

Enciclopedia de la Seguridad Informática

2ª Edición actualizada

En este libro se pretende abordar desde un punto de vista global la problemática de la Seguridad Informática y la Protección de Datos, contemplando tanto los aspectos técnicos, como los factores humanos y organizativos, así como el cumplimiento del entorno legal. Para ello, el contenido de esta obra se ha estructurado en siete grandes bloques:

- La primera parte presenta los principios básicos de la Seguridad de la Información en las organizaciones y en las redes de computadoras, describiendo los elementos de las Políticas, Planes y procedimientos de Seguridad, el análisis y gestión de riesgos, así como la certificación según estándares como los de la familia ISO/IEC 27000.
- En la segunda parte se estudian las vulnerabilidades de los sistemas y redes informáticas, las amenazas y los tipos de ataques más frecuentes. También se analizan los Planes de Respuesta a Incidentes y de Continuidad del Negocio.
- Una tercera parte se dedica a los aspectos relacionados con la identificación y autenticación de los usuarios en los sistemas informáticos, incluyendo el estudio de los más novedosos sistemas biométricos.
- En la cuarta parte se describen los principales sistemas y técnicas criptográficos, así como algunas de sus aplicaciones para mejorar la seguridad de los sistemas informáticos y de los servicios de Internet, analizando las características del DNI electrónico o de la factura electrónica.
- La quinta parte se centra en los aspectos técnicos para implantar las medidas de seguridad en las redes de computadoras, analizando el papel de dispositivos como los cortafuegos (firewalls), sistemas de detección de intrusiones (IDS) o servidores proxy. Así mismo, se aborda el estudio de la seguridad en las redes privadas virtuales y en las redes inalámbricas.
- En la sexta parte del libro se presentan los aspectos relacionados con la seguridad en el uso de los principales servicios de Internet, el desarrollo de los medios de pago on-line, así como la forma de afrontar problemas como el spam, el phishing o la protección de la privacidad de los ciudadanos en Internet.
- Por último, en la séptima parte se analizan diversos aspectos relacionados con el entorno legal y normativo que afectan a la Seguridad Informática: la lucha contra los Delitos Informáticos, la protección de los Datos Personales o el Control de Contenidos, entre otros.

Álvaro Gómez Vieites es Doctor en Economía (con el Premio Extraordinario de Doctorado), Licenciado en Administración y Dirección de Empresas e Ingeniero en Informática de Gestión por la UNED, Ingeniero de Telecomunicación por la Universidad de Vigo. Su formación se ha completado con los programas de posgrado Executive MBA y Diploma in Business Administration de la Escuela de Negocios Caixanova. Catedrático, consultor e investigador en las áreas de sistemas de información, seguridad informática, e-administración y comercio electrónico.

ÍNDICE

EL AUTOR	27
AGRADECIMIENTOS.....	29
PRÓLOGO	31
CAPÍTULO 1. PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA.....	37
1.1 QUÉ SE ENTIENDE POR SEGURIDAD INFORMÁTICA	37
1.2 OBJETIVOS DE LA SEGURIDAD INFORMÁTICA	40
1.3 SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN	42
1.4 CONSECUENCIAS DE LA FALTA DE SEGURIDAD	47
1.5 PRINCIPIO DE “DEFENSA EN PROFUNDIDAD”	51
1.6 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	52
1.6.1 Implantación de un Sistema de Gestión de Seguridad de la Información	57
1.7 ANÁLISIS Y GESTIÓN DE RIESGOS EN UN SISTEMA INFORMÁTICO.....	59
1.7.1 Recursos del sistema	60
1.7.2 Amenazas	60
1.7.3 Vulnerabilidades.....	61
1.7.4 Incidentes de Seguridad	62
1.7.5 Impactos	62
1.7.6 Riesgos	63
1.7.7 Defensas, salvaguardas o medidas de seguridad.....	65
1.7.8 Transferencia del riesgo a terceros.....	67
1.8 REFERENCIAS DE INTERÉS	69

CAPÍTULO 2. POLÍTICAS, PLANES Y PROCEDIMIENTOS DE SEGURIDAD 71

2.1 INTRODUCCIÓN Y CONCEPTOS BÁSICOS	71
2.2 DEFINICIÓN E IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD	76
2.3 INVENTARIO DE LOS RECURSOS Y DEFINICIÓN DE LOS SERVICIOS OFRECIDOS.....	79
2.4 SEGURIDAD FRENTE AL PERSONAL.....	81
2.4.1 Alta de empleados	81
2.4.2 Baja de empleados.....	82
2.4.3 Funciones, obligaciones y derechos de los usuarios	82
2.4.4 Formación y sensibilización de los usuarios.....	83
2.5 ADQUISICIÓN DE PRODUCTOS.....	83
2.6 RELACIÓN CON PROVEEDORES.....	84
2.7 SEGURIDAD FÍSICA DE LAS INSTALACIONES	85
2.8 SISTEMAS DE PROTECCIÓN ELÉCTRICA	87
2.9 CONTROL DEL NIVEL DE EMISIONES ELECTROMAGNÉTICAS	88
2.10 VIGILANCIA DE LA RED Y DE LOS ELEMENTOS DE CONECTIVIDAD.....	90
2.11 PROTECCIÓN EN EL ACCESO Y CONFIGURACIÓN DE LOS SERVIDORES.....	90
2.12 SEGURIDAD EN LOS DISPOSITIVOS DE ALMACENAMIENTO.....	92
2.13 PROTECCIÓN DE LOS EQUIPOS Y ESTACIONES DE TRABAJO	94
2.14 CONTROL DE LOS EQUIPOS QUE PUEDEN SALIR DE LA ORGANIZACIÓN.....	95
2.15 COPIAS DE SEGURIDAD	96
2.16 CONTROL DE LA SEGURIDAD DE IMPRESORAS Y OTROS DISPOSITIVOS PERIFÉRICOS.....	99
2.17 GESTIÓN DE SOPORTES INFORMÁTICOS.....	99
2.18 GESTIÓN DE CUENTAS DE USUARIOS	104
2.19 IDENTIFICACIÓN Y AUTENTICACIÓN DE USUARIOS	106
2.20 AUTORIZACIÓN Y CONTROL DE ACCESO LÓGICO	110
2.21 MONITORIZACIÓN DE SERVIDORES Y DISPOSITIVOS DE LA RED	111
2.22 PROTECCIÓN DE DATOS Y DE DOCUMENTOS SENSIBLES.....	112
2.23 SEGURIDAD EN LAS CONEXIONES REMOTAS.....	114
2.24 DETECCIÓN Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD.....	116
2.25 OTROS ASPECTOS A CONSIDERAR.....	118

