



## ÍNDICE

<b>AUTORES .....</b>	<b>XXIII</b>
<b>PREFACIO.....</b>	<b>XXXV</b>
<b>PARTE I. FUNDAMENTOS.....</b>	<b>1</b>
<b>CAPÍTULO 1. CONTROL INTERNO Y AUDITORÍA DE SISTEMAS DE INFORMACIÓN.....</b>	<b>3</b>
1.1 INTRODUCCIÓN .....	3
1.2 LAS FUNCIONES DE CONTROL INTERNO Y AUDITORÍA INFORMÁTICOS..	5
1.2.1 Control Interno Informático .....	5
1.2.2 Auditoría Informática .....	7
1.2.3 Control Interno y auditoría informáticos: campos análogos.....	8
1.3 SISTEMA DE CONTROL INTERNO INFORMÁTICO .....	9
1.3.1 Definición y tipos de controles internos.....	9
1.3.2 Implantación de un sistema de controles internos  informáticos .....	10
1.4 CONCLUSIONES .....	25
1.5 LECTURAS RECOMENDADAS.....	27
1.6 BIBLIOGRAFÍA .....	28
1.7 CUESTIONES DE REPASO.....	28
<b>CAPÍTULO 2. AUDITORÍA DE SI VS. NORMAS DE BUENAS PRÁCTICAS.....</b>	<b>31</b>
2.1 INTRODUCCIÓN .....	31
2.2 AUDITORÍA DE SI VERSUS COBIT .....	32
2.2.1 La auditoría de SI .....	32
2.2.2 Convergencia de la Auditoría de SI y COBIT.....	39

2.3 AUDITORÍA DE LOS SISTEMAS DE GESTIÓN EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES -TICS-	44
2.3.1 Introducción	44
2.3.2 La implantación de un Sistema de Gestión en las TIC	46
2.3.3 Auditoría Interna	46
2.3.4 El proceso de Certificación de los Sistemas de Gestión de las TIC	47
2.4 CONCLUSIONES	49
2.5 REFERENCIAS Y BIBLIOGRAFÍA	49
2.6 CUESTIONES DE REPASO	51
<b>CAPÍTULO 3. METODOLOGÍAS DE CONTROL INTERNO, SEGURIDAD Y LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN</b>	<b>53</b>
3.1 INTRODUCCIÓN A LAS METODOLOGÍAS	53
3.2 METODOLOGÍAS DE EVALUACIÓN DE SISTEMAS	58
3.2.1 Conceptos fundamentales	58
3.2.2 Tipos de metodologías	60
3.2.2.1 METODOLOGÍA CUANTITATIVAS	60
3.2.2.2 METODOLOGÍA CUALITATIVA / SUBJETIVAS	61
3.2.3 Metodologías más comunes	61
3.2.3.1 Metodologías análisis de riesgos	61
3.2.3.2 COMPARACIÓN	62
3.2.3.3 Plan de contingencias	66
3.3 LAS METODOLOGÍAS DE AUDITORÍA INFORMÁTICA	69
3.3.1 Ejemplo metodología auditoría de una aplicación	71
3.3.1.1 PROGRAMA DE LA REVISIÓN	71
3.3.1.2 CONTROLES	73
3.3.1.3 INFORMES	79
3.4 EL PLAN AUDITOR INFORMÁTICO	80
3.5 CONCLUSIONES	82
3.6 LECTURAS RECOMENDADAS	83
3.7 BIBLIOGRAFÍA	83
3.8 CUESTIONES DE REPASO	84
<b>CAPÍTULO 4. EL CONTRATO DE AUDITORÍA</b>	<b>85</b>
4.1 INTRODUCCIÓN	85
4.2 UNA BREVE REFERENCIA A LA NATURALEZA JURÍDICA DEL CONTRATO DE AUDITORÍA	92
4.3 PARTES EN UN CONTRATO DE AUDITORÍA. EL PERFIL DEL AUDITOR INFORMÁTICO	94

