ÍNDICE

Autores XXI
Presentación XXIX
Prefacio XXXIII

PARTE I. INTRODUCCIÓN 1

CAPÍTULO 1. LA INFORMÁTICA COMO HERRAMIENTA DEL AUDITOR FINANCIERO *(Alonso Hernández García)* 3

1.1 Definición del entorno 3
1.2 Auditoría: concepto 4
1.3 Clases de auditoría 4
1.4 Procedimientos 5
1.5 Variación del objeto 7
1.6 Consultoría. Concepto 9
1.7 Ventajas de la Informática como herramienta de la Auditoría financiera 12
1.7.1 Grado de informatización 12
1.7.2 Mejora de las técnicas habituales 12
1.7.3 Evolución 19
1.7.4. Grado de utilización 20
1.8 Conclusiones 22
1.9 Cuestiones de repaso 22

CAPÍTULO 2. CONTROL INTERNO Y AUDITORÍA INFORMÁTICA *(Gloria Sánchez Valriberas)* 25

2.1 Introducción 25

2.2 Las funciones de control interno y auditoría informáticos 27
2.2.1 Control Interno Informático 27
2.2.2 Auditoría Informática 28
2.2.3 Control interno y auditoría informáticos: campos análogos.... 29
2.3 Sistema de Control Interno Informático 30
2.3.1 Definición y tipos de controles internos 30
2.3.2 Implantación de un sistema de controles internos informáticos 32
2.4 Conclusiones 42
2.5 Lecturas recomendadas 43
2.6 Cuestiones de repaso 43

CAPÍTULO 3. METODOLOGÍAS DE CONTROL INTERNO, SEGURIDAD Y AUDITORÍA INFORMÁTICA *(José María González Zubieta)* **45**

3.1 Introducción a las metodologías 45
3.2 Metodologías de evaluación de sistemas 49
3.2.1 Conceptos fundamentales 49
3.2.2 Tipos de metodologías 51
3.2.3 Metodologías más comunes 52
3.3 Las metodologías de Auditoría Informática 63
3.4 El plan auditor informático 65
3.5 Control interno informático. Sus métodos y procedimientos. Las herramientas de control 67
3.5.1 La función de control 67
3.5.2 Metodologías de clasificación de la información y de obtención de los procedimientos de control 70
3.5.3 Las herramientas de control 75
3.6 Conclusiones 82
3.7 Ejemplo de metodología de auditoría de una aplicación 82
3.8 Lecturas recomendadas 91
3.9 Cuestiones de repaso 91

CAPÍTULO 4. EL INFORME DE AUDITORÍA *(José de la Peña Sánchez)* **93**

4.1 Introducción 93
4.2 Las normas 95
4.3 La evidencia 97
4.4 Las irregularidades 98
4.5 La documentación 98
4.6 El informe 99
4.7 Conclusiones 104
4.8 Lecturas recomendadas 105
4.9 Cuestiones de repaso 106

CAPÍTULO 5. ORGANIZACIÓN DEL DEPARTAMENTO DE AUDITORÍA INFORMÁTICA *(Rafael Ruano Díez)* **107**

5.1 Antecedentes 107
5.2 Clases y tipos de Auditoría Informática 109
5.3 Función de Auditoría Informática 110
5.3.1 Definición 110
5.3.2 Perfiles profesionales de la función de Auditoría Informática 111
5.3.3 Funciones a desarrollar por la función de Auditoría Informática 112
5.4 Organización de la función de Auditoría Informática 115
5.5 Cuestiones de repaso 117

CAPÍTULO 6. EL MARCO JURÍDICO DE LA AUDITORÍA INFORMÁTICA *(Emilio del Peso Navarro)* **119**

6.1 Introducción 119
6.2 La protección de datos de carácter personal 121
6.3 La protección jurídica de los programas de ordenador 124
6.4 Las bases de datos y la multimedia 128
6.5 Los delitos informáticos 131
6.6 Los contratos informáticos 136
6.7 El intercambio electrónico de datos 141
6.8 La transferencia electrónica de fondos 142
6.9 La contratación electrónica 144
6.10 El documento electrónico 147
6.11 Lecturas recomendadas 148
6.12 Cuestiones de repaso 149