2.25.1 Seguridad en el desarrollo, implantación y mantenimiento de aplicaciones informáticas	118
2.25.2 Seguridad en las operaciones de administración y mantenimiento de la red y de los equipos	118
2.25.3 Creación, manejo y almacenamiento de documentos relacionados con la seguridad del sistema informático	119
2.25.4 Cumplimiento de la legislación vigente	119
2.25.5 Actualización y revisión de las medidas de seguridad	119
2.26 REALIZACIÓN DE PRUEBAS Y AUDITORÍAS PERIÓDICAS	120
2.27 REFERENCIAS DE INTERÉS	121
CAPÍTULO 3. LA IMPORTANCIA DEL FACTOR HUMANO EN LA SEGURIDAD	123
3.1 EL FACTOR HUMANO EN LA SEGURIDAD INFORMÁTICA	123
3.2 FUNCIONES Y RESPONSABILIDADES DE LOS EMPLEADOS Y DIRECTIVOS	126
3.3 INGENIERÍA SOCIAL	132
3.4 FORMACIÓN DE LOS USUARIOS	134
3.5 EL CONTROL Y SUPERVISIÓN DE LOS EMPLEADOS	136
3.5.1 El uso de los servicios de Internet en el trabajo	136
3.5.2 Herramientas para el control y vigilancia del acceso a los servicios de Internet	138
3.6 REFERENCIAS DE INTERÉS	144
CAPÍTULO 4. ESTANDARIZACIÓN Y CERTIFICACIÓN EN SEGURIDAD INFORMÁTICA	145
4.1 ESTÁNDARES DE SEGURIDAD	145
4.1.1 Propósito de los estándares	145
4.1.2 Organismos responsables de la estandarización	147
4.2 ESTÁNDARES ESTADOUNIDENSES	149
4.2.1 TCSEC: Trusted Computer System Evaluation Criteria	149
4.2.2 Federal Criteria	151
4.2.3 FISCAM: Federal Information Systems Controls Audit Manual	151
4.2.4 NIST SP 800	151
4.3 ESTÁNDARES EUROPEOS	151
4.3.1 ITSEC: Information Technology Security Evaluation Criteria	151
4.3.2 ITSEM: Information Technology Security Evaluation Metodology	151
4.3.3 Agencia Europea de Seguridad de la Información y las Redes	152

4.4 ESTÁNDARES INTERNACIONALES	152
4.4.1 ISO/IEC 15408: <i>Common Criteria</i>	154
4.4.2 ISO/IEC 17799	158
4.4.3 BS 7799 Parte 2:2002	159
4.4.4 Familia ISO/IEC 27000	159
4.4.4.1 ISO/IEC 27000	159
4.4.4.2 ISO/IEC 27001	160
4.4.4.3 ISO/IEC 27002	164
4.4.4.4 ISO/IEC 27003	167
4.4.4.5 ISO/IEC 27004	167
4.4.4.6 ISO/IEC 27005	167
4.4.4.7 ISO/IEC 27006	167
4.4.5 Estándares relacionados con los sistemas y servicios criptográficos	168
4.6 PROCESO DE CERTIFICACIÓN	169
4.7 REFERENCIAS DE INTERÉS	170
CAPÍTULO 5. VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS.....	173
5.1 INCIDENTES DE SEGURIDAD EN LAS REDES	173
5.2 CAUSAS DE LAS VULNERABILIDADES DE LOS SISTEMAS INFORMÁTICOS	174
5.2.1 Debilidad en el diseño de los protocolos utilizados en las redes	174
5.2.2 Errores de programación	175
5.2.3 Configuración inadecuada de los sistemas informáticos	176
5.2.4 Políticas de Seguridad deficientes o inexistentes	177
5.2.5 Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática	179
5.2.6 Disponibilidad de herramientas que facilitan los ataques	179
5.2.7 Limitación gubernamental al tamaño de las claves criptográficas y a la utilización de este tipo de tecnologías	179
5.2.8 Existencia de “puertas traseras” en los sistemas informáticos	181
5.2.9 Descuido de los fabricantes	182
5.3 TIPOS DE VULNERABILIDADES	182
5.3.1 Vulnerabilidades que afectan a equipos	182
5.3.1.1 ROUTERS Y CABLE-MÓDEMS	182
5.3.1.2 CÁMARAS WEB Y SERVIDORES DE VÍDEO	183

5.3.1.3 VULNERABILIDADES EN OTROS EQUIPOS CONECTADOS A UNA RED: IMPRESORAS, ESCÁNERES, FAXES.....	183
5.3.1.4 TELÉFONOS MÓVILES	184
5.3.1.5 AGENDAS ELECTRÓNICAS	185
5.3.2 Vulnerabilidades que afectan a programas y aplicaciones informáticas.....	185
5.3.2.1 SISTEMAS OPERATIVOS, SERVIDORES Y BASES DE DATOS	185
5.3.2.2 NAVEGADORES	186
5.3.2.3 APLICACIONES OFIMÁTICAS COMO WORD O EXCEL.....	186
5.3.2.4 OTRAS UTILIDADES Y APLICACIONES INFORMÁTICAS	187
5.4 RESPONSABILIDADES DE LOS FABRICANTES DE SOFTWARE.....	188
5.5 HERRAMIENTAS PARA LA EVALUACIÓN DE VULNERABILIDADES	189
5.5.1 Análisis y evaluación de vulnerabilidades	189
5.5.2 Ejecución de Tests de Penetración en el Sistema.....	191
5.6 REFERENCIAS DE INTERÉS	193
CAPÍTULO 6. AMENAZAS A LA SEGURIDAD INFORMÁTICA.....	195
6.1 CLASIFICACIÓN DE LOS INTRUSOS EN LAS REDES	195
6.1.1 <i>Hackers</i>	195
6.1.2 <i>Crackers</i> (“ <i>blackhats</i> ”).....	196
6.1.3 <i>Sniffers</i>	196
6.1.4 <i>Phreakers</i>	196
6.1.5 <i>Spammers</i>	196
6.1.6 Piratas informáticos.....	197
6.1.7 Creadores de virus y programas dañinos	197
6.1.8 <i>Lamers</i> (“ <i>wannabes</i> ”): “ <i>Script-kiddies</i> ” o “ <i>Click-kiddies</i> ”	197
6.1.9 Amenazas del personal interno	198
6.1.10 Ex-empleados.....	198
6.1.11 Intrusos remunerados	198
6.1.12 Algunos “ <i>hackers</i> ”, “ <i>crackers</i> ” y “ <i>phreakers</i> ” famosos.....	198
6.1.12.1 JOHN DRAPER, “CAPITÁN CRUNCH”.....	198
6.1.12.2 VLADIMIR LEVIN	199
6.1.12.3 KEVIN POULSON	199
6.1.12.4 KEVIN MITNICK.....	200
6.2 MOTIVACIONES DE LOS ATACANTES	201