4.3.1	La entidad auditada .....	94
4.3.2	El auditor informático .....	95
4.3.3	Terceras personas .....	100
4.4	<b>OBJETO DEL CONTRATO DE AUDITORÍA INFORMÁTICA</b> .....	102
4.4.1	Protección de datos de carácter personal .....	104
4.4.2	La protección jurídica del software.....	106
4.4.3	La protección jurídica de las bases de datos .....	107
4.4.4	Contratación electrónica.....	108
4.4.5	La contratación informática .....	111
4.4.6	Transferencia electrónica de fondos.....	112
	El outsourcing .....	113
	El delito informático.....	114
4.5	<b>CAUSA</b> .....	115
4.6	<b>EL INFORME DE AUDITORÍA</b> .....	115
4.7	<b>CONCLUSIONES</b> .....	117
4.8	<b>LECTURAS RECOMENDADAS</b> .....	119
4.9	<b>CUESTIONES DE REPASO</b> .....	120
<b>CAPÍTULO 5. EL DEPARTAMENTO DE AUDITORÍA DE LOS SI: ORGANIZACIONES Y FUNCIONES</b> .....		<b>121</b>
5.1	<b>INTRODUCCIÓN</b> .....	121
5.2	<b>MISIÓN DEL DEPARTAMENTO DE AUDITORÍA DE LOS SI</b> .....	122
5.3	<b>ORGANIZACIÓN DEL DEPARTAMENTO DE AUDITORÍA DE LOS SI</b> .....	126
5.3.1	Objetivos .....	126
5.3.2	Ubicación en la Organización .....	127
5.3.3	Recursos necesarios.....	129
5.3.4	Estructura del departamento de auditoría de SI .....	130
5.3.5	El Estatuto de auditoría de SI.....	132
5.3.6	Referencias sobre la función de auditoría de SI.....	133
5.4	<b>PLANIFICACIÓN DEL TRABAJO DE AUDITORÍA DE SI</b> .....	133
5.4.1	Definir el Universo de TI .....	134
5.4.2	Análisis de Riesgos .....	136
5.4.3	Planificación a Largo Plazo .....	138
5.4.4	Planificación a Corto Plazo .....	141
5.5	<b>METODOLOGÍA DEL TRABAJO DE AUDITORÍA DE SI</b> .....	142
5.6	<b>EL EQUIPO DE AUDITORÍA DE SI</b> .....	144
5.7	<b>CONCLUSIONES</b> .....	146

5.8 BIBLIOGRAFÍA Y LECTURAS RECOMENDADAS .....	147
5.9 CUESTIONES DE REPASO .....	147
<b>CAPÍTULO 6. ENTORNO JURÍDICO DE LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN .....</b>	<b>149</b>
6.1 INTRODUCCIÓN .....	149
6.2 LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL .....	151
6.2.1 Legislación .....	151
6.2.2 Objeto de la protección de datos .....	152
6.2.3 Sujetos de la protección de datos .....	153
6.2.4 Principios de la protección de datos .....	154
6.2.5 Derechos de las personas .....	157
6.3 LA PROTECCIÓN JURÍDICA DE LOS PROGRAMAS DE ORDENADOR .....	158
6.3.1 Titularidad de los derechos (artículo 97 TRLPI) .....	159
6.3.2 Duración de la protección (artículo 98 TRLPI) .....	160
6.3.3 Contenido de los derechos de explotación (artículo 99 TRLPI) .....	160
6.4 LOS DELITOS TECNOLÓGICOS .....	161
6.4.1 Delitos contra la intimidad .....	161
6.4.2 Delitos contra el patrimonio .....	161
6.4.3 Delitos de falsedades .....	162
6.4.4 Delitos contra las Administraciones Públicas .....	162
6.4.5 Otros delitos y faltas .....	163
6.5 LA CONTRATACIÓN ELECTRÓNICA .....	163
6.6 LA FIRMA ELECTRÓNICA .....	164
6.7 EL DNI ELECTRÓNICO .....	166
6.8 EL CORREO ELECTRÓNICO .....	167
6.9 LA VIDEOVIGILANCIA .....	169
6.10 LEY ESTADOUNIDENSE SARBANES-OXLEY (SOX) .....	170
6.11 CONCLUSIONES .....	172
6.12 LECTURAS RECOMENDADAS .....	172
6.13 BIBLIOGRAFÍA .....	172
6.14 CUESTIONES DE REPASO .....	173
<b>CAPÍTULO 7. ÉTICA DEL AUTOR DE LOS SISTEMAS DE INFORMACIÓN... 175</b>	
7.1 INTRODUCCIÓN .....	175
7.2 PRINCIPIOS DEONTOLÓGICOS BÁSICOS APLICABLES A LOS AUDITORES DE LOS SISTEMAS DE INFORMACIÓN .....	180
7.2.1 Principio de capacidad profesional .....	180