CAPÍTULO 7. DEONTOLOGÍA DEL AUDITOR INFORMÁTICO Y CÓDIGOS ÉTICOS *(Jorge Páez Mañá)* **151**

7.1 Introducción 151
7.2 Principios deontológicos aplicables a los auditores informáticos 156
7.2.1 Principio de beneficio del auditado 156
7.2.2 Principio de calidad 158
7.2.3 Principio de capacidad 158
7.2.4 Principio de cautela 159
7.2.5 Principio de comportamiento profesional 160
7.2.6 Principio de concentración en el trabajo 160
7.2.7 Principio de confianza 161
7.2.8 Principio de criterio propio 162
7.2.9 Principio de discreción 162
7.2.10 Principio de economía 163
7.2.11 Principio de formación continuada 163

7.2.12 Principio de fortalecimiento y respeto de la profesión 164
7.2.13 Principio de independencia 165
7.2.14 Principio de información suficiente 166
7.2.15 Principio de integridad moral 167
7.2.16 Principio de legalidad 167
7.2.17 Principio de libre competencia 168
7.2.18 Principio de no discriminación 168
7.2.19 Principio de no injerencia 169
7.2.20 Principio de precisión 169
7.2.21 Principio de publicidad adecuada 169
7.2.22 Principio de responsabilidad 170
7.2.23 Principio de secreto profesional 170
7.2.24 Principio de servicio público 172
7.2.25 Principio de veracidad 173
7.3 Conclusiones 174
7.4 Lecturas recomendadas 177
7.5 Cuestiones de repaso 177

PARTE II. PRINCIPALES ÁREAS DE LA AUDITORÍA INFORMÁTICA 179

CAPÍTULO 8. LA AUDITORÍA FÍSICA *(Gabriel Desmonts Basilio)* **181**

8.1 Introducción 181
8.2 La seguridad física 182
8.2.1 Antes 182
8.2.2 Durante 183
8.2.3 Después 184
8.3 Áreas de la seguridad física 185
8.4 Definición de Auditoría Física 187
8.5 Fuentes de la Auditoría Física 188
8.6 Objetivos de la Auditoría Física 189
8.7 Técnicas y herramientas del auditor 189
8.8 Responsabilidades de los auditores 190
8.9 Fases de la Auditoría Física 191
8.10 Desarrollo de las fases de la Auditoría Física 192
8.11 Lecturas recomendadas 195
8.12 Cuestiones de repaso 195

CAPÍTULO 9. AUDITORÍA DE LA OFIMÁTICA
(Manuel Gómez Vaz) **197**

9.1 Introducción 197
9.2 Controles de auditoría 198
9.2.1 Economía, eficacia y eficiencia 199

9.2.2 Seguridad 204
9.2.3 Normativa vigente 207
9.3 Conclusiones 208
9.4 Lecturas recomendadas 209
9.5 Cuestiones de repaso 210

CAPÍTULO 10. AUDITORÍA DE LA DIRECCIÓN
(Juan Miguel Ramos Escobosa) **211**

10.1 Introducción 211
10.2 Planificar 212
10.2.1 Plan estratégico de Sistemas de Información 212
10.2.2 Otros planes relacionados 214
10.3 Organizar y coordinar 215
10.3.1 Comité de Informática 215
10.3.2 Posición del Departamento de Informática en la empresa 217
10.3.3 Descripción de funciones y responsabilidades del Departamento de Informática. Segregación de funciones 218
10.3.4 Estándares de funcionamiento y procedimientos. Descripción de los puestos de trabajo 220
10.3.5 Gestión de recursos humanos: selección, evaluación del desempeño, formación, promoción, finalización 221
10.3.6 Comunicación 223
10.3.7 Gestión económica 223
10.3.8 Seguros 225
10.4 Controlar 226
10.4.1 Control y seguimiento 226
10.4.2 Cumplimiento de la normativa legal 227
10.5 Resumen 227
10.6 Lecturas recomendadas 228
10.7 Cuestiones de repaso 228

