

Es propiedad,
© 2005, **Jordi Velasco Dobaño**
Luis Velasco Massip

Para la presente edición:
© 2005, **Editorial Bosch, S.A.**
Comte d'Urgell, 51 bis. 08011 Barcelona
<http://www.bosch.es>

Primera edición: abril, 2005

ISBN: 84-9790-133-9
Depósito legal: B. 9.825-2005

Prohibida la reproducción total o parcial de esta obra, por
cualquier medio o en cualquier soporte sin consentimiento
expreso de los propietarios del *copyright*.

Abreviaturas utilizadas.....	9
Prólogo	11

PARTE I CONCEPTOS

CAPÍTULO 1. Introducción a la protección de datos de carácter personal	15
1.1. Concepto de dato de carácter personal	15
1.2. Clasificación de los datos de carácter personal.....	16
1.3. Marco legal.....	17
1.4. La Agencia Española de Protección de Datos	18
CAPÍTULO 2. Introducción a las técnicas auditoras	21
2.1. Concepto de auditoría	21
2.2. Evolución histórica	21
2.2.1. La auditoría de cuentas	21
2.2.2. La auditoría de los sistemas de gestión	22
2.2.3. Otras auditorías legales	23
2.3. Características fundamentales de la auditoría.....	23
2.3.1. Objetividad.....	23
2.3.2. Independencia.....	24
2.3.3. Sistematización.....	24
2.3.4. Documentación	24
2.3.5. Periodicidad	25
2.4. Un trabajo de muestreo	25
2.5. Fases de auditoría.....	28
2.6. El perfil del auditor de protección de datos	29
CAPÍTULO 3. La necesidad de la auditoría de protección de datos ..	31
3.1. La necesidad legal	31
3.2. Responsables de la obligación de auditoría	33
3.3. Ampliando conceptos	33
3.4. La auditoría voluntaria	35

CAPÍTULO 4. Elementos a auditar	37
4.1. Los sistemas de la información.....	37
4.2. Los ficheros y tratamientos.....	40
4.2.1. Los ficheros y tratamientos que no contienen datos de carácter personal.....	40
4.2.2. Los ficheros y tratamientos que contienen datos de carácter personal..	40
4.2.3. Los ficheros y tratamientos automatizados y los no automatizados...	41
4.2.4. El fichero de personal propio y su tratamiento	42
4.3. Aspectos legales de la LOPD.....	44
CAPÍTULO 5. Otras normas técnicas relacionadas	47
5.1. ISO 17799, COBIT y COSO	47
5.2. Comparativo ISO 17799 y Reglamento de Seguridad	48
 PARTE II EL TRABAJO PRÁCTICO	
CAPÍTULO 1. La pre-auditoría	57
1.1. Introducción.....	57
1.2. Conocimiento del encargo.....	59
1.2.1. Objetivos.....	59
1.2.2. Alcance	60
1.2.3. Áreas a auditar.....	60
1.3. Configuración del equipo auditor	60
1.3.1. Auditor Jefe	60
1.3.2. Asistentes de auditoría	61
1.3.3. Técnicos Especialistas.....	61
1.4. Solicitud y análisis de la documentación.....	61
1.5. Planificación de auditoría.....	63
1.5.1. Preparación del Programa de trabajo	63
1.5.2. Designación de funciones	63
1.6. Programa de auditoría.....	63
CAPÍTULO 2. La ejecución de la auditoría	65
2.1. Introducción.....	65
2.2. Reunión inicial	65
2.3. Recogida de evidencias.....	66
2.4. Documentación de los resultados	67
2.5. Reunión final.....	67
CAPÍTULO 3. Guía para la ejecución de la auditoría	69
3.1. Explicación de la guía	69
3.1.1. Programa de trabajo.....	70
3.1.2. Papeles de trabajo	71
3.1.3. Cuestionarios	73
3.2. Aplicación de la guía.....	73
3.3. Resumen de la guía	75
CAPÍTULO 4. El programa de trabajo	87
CAPÍTULO 5. Los papeles de trabajo	101

CAPÍTULO 6. Los cuestionarios	121
CAPÍTULO 7. Guía para la redacción del informe de auditoría	131
7.1. Introducción.....	132
7.2. Modelo normalizado de informe	133
7.3. Explicación previa del modelo de informe de auditoría	133
7.3.1. Parte A: Antecedentes	134
7.3.2. Parte B: Valoración de las medidas y controles de seguridad	136
7.3.3. Parte C: Conclusiones	137
7.3.4. Anexos	139
CAPÍTULO 8. El informe de auditoría	149
CAPÍTULO 9. Las conclusiones del responsable de seguridad	149
9.1. Introducción.....	151
9.2. Modelo de ficha de conclusiones del Responsable de Seguridad	153
CAPÍTULO 10. El archivo de la auditoría	153
10.1. Introducción.....	153
10.2. Archivo Permanente.....	154
10.3. Archivo Corriente	154
10.4. Archivo Administrativo	154
10.4.1. La oferta económica	155
10.4.2. Contrato de auditoría	158
10.4.3. Carta de Representación.....	158

PARTE III ANEXO LEGISLATIVO

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal (modificada por la Ley 62/2003).....	163
Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal.....	191
Real Decreto 1332/1994, de 20 de junio, por el que se desarrollan algunos preceptos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal	199
Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos	209
Real Decreto 156/1996, de 2 de febrero, por el que se modifica el Estatuto de la Agencia de Protección de Datos	223
Bibliografía.....	225