7.2.2	Principio de comportamiento profesional .....	182
7.2.3	Principio de confidencialidad .....	187
7.2.4	Principio de independencia .....	189
7.2.5	Principio de beneficio del auditado .....	190
7.2.6	Principio de suficiencia en los trasvases de información .....	193
7.2.7	Principio de veracidad .....	195
7.2.8	Principio de libre competencia .....	196
7.2.9	Principio de servicio público .....	198
7.2.10	Principio de fortalecimiento y respeto de la profesión .....	199
7.2.11	Principio de legalidad .....	200
7.3	CONCLUSIONES .....	200
7.4	LECTURAS RECOMENDADAS .....	201
7.5	CUESTIONES DE REPASO .....	202
<b>CAPÍTULO 8. HERRAMIENTAS PARA LA AUDITORÍA DE LOS SI .....</b>		<b>205</b>
8.1	RESUMEN .....	205
8.2	INTRODUCCIÓN .....	206
8.2.1	Herramientas, máquinas, sistemas, demonios .....	206
8.2.2	Herramientas específicas, substitutivas y multipropósito .....	207
8.2.3	La herramienta "perfecta" .....	208
8.2.4	Herramientas de Auditoría (solamente) SITIC .....	209
8.2.5	Enfoque de este capítulo .....	209
8.2.6	Tipos .....	210
8.2.7	Importancia .....	211
8.2.7.1	Datos de mercado .....	211
8.3	HERRAMIENTAS DE AUDITORÍA SEGÚN SU PROCEDENCIA .....	212
8.3.1	Herramientas del entorno adquisición-construcción .....	213
8.3.2	Herramientas de prueba .....	213
8.3.3	Herramientas del entorno explotación-operación .....	213
8.3.4	Herramientas del SW de Sistema .....	214
8.3.4.1	Utilidades .....	214
8.3.5	Herramientas de TCP/IP e Internet .....	214
8.3.6	Herramientas específicas de auditoría y herramientas ofimáticas .....	218
8.4	HERRAMIENTAS DE AUDITORÍA SEGÚN SU FUNCIÓN .....	218
8.4.1	Captura de datos .....	219
8.4.1.1	Muestras .....	219
8.4.1.2	Vigilancia .....	220

8.4.1.3 Forense.....	220
8.4.2 Análisis.....	221
8.4.2.1 Auditoría cooperativa.....	221
8.5 HERRAMIENTAS DE AUDITORÍA SEGÚN SU USO O PROPÓSITO.....	221
8.5.1 Auditoría SITIC.....	222
8.5.2 Otras Auditorías, coordinadas o no (usualmente no) con la SITIC.....	222
8.5.3 Otros usos.....	222
8.6 HERRAMIENTAS DE AUDITORÍA SEGÚN SU UBICACIÓN.....	222
8.6.1 Herramientas embebidas.....	225
8.6.1.1 Herramientas Intrusivas y no intrusivas.....	225
8.6.1.2 Auditoría continua/auditoría en línea.....	225
8.6.1.3 Auditoría diferida "cooperativa".....	226
8.6.2 Herramientas exentas.....	228
8.6.2.1 Herramientas Horizontales (Ofimática).....	228
8.6.2.2 Verticales Herramientas.....	229
8.6.2.3 Herramientas verticales de gestión.....	229
8.6.2.4 Herramientas verticales técnicas.....	230
8.7 HERRAMIENTAS DE AUDITORÍA SEGÚN SU PRODUCTIVIDAD.....	231
8.8 HERRAMIENTAS DE AUDITORÍA SEGÚN SU COBERTURA.....	233
8.9 ALGUNOS EJEMPLOS DE PRODUCTOS Y EMPRESAS POR TIPOS.....	233
8.9.1 Herramientas gratuitas.....	233
8.9.2 ACL.....	233
8.9.3 IDEA.....	233
8.9.4 Symantec.....	234
8.9.5 Computer Associates.....	234
8.9.6 Otras.....	234
8.10 CONCLUSIONES.....	234
8.11 AGRADECIMIENTOS.....	237
8.12 REFERENCIAS.....	237
8.12.1 Lecturas recomendadas.....	237
8.12.2 Otras referencias.....	238
8.13 CUESTIONES DE REPASO.....	238
<b>PARTE II. PRINCIPALES ÁREAS DE LA AUDITORÍA</b>	
<b>INFORMÁTICA.....</b>	<b>243</b>
<b>CAPÍTULO 9. AUDITORÍA DE OUTSOURCING DE TI.....</b>	<b>243</b>
9.1 INTRODUCCIÓN.....	243
9.2 CONCEPTOS RELATIVOS AL OUTSOURCING DE TI.....	245