6.3 FASES DE UN ATAQUE INFORMÁTICO.....	201
6.4 TIPOS DE ATAQUES INFORMÁTICOS	203
6.4.1 Actividades de reconocimiento de sistemas.....	204
6.4.2 Detección de vulnerabilidades en los sistemas	210
6.4.3 Robo de información mediante la interceptación de mensajes	210
6.4.4 Modificación del contenido y secuencia de los mensajes transmitidos	210
6.4.5 Análisis del tráfico	210
6.4.6 Ataques de suplantación de la identidad	211
6.4.6.1 <i>IP SPOOFING</i>	211
6.4.6.2 <i>DNS SPOOFING</i>	212
6.4.6.3 CAMBIOS EN EL REGISTRO DE NOMBRES DE DOMINIO DE INTERNIC	215
6.4.6.4 <i>SMTP SPOOFING</i>	215
6.4.6.5 CAPTURA DE CUENTAS DE USUARIO Y CONTRASEÑAS	216
6.4.7 Modificaciones del tráfico y de las tablas de enrutamiento	217
6.4.8 Conexión no autorizada a equipos y servidores.....	217
6.4.9 Consecuencias de las conexiones no autorizadas a los sistemas informáticos.....	218
6.4.10 Introducción en el sistema de “ <i>malware</i> ” (código malicioso).....	219
6.4.10.1 VIRUS INFORMÁTICOS, TROYANOS Y GUSANOS	219
6.4.10.2 ATAQUES DE “ <i>CROSS-SITE SCRIPTING</i> ” (XSS)	220
6.4.10.3 ATAQUES DE INYECCIÓN DE CÓDIGO SQL.....	221
6.4.11 Ataques contra los sistemas criptográficos	223
6.4.12 Fraudes, engaños y extorsiones.....	223
6.4.13 Denegación del Servicio (Ataques DoS – <i>Denial of Service</i>).....	225
6.4.14 Ataques de Denegación de Servicio Distribuidos (DDoS)	228
6.4.15 Marcadores telefónicos (“ <i>dialers</i> ”).....	230
6.5 CREACIÓN DE ORGANISMOS ESPECIALIZADOS	230
6.5.1 CERT/CC (<i>Computer Emergency Response Team/Coordination Center</i>)....	230
6.5.2 CERT INTECO	231
6.5.3 Agencia Europea de Seguridad de las Redes y de la Información.....	231
6.5.4 CSRC (<i>Computer Security Resource Center</i>).....	231
6.5.5 US-CERT	232
6.5.6 FIRST (<i>Forum of Incident Response and Security Teams</i>)	232
6.5.7 Otros centros de seguridad y respuesta a incidentes	232

6.5.8 Bases de datos de ataques e incidentes de seguridad	232
6.6 REFERENCIAS DE INTERÉS	234
CAPÍTULO 7. VIRUS INFORMÁTICOS Y OTROS CÓDIGOS DAÑINOS	237
7.1 CARACTERÍSTICAS GENERALES DE LOS VIRUS INFORMÁTICOS.....	237
7.2 TIPOS DE VIRUS Y OTROS PROGRAMAS DAÑINOS	239
7.2.1 Virus de <i>Boot</i> (sector de arranque).....	240
7.2.2 Virus de ficheros ejecutables	241
7.2.2.1 VIRUS DE MS-DOS.....	242
7.2.2.2 VIRUS DE WIN32 (VIRUS DE WINDOWS).....	242
7.2.3 Virus del lenguaje Java	244
7.2.4 Virus de macros.....	244
7.2.5 Troyanos.....	245
7.2.6 <i>Rootkits</i>	248
7.2.7 Gusanos (<i>Worms</i>).....	249
7.2.8 Bacterias	250
7.2.9 Bombas lógicas	250
7.2.10 “ <i>Hoaxes</i> ” (Bulos)	250
7.2.11 “ <i>Jokes</i> ” (Bromas)	251
7.2.12 Programas que permiten construir virus	252
7.3 BREVE HISTORIA DE LOS VIRUS INFORMÁTICOS.....	253
7.4 DAÑOS OCASIONADOS POR LOS VIRUS INFORMÁTICOS.....	262
7.4.1 Posibles síntomas de una infección por código malicioso	262
7.4.2 Daños directos: ejecución de las propias rutinas del virus.....	263
7.4.3 Daños indirectos.....	263
7.5 TÉCNICAS DE “INGENIERÍA SOCIAL” PARA FACILITAR LA PROPAGACIÓN DE LOS VIRUS.....	264
7.6 LA POLÉMICA DE LOS “PROGRAMAS ESPÍA” (“ <i>SPYWARE</i> ”).....	268
7.7 ÚLTIMAS TENDENCIAS EN EL MUNDO DE LOS VIRUS.....	273
7.8 CÓMO COMBATIR LA AMENAZA DE LOS VIRUS Y OTROS CÓDIGOS DAÑINOS.....	277
7.9 UTILIZACIÓN DE UN PROGRAMA ANTIVIRUS	281
7.10 REFERENCIAS DE INTERÉS	284

