normativo y medidas de los gobiernos	609
Conflictos jurisdiccionales	611
FILTRADO, CATALOGACIÓN Y BLOQUEO DE CONTENIDOS	612
DAÑOS A LA IMAGEN Y LA REPUTACIÓN	615
Ataques contra la imagen y reputación de las empresas	615
Campañas contra la reputación y el honor de las personas	618
Campañas de “Google Bombing”	618
Responsabilidad de la empresa por los correos electrónicos no solicitados que reciban sus empleados con contenidos ofensivos	619
REFERENCIAS DE INTERÉS	619
CAPÍTULO 28: PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Y LUCHA CONTRA LA PIRATERÍA DIGITAL	621
LOS DERECHOS DE AUTOR	621
PROTECCIÓN DE LOS PROGRAMAS INFORMÁTICOS	622
PROTECCIÓN DE LOS CONTENIDOS DIGITALES	623
Legislación para proteger los contenidos digitales	624
Tecnología DRM (<i>Digital Rights Management</i>)	627
Soluciones comerciales	629
RIGHTS MANAGEMENT SERVICE DE MICROSOFT	629
AUTHENTICA	629
RECIPROCAL	629

PINION SOFTWARE.....	630
WINDOWS MEDIA RIGHTS MANAGER DE MICROSOFT	630
FAIRPLAY DE APPLE.....	631
HELIX DE REAL NETWORKS.....	631
OTRAS CUESTIONES A CONSIDERAR RELACIONADAS CON LA PROPIEDAD INTELECTUAL ..	631
La problemática del “ <i>News Clipping</i> ”	631
La problemática del “ <i>Linking</i> ”	632
La problemática del “ <i>Framing</i> ”	633
La presencia y los patrocinios en los buscadores.....	633
La problemática del “ <i>Digital Shoplifting</i> ”	634
Plagio de trabajos y proyectos por parte de estudiantes.....	635
Otras cuestiones de interés.....	635
La polémica de las invenciones patentables en Estados Unidos	636
REFERENCIAS DE INTERÉS	638
APÉNDICES	641
ANEXOS INCLUIDOS EN EL CD-ROM DEL LIBRO	643
BIBLIOGRAFÍA	647
ÍNDICE ALFABÉTICO	651