CAPÍTULO 11. AUDITORÍA DE LA EXPLOTACIÓN
(Eloy Peña Ramos) **231**

11.1 Introducción 231
11.2 Sistemas de Información 232
11.3 Carta de encargo 234
11.4 Planificación 234
11.4.1 Planificación estratégica 234
11.4.2 Planificación Administrativa 246
11.4.3 Planificación Técnica 246
11.5 Realización del trabajo (procedimientos) 247
11.5.1 Objetivo general 247
11.5.2 Objetivos específicos 247

11.6 Informes 253
11.6.1 Tipos de informes 253
11.6.2 Recomendaciones 254
11.6.3 Normas para elaborar los informes 254
11.7 La documentación de la auditoría y su organización 255
11.7.1 Papeles de trabajo 255
11.7.2 Archivos 256
11.8 Conclusiones 257
11.9 Lecturas recomendadas 258
11.10 Cuestiones de repaso 258

CAPÍTULO 12. AUDITORÍA DEL DESARROLLO
(José Antonio Rodero Rodero) **261**

12.1 Introducción 261
12.2 Importancia de la auditoría del desarrollo 262
12.3 Planteamiento y metodología 263
12.4 Auditoría de la organización y gestión del área de desarrollo 265
12.5 Auditoría de proyectos de desarrollo de S.I. 273
12.5.1 Aprobación, planificación y gestión del proyecto 274
12.5.2 Auditoría de la fase de análisis 278
12.5.3 Auditoría de la fase de diseño 284
12.5.4 Auditoría de la fase de construcción 286
12.5.5 Auditoría de la fase de implantación 289
12.6 Conclusiones 292
12.7 Lecturas recomendadas 292
12.8 Cuestiones de repaso 293

CAPÍTULO 13. AUDITORÍA DEL MANTENIMIENTO
(Juan Carlos Granja Alvarez) **295**

13.1 Introducción a la Auditoría Informática del mantenimiento del software 295
13.2 Listas de comprobación en Auditoría Informática del Mantenimiento 297
13.3 Modelización en la etapa de mantenimiento 297
13.4 Modelo de estimación en el mantenimiento 298
13.4.1 Elementos de la mantenibilidad 300
13.4.2 Métricas de mantenibilidad 300
13.4.3 Funciones de mantenibilidad 301
13.4.4 Métodos de implementación 302
13.5 Caso de estudio 306
13.6 Conclusiones 309
13.7 Lecturas recomendadas 309
13.8 Cuestiones de repaso 310

CAPÍTULO 14. AUDITORÍA DE BASES DE DATOS
(Mario G. Piattini Velthuis) **311**

14.1 Introducción 311
14.2 Metodologías para la auditoría de bases de datos 311
14.2.1 Metodología tradicional 312
14.2.2 Metodología de evaluación de riesgos 312
14.3 Objetivos de control en el ciclo de vida de una base de datos 314
14.3.1 Estudio previo y plan de trabajo 314
14.3.2 Concepción de la base de datos y selección del equipo 318
14.3.3 Diseño y carga 319
14.3.4 Explotación y mantenimiento 320
14.3.5 Revisión post-implantación 321
14.3.6 Otros procesos auxiliares 322
14.4 Auditoría y control interno en un entorno de bases de datos 322
14.4.1 Sistema de Gestión de Bases de Datos (SGBD) 323
14.4.2 Software de auditoría 324
14.4.3 Sistema de monitorización y ajuste (*tuning*) 324
14.4.4 Sistema Operativo (SO) 324
14.4.5 Monitor de Transacciones 324
14.4.6 Protocolos y Sistemas Distribuidos 325
14.4.7 Paquete de seguridad 325
14.4.8 Diccionarios de datos 326
14.4.9 Herramientas CASE (Computer Aided System/Software Engineering)/IPSE (Integrated Project Support Environments) 326
14.4.10 Lenguajes de Cuarta Generación (L4G) independientes 326
14.4.11 Facilidades de usuario 327
14.4.12 Herramientas de "minería de datos" 328
14.4.13 Aplicaciones 328
14.5 Técnicas para el control de bases de datos en un entorno complejo 329
14.5.1 Matrices de control 329
14.5.2 Análisis de los caminos de acceso 330
14.6 Conclusiones 330
14.7 Lecturas recomendadas 332
14.8 Cuestiones de repaso 332