CAPÍTULO 8. CIBERTERRORISMO Y ESPIONAJE EN LAS REDES DE ORDENADORES.....	285
8.1 LA AMENAZA DEL CIBERTERRORISMO Y DE LAS GUERRAS INFORMÁTICAS	285
8.2 CONSECUENCIAS DE LOS FALLOS Y ATAQUES EN LAS EMPRESAS	290
8.3 EL ESPIONAJE EN LAS REDES DE ORDENADORES	291
8.3.1 El polémico chip “Clipper” y el papel de la NSA.....	291
8.3.2 ECHELON	292
8.3.3 ENFOPOL (<i>Enforcement Police</i>)	294
8.3.4 CARNIVORE.....	295
8.4 REFERENCIAS DE INTERÉS	296
CAPÍTULO 9. RESPUESTA A INCIDENTES DE SEGURIDAD Y PLANES PARA LA CONTINUIDAD DEL NEGOCIO	297
9.1 INCIDENTES DE SEGURIDAD.....	297
9.2 PLAN DE RESPUESTA A INCIDENTES.....	297
9.2.1 Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT)	298
9.2.2 Procedimientos y actividades a realizar	299
9.2.3 Detección de un Incidente de Seguridad.....	299
9.2.4 Análisis de un Incidente de Seguridad	301
9.2.5 Contención, Erradicación y Recuperación	303
9.2.6 Identificación del atacante y posibles actuaciones legales.....	304
9.2.7 Comunicación con terceros y Relaciones Públicas.....	306
9.2.8 Documentación del Incidente de Seguridad.....	307
9.2.9 Análisis y revisión “ <i>a posteriori</i> ” del incidente.....	308
9.3 PRÁCTICAS RECOMENDADAS POR EL CERT/CC.....	309
9.3.1 Preparación de la respuesta ante incidentes de seguridad.....	309
9.3.2 Gestión del incidente de seguridad	310
9.3.3 Seguimiento del incidente de seguridad.....	311
9.4 OBLIGACIÓN LEGAL DE NOTIFICACIÓN DE ATAQUES E INCIDENCIAS ..	311
9.5 INFORMÁTICA FORENSE	312
9.5.1 Fundamentos de la Informática Forense	312
9.5.2 Etapas en el análisis forense de un incidente informático.....	313
9.5.2.1 CAPTURA DE LAS EVIDENCIAS.....	314
9.5.2.2 PRESERVACIÓN DE LAS EVIDENCIAS DIGITALES	316
9.5.2.3 ANÁLISIS DE LAS EVIDENCIAS OBTENIDAS	317

9.5.3 Herramientas de análisis forense.....	319
9.5.4 Organismos y medios especializados en Informática Forense.....	319
9.6 PLAN DE RECUPERACIÓN DEL NEGOCIO	320
9.7 REFERENCIAS DE INTERÉS	324
CAPÍTULO 10. AUTENTICACIÓN, AUTORIZACIÓN Y REGISTRO DE USUARIOS.....	327
10.1 MODELO DE SEGURIDAD AAA	327
10.2 CONTROL DE ACCESO (SEGURIDAD LÓGICA)	328
10.3 IDENTIFICACIÓN DE USUARIOS	329
10.4 VERIFICACIÓN DE CONTRASEÑAS	330
10.4.1 Principios básicos.....	330
10.4.2 Protocolos de Desafío/Respuesta (<i>Challenge/Response</i>).....	333
10.4.3 Otras alternativas para la gestión de contraseñas.....	334
10.4.3.1 LISTA DE CONTRASEÑAS (OTP: <i>ONE TIME PASSWORD</i>).....	334
10.4.3.2 CONTRASEÑA VARIABLE	334
10.4.3.3 LAS IMÁGENES COMO CONTRASEÑAS.....	334
10.4.3.4 TARJETAS DE AUTENTICACIÓN (“ <i>AUTHENTICATION TOKENS</i> ”)	334
10.5 AUTENTICACIÓN BASADA EN CERTIFICADOS DIGITALES	335
10.6 IDENTIFICACIÓN DE LOS USUARIOS REMOTOS	335
10.6.1 Protocolos de autenticación de acceso remoto.....	335
10.6.2 Servidores de autenticación.....	336
10.7 INICIO DE SESIÓN ÚNICO (“ <i>SINGLE SIGN-ON</i> ”)	338
10.8 GESTORES DE CONTRASEÑAS	338
10.9 REFERENCIAS DE INTERÉS	339
CAPÍTULO 11. SISTEMAS BIOMÉTRICOS	341
11.1 CARACTERÍSTICAS DE LOS SISTEMAS BIOMÉTRICOS	341
11.2 TIPOS DE SISTEMAS BIOMÉTRICOS	343
11.2.1 Reconocimiento de voz	343
11.2.2 Reconocimiento de firmas manuscritas	344
11.2.3 Huellas dactilares	345
11.2.4 Patrones basados en la geometría de las manos.....	347
11.2.5 Patrones faciales.....	348
11.2.6 Análisis del fondo del ojo	349

11.2.7 Análisis del iris.....	350
11.2.8 Otros sistemas biométricos	352
11.3 IMPLANTACIÓN DE LOS SISTEMAS BIOMÉTRICOS	353
11.4 IMPLANTACIÓN DE MICROCHIPS EN LAS PERSONAS.....	356
11.5 REFERENCIAS DE INTERÉS	358
CAPÍTULO 12. FUNDAMENTOS DE CRIPTOGRAFÍA.....	361
12.1 CRIPTOGRAFÍA, CRIPTOANÁLISIS Y CRIPTOLOGÍA	361
12.2 FUNCIONAMIENTO DE UN SISTEMA CRIPTOGRÁFICO	362
12.3 HISTORIA DE LOS SISTEMAS CRIPTOGRÁFICOS	364
12.4 CRIPTOANÁLISIS	367
12.4.1 Tipos de ataques contra un sistema criptográfico	367
12.4.2 Técnicas de criptoanálisis	368
12.5 CLASIFICACIÓN DE LOS SISTEMAS CRIPTOGRÁFICOS.....	369
12.6 SISTEMAS CRIPTOGRÁFICOS SIMÉTRICOS.....	371
12.6.1 Fundamentos de los sistemas simétricos.....	371
12.6.2 DES (<i>Data Encryption Standard</i>)	372
12.6.3 DES Múltiple.....	373
12.6.4 IDEA (<i>International Data Encryption Algorithm</i>)	374
12.6.5 Blowfish	374
12.6.6 Skipjack.....	374
12.6.7 CAST.....	375
12.6.8 RC2.....	375
12.6.9 RC4.....	375
12.6.10 RC5.....	375
12.6.11 GOST	375
12.6.12 AES (<i>Advanced Encryption Standard</i>)	375
12.7 SISTEMAS CRIPTOGRÁFICOS ASIMÉTRICOS	376
12.8 AUTENTICACIÓN MEDIANTE LOS SISTEMAS CRIPTOGRÁFICOS ASIMÉTRICOS.....	379
12.9 ALGORITMOS DE DIGESTIÓN DE MENSAJES. CONCEPTO DE “HUELLA DIGITAL”.....	380
12.10 DE QUÉ DEPENDE LA SEGURIDAD DE LOS SISTEMAS CRYPTOGRÁFICOS	382
12.10.1 Robustez del esquema de cifrado diseñado.....	382
12.10.2 Adecuada gestión de las claves	385