9.2.1	Definición de Outsourcing .....	245
9.2.2	El outsourcing de ti .....	248
9.2.3	Tipos de outsourcing .....	251
9.2.4	Ciclo de vida del outsourcing .....	254
9.2.5	Riesgos y oportunidades .....	257
9.2.6	MITOS DEL OUTSOURCING .....	257
9.3	AUDITORÍA DEL OUTSOURCING DE TI .....	258
9.3.1	El contrato de outsourcing .....	261
9.3.2	El Acuerdo de Nivel de Servicio .....	267
	Reflexiones sobre el Acuerdo de Nivel de Servicio: .....	270
9.3.3	El sistema de penalizaciones .....	270
	Reflexión sobre el Sistemas de Penalizaciones: .....	271
9.3.4	Los informes de gestión (IG) .....	271
9.3.5	Conclusión.....	272
9.4	OUTSOURCING Y MARCOS DE REFERENCIA .....	274
9.4.1	CMMI (Capability Maturity Model Integration) .....	275
9.4.2	ISO 27001 / BS 7799 .....	277
9.4.3	ITIL (IT infrastructure library).....	278
9.5	PROGRAMA DE AUDITORÍA AL OUTSOURCING .....	280
9.6	LECTURA RELACIONADAS .....	285
9.7	BIBLIOGRAFIA. ....	286
<b>CAPÍTULO 10. AUDITORÍA DE LA SEGURIDAD FÍSICA .....</b>		<b>287</b>
10.1	INTRODUCCIÓN .....	287
10.2	SEGURIDAD FÍSICA VS. SEGURIDAD LÓGICA .....	288
10.3	COBIT – DS 12 GESTIÓN DEL ENTORNO FÍSICO .....	289
10.3.1	DS 12.1 Selección y diseño de los centros de proceso de datos. ....	290
10.3.2	DS12.2 Medidas de seguridad física.....	291
10.3.3	DS12.3 Acceso físico .....	291
10.3.4	DS12.4 Protección contra factores ambientales.....	291
10.3.5	DS12.5 Gestión de las instalaciones .....	291
10.4	ISO 27002:2005 – SEGURIDAD FÍSICA Y DEL ENTORNO.....	291
10.4.1	Seguridad Física y del Entorno .....	292
10.4.2	Control de Acceso .....	293
10.5	CSCN DEL MAP – SEGURIDAD FÍSICA.....	294
10.5.1	Seguridad Física.....	294
10.5.1.1	Criterios .....	294

10.5.1.2 Recomendaciones .....	297
10.5.2 Protección de Soportes de Información .....	298
10.5.2.1 Criterios .....	298
10.6 CONTROLES DE SEGURIDAD FÍSICA .....	299
10.6.1 Perimetro de seguridad física .....	300
10.6.2 Control de entrada .....	301
10.7 PLANIFICACIÓN Y EJECUCIÓN DE LA AUDITORÍA DE LA SEGURIDAD FÍSICA .....	304
10.7.1 Cuestionario de Seguridad Física .....	305
10.8 CONCLUSIONES .....	320
10.9 LECTURAS RECOMENDADAS .....	321
10.10 BIBLIOGRAFÍA .....	322
10.11 CUESTIONES DE REPASO .....	322
<b>CAPÍTULO 11. LA AUDITORÍA DE LA DIRECCIÓN DE INFORMÁTICA .....</b>	<b>323</b>
11.1 INTRODUCCIÓN .....	323
11.2 PLANIFICAR .....	324
11.2.1 Plan Estratégico de Sistemas de Información .....	325
11.2.2 Otros planes relacionados .....	327
11.3 ORGANIZAR Y COORDINAR .....	329
11.3.1 Comité de Informática .....	329
11.3.2 Posición del Departamento de Informática en la empresa .....	331
11.3.3 Descripción de funciones y responsabilidades del Departamento de Informática. Segregación de funciones .....	332
11.3.3.1 Estándares de funcionamiento y procedimientos. Descripción de los puestos de trabajo .....	335
11.3.3.2 Gestión de recursos humanos: selección, evaluación del desempeño, formación, promoción, finalización .....	336
11.3.3.3 Gestión económica .....	338
11.4 CONTROLAR .....	341
11.4.1 Control y Seguimiento .....	341
11.4.2 Cumplimiento de la normativa legal .....	342
11.5 CONCLUSIONES .....	343
11.6 LECTURAS RECOMENDADAS .....	343
11.7 CUESTIONES DE REPASO .....	343
<b>CAPÍTULO 12. AUDITORÍA DE LA EXPLOTACIÓN .....</b>	<b>345</b>
12.1 INTRODUCCIÓN .....	345
12.2 SISTEMAS DE INFORMACION .....	346