CAPÍTULO 15. LA AUDITORÍA DE TÉCNICA DE SISTEMAS
(Julio A. Novoa Bermejo) **335**

15.1 Ámbito de técnica de sistemas 335
15.2 Definición de la función 337
15.3 El nivel de servicio 337
15.4 Los procedimientos 339
15.4.1 Instalación y puesta en servicio 339
15.4.2 Mantenimiento y soporte 340

15.4.3 Requisitos para otros componentes 340
15.4.4 Resolución de incidencias 341
15.4.5 Seguridad y control 342
15.4.6 Información sobre la actividad 343
15.5 Los controles 343
15.6 Auditoría de la función 351
15.7 Consideraciones sobre la tecnología y su evolución 356
15.8 Algunas referencias 358
15.9 Lecturas recomendadas 359
15.10 Cuestiones de repaso 359

CAPÍTULO 16. AUDITORÍA DE LA CALIDAD
(José Luis Lucero Manresa) **361**

16.1 Preámbulo 361
16.2 Definiciones previas 362
16.3 Introducción 363
16.3.1 Revisión 364
16.3.2 Elemento software 364
16.3.3 Auditoría 364
16.3.4 Concepto de evaluación según la EEA 365
16.3.5 Concepto de Auditoría según la EEA 365
16.4 Características de la calidad según ISO 9126 365
16.4.1 Características 365
16.4.2 Modelo ISO Extendido 367
16.5 Objetivos de las Auditorías de Calidad 370
16.6 Procesos de Calidad 371
16.7 El proceso de Auditoría del Software 375
16.8 Auditoría de Sistemas de Calidad de Software 381
16.9 Proceso de aseguramiento de la calidad descrito por ISO 12207 381
16.9.1 Implementación del proceso 383
16.9.2 Aseguramiento del producto 384
16.9.3 Aseguramiento del proceso 384
16.9.4 Aseguramiento de la calidad de los sistemas 385
16.10 Proceso de Auditoría descrito por ISO 12207 385
16.10.1 Implementación del proceso 385
16.10.2 Auditoría 386
16.11 Conclusiones 386
16.12 Lecturas recomendadas 387
16.13 Cuestiones de repaso 387

CAPÍTULO 17. AUDITORÍA DE LA SEGURIDAD
(Miguel Ángel Ramos González) **389**

17.1 Introducción 389

17.2 Áreas que puede cubrir la auditoría de la seguridad 393
17.3 Evaluación de riesgos 395
17.4 Fases de la auditoría de seguridad 399
17.5 Auditoría de la seguridad física 400
17.6 Auditoría de la seguridad lógica 402
17.7 Auditoría de la seguridad y el desarrollo de aplicaciones 404
17.8 Auditoría de la seguridad en el área de producción 404
17.9 Auditoría de la seguridad de los datos 405
17.10 Auditoría de la seguridad en comunicaciones y redes 407
17.11 Auditoría de la continuidad de las operaciones 409
17.12 Fuentes de la auditoría 411
17.13 El perfil del auditor 411
17.14 Técnicas, métodos y herramientas 413
17.15 Consideraciones respecto al informe 414
17.16 Contratación de auditoría externa 416
17.17 Relación de Auditoría con Administración de Seguridad 417
17.18 Conclusiones 419
17.19 Lecturas recomendadas 421
17.20 Cuestiones de repaso 422