12.11 IMPLEMENTACIÓN PRÁCTICA DE LOS ALGORITMOS	386
12.11.1 Hardware especializado vs Software	386
12.11.2 Utilización en protocolos de comunicaciones para redes de ordenadores	387
12.11.3 Cifrado de datos para su almacenamiento en un soporte informático	389
12.12 GESTIÓN DE CLAVES	389
12.12.1 La problemática de la gestión de claves.....	389
12.12.2 Generación y cambio de las claves	391
12.12.3 Transmisión de las claves a los distintos usuarios	391
12.12.4 Activación y utilización de las claves	392
12.12.5 Almacenamiento de las claves	393
12.12.6 Destrucción de las claves	393
12.12.7 Servidor para la distribución de claves	394
12.12.8 Algoritmos de intercambio seguro de claves	395
12.13 REFERENCIAS DE INTERÉS	395
CAPÍTULO 13. ESTEGANOGRAFÍA Y MARCAS DE AGUA (“WATERMARKS”)	397
13.1 ESTEGANOGRAFÍA.....	397
13.1.1 Los orígenes de la Esteganografía.....	397
13.1.2 Funcionamiento de las técnicas esteganográficas modernas	398
13.1.3 Programas informáticos para la esteganografía	400
13.2 TECNOLOGÍA DE MARCAS DE AGUA (“WATERMARKS”)	402
13.2.1 Aplicaciones de las marcas de agua digitales	402
13.2.2 Propiedades de las marcas de agua digitales.....	403
13.2.3 Soluciones comerciales para las marcas de agua	404
13.2.4 Comparación entre la esteganografía y las marcas de agua.....	405
13.3 REFERENCIAS DE INTERÉS	405
CAPÍTULO 14. FIRMA ELECTRÓNICA	407
14.1 QUÉ ES LA FIRMA ELECTRÓNICA.....	407
14.2 CARACTERÍSTICAS DE LA FIRMA ELECTRÓNICA.....	409
14.3 AUTORIDADES DE CERTIFICACIÓN.....	410
14.3.1 Funciones de una Autoridad de Certificación.....	411
14.3.2 Infraestructura de Clave Pública	413
14.3.3 Autoridades de Certificación en España y a nivel internacional	414

14.3.4 Redes o anillos de confianza	414
14.4 CERTIFICADOS DIGITALES	415
14.4.1 Tipos de certificados digitales.....	418
14.4.1.1 CERTIFICADOS DE USUARIO FINAL.....	418
14.4.1.2 CERTIFICADOS DE FIRMA DE SOFTWARE O DE UN COMPONENTE INFORMÁTICO	418
14.4.1.3 CERTIFICADOS DE SERVIDOR SSL	419
14.4.2 Clases de certificados digitales de usuario final	419
14.4.3 Certificados de atributos para el control de accesos	419
14.5 SERVICIOS BASADOS EN LA FIGURA DEL “TERCERO DE CONFIANZA”	421
14.5.1 El sellado temporal de mensajes	421
14.5.2 Otros servicios de valor añadido	422
14.6 UTILIZACIÓN PRÁCTICA DE LA FIRMA ELECTRÓNICA	423
14.6.1 Estándares en la Tecnología de Clave Pública: PKCS.....	423
14.6.2 Seguridad de los sistemas basados en la firma electrónica	424
14.6.3 Dispositivos personales de firma electrónica	426
14.6.4 Utilización de un servidor de firma electrónica	428
14.7 DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO.....	430
14.8 FACTURA ELECTRÓNICA	433
14.9 REFERENCIAS DE INTERÉS	437
CAPÍTULO 15. PROTOCOLOS CRIPTOGRÁFICOS	439
15.1 REQUISITOS DE SEGURIDAD EN LAS TRANSACCIONES ELECTRÓNICAS	439
15.2 PROTOCOLOS CRIPTOGRÁFICOS	440
15.2.1 Los protocolos SSL (<i>Secure Sockets Layer</i>) y TLS	441
15.2.2 Protocolo S-HTTP (<i>Secure Hypertext Transport Protocol</i>)	443
15.2.3 El protocolo SET (<i>Secure Electronic Transaction</i>)	444
15.2.4 Protocolo SSH.....	447
15.3 REFERENCIAS DE INTERÉS	449
CAPÍTULO 16. HERRAMIENTAS PARA LA SEGURIDAD EN REDES DE ORDENADORES.....	453
16.1 EL PROBLEMA DE LA SEGURIDAD EN LA CONEXIÓN A INTERNET.....	453
16.2 LA SEGURIDAD EN LA RED INTERNA DE LA ORGANIZACIÓN	457
16.3 EL PAPEL DE LOS SERVIDORES “ <i>PROXY</i> ”	458