12.3	NORMAS TÉCNICAS DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN	347
12.3.1	Introducción	347
12.3.2	Organismos emisores de normas de auditoría	348
12.3.3	Obligación de cumplir las normas	348
12.3.4	Normas técnicas de auditoría de sistemas de información	349
12.3.5	Clasificación de las Normas	349
12.4	PRINCIPIOS DE AUDITORÍA	349
12.4.1	Formalidad	350
12.4.2	Independencia	350
12.4.3	Ética y normas profesionales	350
12.4.4	Idoneidad	351
12.4.5	Planificación	351
12.4.6	Ejecución de la auditoría	351
12.4.7	Información	352
12.5	ALCANCE DE LA AUDITORÍA	352
12.6	SERVICIOS QUE PUEDE PRESTAR EL AUDITOR DE SI	353
12.6.1	Auditoría y Revisión	353
12.6.2	Hechos concretos o procedimientos acordados	354
12.6.3	El mandato del encargo	354
12.7	CICLO DE VIDA	355
12.7.1	Inicio	355
12.7.2	Fase de Planificación	356
12.7.3	Fase de Ejecución	357
12.7.4	Fase de Revisión	357
12.7.5	Fase de Corrección	357
12.7.6	Fin	357
12.8	ENTREVISTA INICIAL	357
12.9	INVENTARIO DE RECURSOS Y MEMORIA	357
12.10	CARTA DE ENCARGO	358
12.11	PLANIFICACIÓN	358
12.11.1	Planificación estratégica	358
12.11.1.1	Clasificación de los controles internos	360
12.11.1.2	Evaluación de los Controles Internos	365
12.11.1.3	Establecimiento de objetivos	370
12.11.2	Planificación Administrativa	372
12.11.3	Planificación técnica	372

12.12 REALIZACIÓN DEL TRABAJO (PROCEDIMIENTOS).....	373
12.12.1 Objetivo General .....	373
12.12.2 Objetivos específicos .....	373
12.12.2.1 1. Objetivo General.....	374
12.12.2.2 2. Objetivos específicos.....	374
12.13 INFORMES .....	377
12.13.1 Tipos de informes.....	377
12.13.2 Recomendaciones.....	379
12.13.3 Normas para elaborar los informes .....	379
12.13.4 Ejemplo de informe de auditoría.....	380
12.14 LA DOCUMENTACIÓN DE LA AUDITORÍA Y SU ORGANIZACIÓN .....	382
12.14.1 Papeles de trabajo.....	382
12.14.2 Archivos .....	383
12.14.2.1 Archivo permanente.....	383
12.14.2.2 Archivo corriente.....	384
12.15 CONCLUSIONES .....	385
12.16 BIBLIOGRAFÍA .....	385
12.17 CUESTIONES DE REPASO.....	386
<b>CAPÍTULO 13. AUDITORIA DE BASES DE DATOS.....</b>	<b>387</b>
13.1 INTRODUCCIÓN.....	387
13.2 METODOLOGIA PARA LA AUDITORIA DE BASES DE DATOS .....	388
13.3 RECOMENDACIONES DE LOS COBIT PARA AUDITORÍA DE BASES DE DATOS .....	389
13.4 OBJETIVOS DE CONTROL EN EL CICLO DE VIDA DE UNA BASE DE DATOS.....	392
13.4.1 Estudio previo y plan de trabajo.....	392
13.4.2 Concepción de la base de datos y selección del equipo .....	395
13.4.3 Diseño y carga.....	395
13.4.4 Explotación y mantenimiento .....	396
13.4.5 Revisión post-implantación.....	397
13.4.6 Otros procesos auxiliares .....	397
13.5 AUDITORÍA Y CONTROL INTERNO EN UN ENTORNO DE BASES DE DATOS.....	398
13.5.1 Sistema de Gestión de Bases de Datos (SGBD) .....	399
13.5.2 Software de auditoría .....	399
13.5.3 Sistema de monitorización y ajuste ( <i>tuning</i> ).....	399
13.5.4 Sistema Operativo (SO) .....	400