CAPÍTULO 18. AUDITORÍA DE REDES
(José Ignacio Boixo Pérez-Holanda) **423**

18.1 Terminología de redes. Modelo OSI 423
18.2 Vulnerabilidades en redes 426
18.3 Protocolos de alto nivel 428
18.4 Redes abiertas (TCP/IP) 430
18.5 Auditando la gerencia de comunicaciones 434
18.6 Auditando la red física 437
18.7 Auditando la red lógica 440
18.8 Lecturas recomendadas 443
18.9 Cuestiones de repaso 444

CAPÍTULO 19. AUDITORÍA DE APLICACIONES
(José María Madurga Oteiza) **445**

19.1 Introducción 445
19.2 Problemática de la auditoria de una aplicación informática 446
19.3 Herramientas de uso más común en la auditoría de una aplicación 450
19.3.1 Entrevistas 450
19.3.2 Encuestas 451
19.3.3 Observación del trabajo realizado por los usuarios 452
19.3.4 Pruebas de conformidad 452
19.3.5 Pruebas substantivas o de validación 453
19.3.6 Uso del ordenador 454

19.4 Etapas de la auditoría de una aplicación informática 456
19.4.1 Recogida de información y documentación sobre la aplicación 456
19.4.2 Determinación de los objetivos y alcance de la auditoría 458
19.4.3 Planificación de la auditoría 461
19.4.4 Trabajo de campo, informe e implantación de mejoras 462
19.5 Conclusiones 463
19.6 Lecturas recomendadas 464
19.7 Cuestiones de repaso 464

CAPÍTULO 20. AUDITORÍA INFORMÁTICA DE EIS/DSS Y APLICACIONES DE SIMULACIÓN *(Manuel Palao García-Suelto)* ... **467**

20.1 Propósito y enfoque 467
20.2 Desarrollo de las definiciones operativas de los conceptos clave 468
20.2.1 Auditoría Informática 468
20.2.2 SID[EIS]/SAD[DSS] 469
20.2.3 Aplicaciones de Simulación 472
20.3 Singularidades de la AI de los SID[EIS], SAD[DSS] y Simulación 474
20.3.1 AI de los SID[EIS] 475
20.3.2 AI de los SAD[DSS] y Simulación 480
20.4 Conclusiones 481
20.5 Lecturas recomendadas 481
20.6 Cuestiones de repaso 481

CAPÍTULO 21. AUDITORÍA JURÍDICA DE ENTORNOS INFORMÁTICOS *(Josep Jover i Padró y Silvia Cabrera Vilaplana)* **483**

21.1 Introducción 483
21.2 Auditoría del entorno 485
21.3 Auditoría de las personas 488
21.4 Auditoría de la información 493
21.5 Auditoría de los ficheros 493
21.5.1 Niveles de protección de los ficheros 494
21.5.2 Mecanismos de seguridad del fichero 496
21.5.3 Formación de la figura del responsable del fichero 496
21.6 Conclusiones 504
21.7 Lecturas recomendadas 505
21.8 Cuestiones de repaso 505

PARTE III. AUDITORÍA INFORMÁTICA EN DIVERSOS SECTORES **507**

CAPÍTULO 22. AUDITORÍA INFORMÁTICA EN EL SECTOR BANCARIO *(Pilar Amador Contra)* **509**

22.1 Características generales de la Auditoría Informática en las entidades financieras 509
22.1.1 Necesidad y beneficios de la auditoría informática en la banca 509
22.1.2 Tipología de las actividades a auditar 511
22.1.3 Objetivos de la auditoría y preparación del plan de trabajo 514
22.2 Auditoría Informática de una aplicación bancaria típica 515
22.2.1 Criterios para la planificación anual de los trabajos 516
22.2.2 Establecimiento del ámbito de la auditoría 517
22.2.3 Procedimientos de auditoría a emplear 519
22.2.4 Consideraciones a tener en cuenta durante la realización de la auditoría 521
22.3 Auditoría informática de la protección de datos personales 523
22.3.1 La importancia y el valor de la información en el sector bancario 523
22.3.2 Actividades de auditoría en relación con la protección de datos personales 525
22.4 Cuestiones de repaso 530