16.3.1 Características de un servidor <i>proxy</i>	458
16.3.2 Servicio de <i>proxy</i> inverso	462
16.4 EL PAPEL DE LOS CORTAFUEGOS (“ <i>FIREWALLS</i> ”)	463
16.4.1 Características básicas de un cortafuegos	463
16.4.2 Servicios de protección ofrecidos por un cortafuegos	466
16.4.3 Tipos de cortafuegos	468
16.4.4 Configuración típica de una red protegida por un cortafuegos	469
16.4.5 Recomendaciones para la configuración de un cortafuegos	471
16.4.6 Limitaciones de los cortafuegos	474
16.4.7 Cortafuegos personales	475
16.5 SERVIDORES DE AUTENTICACIÓN PARA CONEXIONES REMOTAS	477
16.5.1 RADIUS	477
16.5.2 TACACS y TACACS+	478
16.5.3 Servidor Kerberos	478
16.6 ANÁLISIS DE LOS REGISTROS DE ACTIVIDAD (“ <i>LOGS</i> ”)	481
16.7 SISTEMAS DE DETECCIÓN DE INTRUSIONES (IDS)	485
16.7.1 Características básicas de los IDS	485
16.7.2 Tipos de IDS	487
16.7.2.1 HIDS (“ <i>HOST IDS</i> ”)	487
16.7.2.2 MHIDS (“ <i>MULTIHOST IDS</i> ”)	488
16.7.2.3 NIDS (“ <i>NETWORK IDS</i> ”)	488
16.7.2.4 IPS (“ <i>INTRUSION PREVENTION SYSTEMS</i> ”)	490
16.7.3 Arquitecturas de los IDS	490
16.8 LOS “ <i>HONEYPOTS</i> ” Y LAS “ <i>HONEYNETS</i> ” (SEÑUELOS)	492
16.9 OTRAS HERRAMIENTAS Y APLICACIONES DE UTILIDAD	495
16.10 REFERENCIAS DE INTERÉS	498
CAPÍTULO 17. SEGURIDAD EN REDES PRIVADAS VIRTUALES	499
17.1 EL PAPEL DE LAS REDES PRIVADAS VIRTUALES	499
17.2 PROTOCOLOS PARA REDES PRIVADAS VIRTUALES	502
17.2.1 PPTP, L2F y L2TP	502
17.2.2 IPSec	503
17.2.3 Redes privadas virtuales basadas en SSL	506
17.2.4 Otras consideraciones	507
17.3 REFERENCIAS DE INTERÉS	508

CAPÍTULO 18. SEGURIDAD EN LAS REDES INALÁMBRICAS	509
18.1 SEGURIDAD TRADICIONAL EN LAS REDES INALÁMBRICAS	509
18.2 POSIBLES ATAQUES CONTRA REDES INALÁMBRICAS.....	511
18.2.1 Conexión no autorizada a la red inalámbrica.....	511
18.2.2 Análisis del tráfico y sustracción de información confidencial	511
18.2.3 Instalación de un Punto de Acceso falso.....	513
18.2.4 Instalación de Puntos de Acceso no autorizados.....	513
18.2.5 Interferencias electromagnéticas (“jamming”).....	514
18.2.6 Descubriendo redes inalámbricas desde redes cableadas.....	514
18.2.7 Ataques contra los terminales de usuarios de redes inalámbricas	514
18.2.8 “WarDriving” y “WarChalking”	515
18.3 EL PROTOCOLO WEP.....	515
18.4 ESTÁNDARES PROPUESTOS PARA MEJORAR LA SEGURIDAD DE LAS REDES WIFI.....	519
18.4.1 Protocolo WPA – Wi-Fi Protected Access	519
18.4.2 Autenticación robusta en redes inalámbricas: estándar 802.1x	520
18.4.3 El nuevo estándar WPA2-RSN (<i>Robust Security Network</i>).....	522
18.5 RECOMENDACIONES PARA REFORZAR LA SEGURIDAD	523
18.6 REFERENCIAS DE INTERÉS	525
CAPÍTULO 19. DESARROLLO SEGURO DE APLICACIONES EN INTERNET ...	527
19.1 LOS PROBLEMAS DE SEGURIDAD EN LAS APLICACIONES WEB	527
19.2 EL MODELO DE DESARROLLO DE APLICACIONES BASADAS EN EL WEB	533
19.3 DESARROLLO DE APLICACIONES WEB SEGURAS	534
19.3.1 Principios fundamentales y recomendaciones básicas de seguridad	534
19.3.2 Actividades para el desarrollo seguro de aplicaciones.....	537
19.3.2.1 PROTECCIÓN DE LA INFORMACIÓN TRANSMITIDA	537
19.3.2.2 AUTENTICACIÓN DEL USUARIO.....	539
19.3.2.3 GESTIÓN DE SESIONES DE USUARIO.....	541
19.3.2.4 VALIDACIÓN DE ENTRADAS Y SALIDAS DE DATOS EN LAS APLICACIONES.....	543
19.3.2.5 INTERACCIÓN ENTRE EL CLIENTE Y EL SERVIDOR WEB....	546
19.3.2.6 OTRAS CUESTIONES A CONSIDERAR	548
19.4 INICIATIVAS PARA MEJORAR LA SEGURIDAD DE LAS APLICACIONES	550

19.5 REFERENCIAS DE INTERÉS	552
CAPÍTULO 20. LA NAVEGACIÓN SEGURA EN EL <i>WORLD WIDE WEB</i>	555
20.1 EL SERVICIO <i>WORLD WIDE WEB</i>	555
20.2 PROBLEMAS DE SEGURIDAD EN EL <i>WORLD WIDE WEB</i>	559
20.3 RECOMENDACIONES DE SEGURIDAD.....	560
20.4 PROTECCIÓN DE LA PRIVACIDAD EN INTERNET	565
20.4.1 Técnicas para la identificación de visitantes a un Website	565
20.4.1.1 CONTROL DE LA PROCEDENCIA A PARTIR DE LA DIRECCIÓN IP.....	566
20.4.1.2 UTILIZACIÓN DE <i>COOKIES</i>	566
20.4.1.3 USUARIOS REGISTRADOS MEDIANTE UN NOMBRE (<i>LOGIN</i>) Y UNA CONTRASEÑA (<i>PASSWORD</i>).....	569
20.4.2 Servicios de Navegación Anónima	570
20.4.3 Estándares para la protección de la privacidad en Internet	570
20.5 REFERENCIAS DE INTERÉS	572
CAPÍTULO 21. UTILIZACIÓN SEGURA DEL CORREO ELECTRÓNICO.....	575
21.1 CARACTERÍSTICAS DEL CORREO ELECTRÓNICO.....	575
21.2 PROBLEMAS DE SEGURIDAD QUE AFECTAN AL CORREO ELECTRÓNICO.....	578
21.3 RECOMENDACIONES PARA MEJORAR LA SEGURIDAD DEL CORREO ELECTRÓNICO	579
21.3.1 Evitar la ejecución de código dañino asociado al correo electrónico	580
21.3.2 Garantizar la confidencialidad, integridad y autenticidad de los mensajes y de los usuarios	581
21.3.2.1 S/MIME	582
21.3.2.2 PGP (<i>PRETTY GOOD PRIVACY</i>).....	583
21.3.3 Configuración más segura de la red de la organización para el servicio de correo electrónico	586
21.4 SERVICIOS DE CORREO ELECTRÓNICO AVANZADOS	587
21.4.1 Nuevos servicios de seguridad previstos.....	587
21.4.2 Clasificación y respuesta automática del correo electrónico	588
21.5 EL USO DEL CORREO ELECTRÓNICO POR PARTE DE LOS EMPLEADOS	589
21.5.1 Normas de utilización para los usuarios del correo	589
21.5.2 Privacidad de los mensajes de correo de los empleados.....	590
21.6 REFERENCIAS DE INTERÉS	591