13.5.5	Monitor de Transacciones .....	400
13.5.6	Protocolos y Sistemas Distribuidos .....	400
13.5.7	Paquetes de seguridad .....	400
13.5.8	Diccionarios de datos .....	400
13.5.9	Herramientas CASE (Computer Aided System/Software Engineering)/IPSE (Integrated Project Support Environments) .....	401
13.5.10	Lenguajes de Cuarta Generación (L4G) independientes .....	401
13.5.11	Facilidades de usuario .....	402
13.5.12	Herramientas de "minería de datos" .....	402
13.5.13	Aplicaciones .....	402
13.6	TÉCNICAS PARA EL CONTROL DE BASES DE DATOS EN UN ENTORNO COMPLEJO .....	402
13.7	CONCLUSIONES .....	403
13.8	LECTURAS RECOMENDADAS .....	404
13.9	BIBLIOGRAFÍA .....	405
13.10	CUESTIONES DE REPASO .....	406
<b>CAPÍTULO 14.</b>	<b>AUDITORÍA DE TÉCNICA DE SISTEMAS .....</b>	<b>407</b>
14.1	ÁMBITO DE TÉCNICA DE SISTEMAS .....	407
14.2	DEFINICIÓN DE LA FUNCIÓN .....	409
14.3	EL NIVEL DE SERVICIO .....	410
14.4	LOS PROCEDIMIENTOS .....	411
14.5	LOS CONTROLES .....	417
14.6	AUDITORÍA DE LA FUNCIÓN .....	428
14.7	CONSIDERACIONES SOBRE LA TECNOLOGÍA Y SU EVOLUCIÓN .....	436
14.8	LECTURAS RECOMENDADAS .....	437
14.9	CUESTIONES DE REPASO .....	438
<b>CAPÍTULO 15.</b>	<b>AUDITORÍA DE LA SEGURIDAD .....</b>	<b>441</b>
15.1	INTRODUCCIÓN .....	441
15.2	CONTROL INTERNO Y SEGURIDAD .....	445
15.3	PERFIL DEL AUDITOR DE SEGURIDAD .....	447
15.4	NORMA ISO 17799 (27002) Y OTRAS .....	451
15.5	COBIT Y OTRAS FUENTES DE ISACA .....	453
15.6	CÓMO REALIZAR UNA AUDITORÍA DE SEGURIDAD .....	463
15.7	EVALUACIÓN DE RIESGOS .....	465
15.8	ÁREAS A REVISAR .....	469
15.9	FUENTES A UTILIZAR .....	480

15.10 TÉCNICAS, MÉTODOS Y HERRAMIENTAS .....	482
15.11 CONSIDERACIONES SOBRE EL INFORME .....	483
15.12 INDICADORES Y MÉTRICAS DE SEGURIDAD .....	487
15.13 CONCLUSIONES .....	489
15.14 LECTURAS RECOMENDADAS .....	490
15.15 BIBLIOGRAFÍA .....	490
15.16 CUESTIONES DE REPASO .....	491
<b>CAPÍTULO 16. AUDITORÍA DE REDES .....</b>	<b>493</b>
16.1 TERMINOLOGÍA DE REDES .....	493
16.2 VULNERABILIDADES EN REDES .....	497
16.3 VULNERABILIDAD EN CAPAS FÍSICA, ENLACES Y RED .....	497
16.4 VULNERABILIDAD EN EL TRANSPORTE .....	499
16.5 REDES INTERNAS Y EXTERNAS .....	500
16.6 AUDITANDO A LA ORGANIZACIÓN .....	505
16.7 AUDITANDO LA RED FÍSICA .....	508
16.8 AUDITANDO LA RED LÓGICA .....	509
16.9 CONCLUSIONES .....	510
16.10 LECTURAS RECOMENDADAS .....	511
16.11 BIBLIOGRAFÍA .....	511
16.12 CUESTIONES DE REPASO .....	512
<b>CAPÍTULO 17. AUDITORÍA DE INTERNET .....</b>	<b>513</b>
17.1 INTRODUCCIÓN .....	513
17.2 PRINCIPIOS Y DERECHOS DE PROTECCIÓN DE DATOS .....	515
17.2.1 Notificación de los tratamientos .....	517
17.2.2 Encargo de tratamientos .....	518
17.2.3 Legitimación de los tratamientos .....	519
17.2.4 Información al interesado .....	522
17.2.5 Calidad de los datos .....	528
17.2.6 Confidencialidad de la información .....	530
17.2.7 Derechos de acceso, rectificación, cancelación y oposición .....	532
17.2.8 Transferencias internacionales de datos personales .....	534
17.2.9 Medidas de seguridad .....	536
17.2.10 Comunicaciones comerciales no solicitadas ( <i>spam</i> ) .....	536
17.3 CONTROLES .....	538
17.3.1 Notificación de los tratamientos .....	538
17.3.2 Encargo de tratamientos .....	539