CAPÍTULO 23. AUDITORÍA INFORMÁTICA EN EL SECTOR AÉREO *(Aurelio Hermoso Baños)* **533**

23.1 Introducción 533
23.2 Sistema de reservas Amadeus 534
23.3 Facturación entre compañías aéreas 535
23.4 Código de conducta para CRS 536
23.5 Procesos informáticos 538
23.6 Auditoría Informática 540
23.7 Conclusiones 548
23.8 Lecturas recomendadas 548
23.9 Cuestiones de repaso 549

CAPÍTULO 24. AUDITORÍA INFORMÁTICA EN LA ADMINISTRACIÓN *(Víctor Izquierdo Loyola)* **551**

24.1 Introducción 551
24.2 Las TIC en la LRJ-PAC 552
24.3 La informatización de registros 554

24.4 Las previsiones del Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de las técnicas EIT por la Administración General del Estado 555
24.5 Identificación de los requisitos de seguridad, normalización y conservación en el texto del Real Decreto 263/1996 556
24.5.1 Garantías de seguridad de soportes, medios y aplicaciones 556
24.5.2 Emisión de documentos: procedimientos para garantizar la validez de los medios; integridad, conservación, identidad del autor y autenticidad de la voluntad 557
24.5.3 Validez de las copias: garantía de su autenticidad, integridad y conservación 558
24.5.4 Garantía de realización de las comunicaciones 558
24.5.5 Validez de comunicaciones y notificaciones a los ciudadanos; constancia de transmisión y recepción, estampación de fechas y contenido integro, identificación fidedigna de remitente y destinatario 559
24.5.6 Comunicaciones por medios preferentes del usuario; comunicación de la forma y código de accesos a sus sistemas de comunicación 559
24.5.7 Validez de fechas de notificación para cómputo de plazos; anotación en los registros generales o auxiliares a que hace referencia el artículo 38 de la LRJ-PAC 560
24.5.8 Conservación de documentos; medidas de seguridad que garanticen la identidad e integridad de la información necesaria para reproducirlos 561
24.5.9 Acceso a documentos almacenados; disposiciones del artículo 37 de la Ley 30/1992, y, en su caso, de la Ley Orgánica 5/1992. Normas de desarrollo 561
24.5.10 Almacenamiento de documentos; medidas de seguridad que garanticen su integridad, autenticidad, calidad, protección y conservación 562
24.6 Conclusiones sobre el papel de la Auditoría Informática en la Administración Electrónica 563
24.7 Cuestiones de repaso 565

CAPÍTULO 25. AUDITORÍA INFORMÁTICA EN LAS PYMES *(Carlos M. Fernández Sánchez)* **567**

25.1 Preámbulo 567
25.1.1 Las PYMES y las tecnologías de la Información 567
25.1.2 Metodología de la Auditoría Informática 568
25.2 Introducción 568
25.2.1 ¿En qué consiste la guía de autoevaluación? 568
25.2.2 ¿A quién va dirigida? 569
25.2.3 Conocimientos necesarios 569
25.2.4 Entornos de aplicación 570

25.2.5 Metodología utilizada 570
25.3 Utilización de la guía 571
25.3.1 Fases de la autoevaluación 571
25.3.2 Valoración de resultados 573
25.4. Miniordenadores e informática distribuida. Riesgo en la eficacia del servicio informático 574
25.5 Conclusiones 581
25.6 Lecturas recomendadas 582
25.7 Cuestiones de repaso 583

Apéndice: Formulario de protección de datos *(Josep Jover i Padró y Silvia Cabrera Vilaplana)* **585**

Acrónimos **593**

Bibliografía **599**

Índice alfabético **605**