CAPÍTULO 22. LA LUCHA CONTRA EL “SPAM”	593
22.1 QUÉ ES EL <i>SPAM</i>	593
22.2 PROBLEMAS OCASIONADOS POR EL <i>SPAM</i>	597
22.3 PRÁCTICAS HABITUALES DE LOS <i>SPAMMERS</i>	598
22.4 NUEVAS FORMAS DE <i>SPAM</i>	600
22.5 CÓMO COMBATIR EL <i>SPAM</i>	601
22.5.1 Recomendaciones a los usuarios de los servicios de Internet.....	601
22.5.2 Tecnologías y herramientas para luchar contra el <i>spam</i>	603
22.5.2.1 UTILIZACIÓN DE SISTEMAS DE FILTRADO.....	603
22.5.2.2 TÉCNICA DE DESAFÍO/RESPUESTA (“ <i>CHALLENGE/RESPONSE</i> ”).....	605
22.5.2.3 CONFIGURACIÓN MÁS ROBUSTA DE LOS SERVIDORES DE CORREO.....	605
22.5.2.4 ALTERNATIVAS PARA MEJORAR LA AUTENTICIDAD DE LOS MENSAJES	606
22.5.2.5 UTILIZACIÓN DE PROTOCOLOS CRIPTOGRÁFICOS Y DE LA FIRMA ELECTRÓNICA	607
22.5.2.6 OTRAS ASPECTOS A TENER EN CUENTA.....	607
22.6 RECOMENDACIONES DE LA UNIÓN EUROPEA CONTRA EL <i>SPAM</i>	607
22.7 LEGISLACIÓN CONTRA EL <i>SPAM</i>	609
22.8 ACTUACIONES DESTACADAS CONTRA EL <i>SPAM</i>	611
22.9 REFERENCIAS DE INTERÉS	613
CAPÍTULO 23. EL “PHISHING” Y LAS ESTAFAS EN INTERNET	615
23.1 QUÉ ES EL <i>PHISHING</i>	615
23.2 EJEMPLOS DE CASOS DE “ <i>PHISHING</i> ” EN LA BANCA ELECTRONICA Y CONTRA OTRAS ENTIDADES	621
23.3 OPERACIONES POLICIALES CONTRA EL FRAUDE EN INTERNET.....	625
23.4 RECOMENDACIONES DE SEGURIDAD PARA COMBATIR EL “ <i>PHISHING</i> ”	627
23.5 REFERENCIAS DE INTERÉS	629
CAPÍTULO 24. MEDIOS DE PAGO EN INTERNET	631
24.1 MEDIOS DE PAGO TRADICIONALES.....	631
24.2 MEDIOS DE PAGO PARA EL COMERCIO ELECTRÓNICO.....	633
24.2.1 Requisitos de los Medios de Pago Electrónicos.....	633
24.2.2 Dinero electrónico: “ <i>e-money</i> ”	634
24.2.3 Cheques electrónicos: eCheck, NetCheque, NetChex	634

24.2.4 First Virtual	636
24.2.5 Tarjeta Virtu@lcash de Banesto	636
24.2.6 Cybercash	637
24.2.7 Cybercoin	639
24.2.8 ECash de la empresa DigiCash	639
24.2.9 Millicent	642
24.2.10 PayPal	643
24.2.11 EPagado	645
24.2.12 Ukash y otros sistemas basados en tarjetas prepago	646
24.2.13 Alternativas para los micropagos	648
24.3 TARJETAS INTELIGENTES (“SMART CARDS”)	648
24.4 EL TELÉFONO MÓVIL COMO INSTRUMENTO DE PAGO	652
24.5 TPV VIRTUAL	654
24.6 EL PROBLEMA DEL FRAUDE EN INTERNET	655
24.7 REFERENCIAS DE INTERÉS	661
CAPÍTULO 25. DELITOS INFORMÁTICOS	665
25.1 LA LUCHA CONTRA LOS DELITOS INFORMÁTICOS	665
25.2 CONVENIO SOBRE CIBERDELINCUENCIA DE LA UNIÓN EUROPEA	667
25.3 LEGISLACIÓN CONTRA LOS DELITOS INFORMÁTICOS	668
25.3.1 Tratamiento de los Delitos Informáticos en el Código Penal español	668
25.3.2 Estados Unidos	672
25.3.3 Alemania	673
25.3.4 China	673
25.4 CREACIÓN DE UNIDADES POLICIALES ESPECIALES	673
25.5 REFERENCIAS DE INTERÉS	678
CAPÍTULO 26. LA PROTECCIÓN DE DATOS PERSONALES	679
26.1 DERECHO A LA INTIMIDAD Y A LA PRIVACIDAD	679
26.2 CÓMO GARANTIZAR LA PROTECCIÓN DE DATOS PERSONALES Y LA PRIVACIDAD	679
26.3 EL MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES EN ESPAÑA	686
26.3.1 La aprobación y entrada en vigor de la LOPD	686
26.3.2 Ámbito de aplicación de la LOPD	687
26.3.3 Responsable del fichero	688