17.3.3	Legitimación de los tratamientos .....	539
17.3.4	Información al interesado.....	540
17.3.5	Calidad de los datos.....	541
17.3.6	Confidencialidad de la información.....	542
17.3.7	Derechos de acceso, rectificación, cancelación y oposición.....	543
17.3.8	Transferencias internacionales de datos personales.....	543
17.3.9	Medidas de seguridad.....	544
17.3.10	Comunicaciones comerciales no solicitadas (spam).....	545
17.4	CONCLUSIONES.....	545
17.5	LECTURAS RECOMENDADAS.....	546
17.6	CUESTIONES DE REPASO.....	547
<b>CAPÍTULO 18.</b>	<b>AUDITORÍA DE APLICACIONES.....</b>	<b>549</b>
18.1	INTRODUCCIÓN.....	549
18.2	PRINCIPALES MODELOS DE REFERENCIA .....	551
18.3	LAS MÉTRICAS COMO HERRAMIENTA BÁSICA EN LAS AUDITORÍAS DE APLICACIONES .....	555
18.4	ENTORNOS PARA LA EVALUACIÓN DE LA CALIDAD DE LAS APLICACIONES .....	555
18.5	UN MÉTODO PARA AUDITAR APLICACIONES SOFTWARE .....	557
18.5.1	Fase 1.- Definir el plan de la auditoría de la aplicación.....	557
18.5.1.1	Definir el alcance de la auditoría, objetivo y método .....	557
18.5.1.2	Estimación y planificar .....	559
18.5.1.3	Definir el equipo de la auditoría y el plan de comunicación.....	559
18.5.1.4	Definir las herramientas de uso en la auditoría.....	559
18.5.2	Fase 2.- Ejecución de la auditoría .....	561
18.5.3	Fase 3.- Análisis, síntesis y presentación de resultados.....	562
18.6	RECOMENDACIONES Y BUENAS PRÁCTICAS .....	565
18.7	CONCLUSIONES.....	566
18.8	LECTURAS RECOMENDADAS .....	566
18.9	BIBLIOGRAFÍA .....	567
18.10	CUESTIONES DE REPASO .....	568
<b>CAPÍTULO 19.</b>	<b>DESARROLLO Y MANTENIMIENTO DE SISTEMAS INFORMÁTICOS.....</b>	<b>571</b>
19.1	INTRODUCCIÓN.....	571
19.2	PLANTEAMIENTO Y METODOLOGÍA.....	572