26.3.4 Principios de la protección de los datos	690
26.3.4.1 PRINCIPIO FUNDAMENTAL DE “ <i>HABEAS DATA</i> ”	690
26.3.4.2 CALIDAD DE LOS DATOS	690
26.3.4.3 SEGURIDAD DE LOS DATOS	691
26.3.4.4 DEBER DE SECRETO	691
26.3.4.5 INFORMACIÓN EN LA RECOPIACIÓN DE LOS DATOS.....	691
26.3.4.6 CONSENTIMIENTO DEL AFECTADO PARA EL TRATAMIENTO	692
26.3.4.7 COMUNICACIÓN O CESIÓN DE DATOS A TERCEROS	692
26.3.4.8 TRANSFERENCIAS DE DATOS PERSONALES A TERCEROS PAÍSES	694
26.3.4.9 DATOS ESPECIALMENTE PROTEGIDOS	694
26.3.4.10 DATOS RELATIVOS A LA SALUD DE LAS PERSONAS.....	695
26.3.5 Derechos de los ciudadanos	696
26.3.6 Agencia Española de Protección de Datos.....	698
26.3.7 Órganos de control autonómicos.....	700
26.3.8 Inscripción de ficheros con datos de carácter personal.....	701
26.3.9 Implantación de las medidas de seguridad sobre los ficheros	702
26.3.10 Infracciones y sanciones.....	707
26.3.11 La problemática de la adaptación de una empresa a la LOPD.....	709
26.3.12 Recomendaciones prácticas para cumplir con la LOPD	713
26.3.12.1 DECÁLOGO DE RECOMENDACIONES	713
26.3.12.2 IDENTIFICACIÓN E INSCRIPCIÓN DE FICHEROS.....	714
26.3.12.3 INFORMACIÓN Y PETICIÓN DE CONSENTIMIENTO	717
26.3.12.4 AUDITORÍAS PERIÓDICAS	717
26.4 REFERENCIAS DE INTERÉS	719

CAPÍTULO 27. CONTROL DE CONTENIDOS..... 721

27.1 LA DISTRIBUCIÓN DE CONTENIDOS DIGITALES A TRAVÉS DE INTERNET	721
27.1.1 El papel de Internet como nuevo medio de comunicación	721
27.1.2 Contenidos ilícitos y contenidos nocivos.....	722
27.1.3 Agentes involucrados en la difusión de contenidos	723
27.2 MEDIDAS LEGALES PARA COMBATIR LOS CONTENIDOS ILÍCITOS	723
27.2.1 Aspectos a tener en cuenta desde el punto de vista legal.....	723
27.2.2 Entorno normativo y medidas de los gobiernos.....	725

27.2.3 Conflictos jurisdiccionales	727
27.3 FILTRADO, CATALOGACIÓN Y BLOQUEO DE CONTENIDOS	728
27.4 DAÑOS A LA IMAGEN Y LA REPUTACIÓN	730
27.4.1 Ataques contra la imagen y reputación de las empresas	730
27.4.2 Campañas contra la reputación y el honor de las personas	733
27.4.3 Campañas de “Google Bombing”	734
27.4.4 Responsabilidad de la empresa por los correos electrónicos no solicitados que reciban sus empleados con contenidos ofensivos	735
27.5 REFERENCIAS DE INTERÉS	735
CAPÍTULO 28. PROTECCIÓN DE LA PROPIEDAD INTELECTUAL Y LUCHA CONTRA LA PIRATERÍA DIGITAL.....	737
28.1 LOS DERECHOS DE AUTOR	737
28.2 PROTECCIÓN DE LOS PROGRAMAS INFORMÁTICOS	738
28.3 PROTECCIÓN DE LOS CONTENIDOS DIGITALES.....	739
28.3.1 Legislación para proteger los contenidos digitales	740
28.3.2 Tecnología DRM (<i>Digital Rights Management</i>).....	744
28.3.3 Soluciones comerciales	745
28.3.3.1 RIGHTS MANAGEMENT SERVICE DE MICROSOFT.....	745
28.3.3.2 AUTHENTICA	746
28.3.3.3 GIGA TRUST.....	746
28.3.3.4 FAIRPLAY DE APPLE	746
28.3.3.5 WINDOWS MEDIA RIGHTS MANAGER DE MICROSOFT	747
28.3.3.6 HELIX DE REAL NETWORKS	747
28.4 OTRAS CUESTIONES A CONSIDERAR	748
28.4.1 La problemática del “ <i>News Clipping</i> ”	748
28.4.2 La problemática del “ <i>Linking</i> ”	749
28.4.3 La problemática del “ <i>Framing</i> ”	749
28.4.4 La presencia y los patrocinios en los buscadores.....	750
28.4.5 La problemática del “ <i>Digital Shoplifting</i> ”	751
28.4.6 Plagio de trabajos y proyectos por parte de estudiantes.....	751
28.4.7 Otras cuestiones de interés	752
28.4.8 La polémica de las invenciones patentables en Estados Unidos.....	753
28.5 REFERENCIAS DE INTERÉS	755

ANEXO I. FUNDAMENTOS DE REDES DE ORDENADORES E INTERNET.....	759
AI.1 REDES DE ORDENADORES Y PROTOCOLOS DE COMUNICACIONES.....	759
AI.2 ELEMENTOS UTILIZADOS EN LAS REDES DE ORDENADORES	763
AI.3 DISPOSITIVOS DE INTERCONEXIÓN	764
AI.3.1 Repetidores.....	764
AI.3.2 Puentes (<i>bridges</i>).....	764
AI.3.3 Concentradores (<i>hubs y switches</i>).....	764
AI.3.4 Encaminadores (<i>routers</i>).....	766
AI.3.5 Pasarelas (<i>gateways</i>)	766
AI.4 REDES DE ÁREA LOCAL (LAN).....	766
AI.5 REDES INALÁMBRICAS (WLAN).....	769
AI.5.1 El estándar 802.11 (Wi-Fi)	772
AI.5.2 El estándar WiMAX	774
AI.5.3 Bluetooth y otras tecnologías.....	775
AI.6 REDES DE ÁREA AMPLIA (WAN).....	776
AI.7 INTERNET: LA GRAN “RED DE REDES”	777
AI.7.1 Los orígenes de Internet.....	777
AI.7.2 Características básicas del funcionamiento de Internet	780
AI.7.3 El protocolo TCP/IP	782
AI.7.4 Direccionamiento de los equipos	783
AI.7.5 Enrutamiento del tráfico	787
AI.7.6 Puertos y servicios de una red IP	788
AI.7.7 Principales protocolos de Internet.....	792
AI.7.8 Servicio de Nombres de Dominio.....	796
AI.7.9 Calidad del Servicio en Redes IP (<i>Quality of Service</i>)	799
AI.7.10 Organizaciones que gestionan Internet	801
AI.8 REFERENCIAS DE INTERÉS	803
BIBLIOGRAFÍA	805
ÍNDICE ALFABÉTICO.....	809