19.3 AUDITORÍA DE LA ORGANIZACIÓN Y GESTIÓN DEL ÁREA DE DESARROLLO Y MANTENIMIENTO .....	575
19.4 AUDITORÍA DE PROYECTOS DE DESARROLLO Y MANTENIMIENTO .....	585
19.4.1 Auditoría de la gestión y planificación del proyecto .....	586
19.4.2 Auditoría de la fase de estudio de viabilidad .....	591
19.4.3 Auditoría de la fase de análisis.....	593
19.4.4 Auditoría de la fase de diseño .....	596
19.4.5 Auditoría de la fase de construcción .....	598
19.4.6 Auditoría de la fase de implantación y aceptación.....	602
19.4.7 Auditoría de la fase de mantenimiento.....	605
19.5 CONCLUSIONES .....	609
19.6 LECTURAS RECOMENDADAS.....	609
19.7 BIBLIOGRAFÍA .....	610
19.8 CUESTIONES DE REPASO .....	610
<b>CAPÍTULO 20. AUDITORÍA DE LA VIDEOVIGILANCIA .....</b>	<b>613</b>
20.1 INTRODUCCIÓN .....	613
20.2 SISTEMAS AVANZADOS DE RECOGIDA DE DATOS PERSONALES (SARDP).....	614
20.3 PRINCIPIOS RECTORES DE LA UTILIZACIÓN DE LOS SISTEMAS AVANZADOS DE RECOGIDA DE DATOS PERSONALES (SARP).....	615
20.4 DATOS PERSONALES ¿O NO? .....	617
20.5 LA FUERZA PREVENTIVA LLAMADA VIDEOVIGILANCIA .....	619
20.6 VIDEOVIGILANCIA ESTABLECIDA POR LAS FUERZAS Y CUERPOS DE SEGURIDAD DEL ESTADO .....	620
20.7 LA GRAN EXCEPCIÓN: LA VIDEOVIGILANCIA DE VÍAS PÚBLICAS Y REGULACIÓN DEL TRÁFICO.....	623
20.8 VIDEOVIGILANCIA ESTABLECIDA EN ZONAS PRIVADAS, DE SOPORTE A LA SEGURIDAD PÚBLICA .....	624
20.9 VIDEOVIGILANCIA AL SERVICIO DE LOS PARTICULARES .....	627
20.10 UNA PARTICULARIDAD, EL ACCESO A EDIFICIOS .....	629
20.11 LAS EMPRESAS DE SEGURIDAD .....	630
20.12 CONCLUSIONES .....	630
20.13 NORMATIVA BÁSICA A TENER EN CUENTA EN ESPAÑA .....	634
20.13.1 Rango de Ley Orgánica.....	634
20.13.2 Rango de Ley .....	634
20.13.3 Rango de Decreto-Ley .....	635
20.13.4 Rango de orden Ministerial.....	635
20.13.5 Rango de Instrucción de la Agencia Española de Protección de Datos.....	635

20.13.6 Rango autonómico .....	636
20.13.6.1 País Vasco.....	636
20.13.6.2 Catalunya.....	637
20.13.6.3 Madrid .....	637
20.14 BIBLIOGRAFÍA .....	637
20.15 CUESTIONES DE REPASO.....	638
<b>CAPÍTULO 21. AUDITORÍA REGLAMENTARIA DE LOS DATOS DE CARÁCTER PERSONAL .....</b>	<b>639</b>
21.1 INTRODUCCIÓN .....	639
21.1.1 El desarrollo reglamentario de la LORTAD.....	639
21.1.2 Hacia un nuevo desarrollo reglamentario .....	641
21.1.3 El concepto de fichero.....	641
21.2 NIVELES DE SEGURIDAD.....	643
21.3 LA OBLIGACIÓN DE AUDITAR .....	646
21.4 ANTES DE EMPEZAR.....	649
21.4.1 Contenido del informe.....	649
21.4.2 Pasos previos: consulta al Registro General de la AEPD.....	650
21.4.3 Interlocutores: la figura del Responsable de Seguridad.....	651
21.5 DESARROLLO DE LA AUDITORÍA.....	652
21.5.1 Alerta desde el primer momento: control de acceso físico a las instalaciones.....	652
21.5.2 Punto de partida: el documento de seguridad .....	653
21.5.3 Identificación y autenticación y control de accesos.....	658
21.5.4 Gestión de soportes .....	660
21.5.5 Copias de respaldo y recuperación.....	663
21.5.6 Registro de incidencias .....	665
21.5.7 Pruebas con datos reales.....	666
21.5.8 Telecomunicaciones.....	667
21.5.9 Régimen de trabajo fuera de los locales de la ubicación del fichero .....	667
21.5.10 Ficheros temporales .....	668
21.5.11 Control de acceso físico a la Sala de Servidores.....	668
21.5.12 Auditoría.....	669
21.5.13 Difusión de la normativa en materia de seguridad.....	670
21.5.14 ¿Nuevas verificaciones?.....	670
21.5.15 Medidas de seguridad aplicables a los ficheros y tratamientos no automatizados.....	671
21.6 INFRACCIONES Y SANCIONES .....	673

21.7 CONCLUSIONES .....	674
21.8 LECTURAS RECOMENDADAS.....	675
21.9 BIBLIOGRAFÍA .....	675
21.10 CUESTIONES DE REPASO.....	675
<b>ACRÓNIMOS .....</b>	<b>677</b>
<b>ÍNDICE ALFABÉTICO.....</b>	<b>691</b>