



Índice

AGRADECIMIENTOS	13
INTRODUCCIÓN	15
CAPÍTULO 1. SEGURIDAD INFORMÁTICA.....	17
1.1 PRINCIPIOS DE LA SEGURIDAD INFORMÁTICA	19
1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD	21
1.2.1 Confidencialidad	23
1.2.2 Integridad	25
1.2.3 Disponibilidad.....	26
1.2.4 Autenticación.....	28
1.2.5 No repudio.....	28
1.3 ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO: HARDWARE, SOFTWARE Y DATOS.....	30
1.4 AMENAZAS.....	32
1.5 REFERENCIAS WEB.....	44
RESUMEN DEL CAPÍTULO.....	45
EJERCICIOS PROPUESTOS.....	46
TEST DE CONOCIMIENTOS	48
CAPÍTULO 2. SEGURIDAD FÍSICA	49
2.1 PRINCIPIOS DE LA SEGURIDAD FÍSICA	50
2.1.1 Control de acceso	51
2.1.2 Sistemas biométricos	55
2.1.3 Protección electrónica	61
2.1.4 Condiciones ambientales.....	64
2.2 SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (SAI).....	66
2.2.1 Causas y efectos de los problemas de la red eléctrica.....	67
2.2.2 Tipos de SAI	70
2.2.3 Potencia necesaria	72
2.3 CENTROS DE PROCESADO DE DATOS (CPD)	74
2.3.1 Equipamiento de un CPD.....	75

2.4 REFERENCIAS WEB.....	84
RESUMEN DEL CAPÍTULO.....	84
EJERCICIOS PROPUESTOS.....	86
TEST DE CONOCIMIENTOS	86
CAPÍTULO 3. SEGURIDAD LÓGICA.....	89
3.1 PRINCIPIOS DE LA SEGURIDAD LÓGICA.....	90
3.2 CONTROLES DE ACCESO	91
3.2.1 Identificación y autenticación.....	91
3.2.2 Roles	93
3.2.3 Limitaciones a los servicios	93
3.2.4 Modalidad de acceso	93
3.2.5 Ubicación y horario.....	96
3.2.6 Administración	96
3.2.7 Administración del personal y usuarios - Organización del personal.....	97
3.3 IDENTIFICACIÓN	104
3.3.1 ¿Qué hace que una contraseña sea segura?.....	104
3.3.2 Estrategias que deben evitarse con respecto a las contraseñas.....	105
3.4 ACTUALIZACIÓN DE SISTEMAS Y APLICACIONES.....	112
3.4.1 Actualizaciones automáticas.....	113
3.4.2 Actualización automática del navegador web	116
3.4.3 Actualización del resto de aplicaciones.....	117
3.5 REFERENCIAS WEB.....	119
RESUMEN DEL CAPÍTULO.....	120
EJERCICIOS PROPUESTOS.....	121
TEST DE CONOCIMIENTOS	121
CAPÍTULO 4. SOFTWARE DE SEGURIDAD.....	123
4.1 SOFTWARE MALICIOSO	124
4.1.1 ¿Qué son los virus?.....	124
4.2 CLASIFICACIÓN. TIPOS DE VIRUS.....	129
4.2.1 Según su capacidad de propagación.....	129
4.2.2 Según las acciones que realizan	132
4.2.3 Otras clasificaciones	138
4.2.4 Programas no recomendables	140
4.3 PROTECCIÓN Y DESINFECCIÓN.....	142
4.3.1 Seguridad en Internet	144
4.4 HERRAMIENTAS SOFTWARE ANTIMALWARE.....	147
4.4.1 Antivirus	147
4.4.1.1 Antivirus de Escritorio	148
4.4.1.2 Antivirus en Línea	150

4.4.1.3 Laboratorios de pruebas.....	152
4.4.2 Antispyware.....	154
4.4.3 Otras herramientas Antimalware	156
4.4.3.1 Herramientas de bloqueo:.....	156
4.5 REFERENCIAS WEB.....	160
RESUMEN DEL CAPÍTULO.....	161
EJERCICIOS PROPUESTOS.....	162
TEST DE CONOCIMIENTOS	162
CAPÍTULO 5. GESTIÓN DEL ALMACENAMIENTO DE LA INFORMACIÓN	165
5.1 ALMACENAMIENTO DE LA INFORMACIÓN: RENDIMIENTO, DISPONIBILIDAD, ACCESIBILIDAD	166
5.1.1 Rendimiento.....	168
5.1.2 Disponibilidad.....	170
5.1.3 Accesibilidad.....	171
5.2 MEDIOS DE ALMACENAMIENTO.....	172
5.2.1 Soporte de almacenamiento de la información.....	172
5.2.2 Lectura/Escritura	174
5.2.3 Acceso a la información	174
5.2.4 Ubicación de la unidad	175
5.2.5 Conexión entre soporte y unidad.....	175
5.3 ALMACENAMIENTO REDUNDANTE Y DISTRIBUIDO.....	177
5.3.1 RAID.....	177
5.3.1.1 RAID 0 (Data Striping)	180
5.3.1.2 RAID 1 (Data Mirroring).....	181
5.3.1.3 RAID 2, 3 y 4	182
5.3.1.4 RAID 5.....	183
5.3.1.5 Niveles RAID anidados	184
5.3.2 CENTROS DE RESPALDO	185
5.4 ALMACENAMIENTO REMOTO	186
5.5 COPIAS DE SEGURIDAD Y RESTAURACIÓN.....	191
5.5.1 Modelos de almacén de datos	192
5.5.2 Propuestas de copia de seguridad de datos	193
5.5.3 Manipulación de los datos de la copia de seguridad	194
5.5.4 Software de copias de seguridad y restauración.....	195
5.6 REFERENCIAS WEB.....	198
RESUMEN DEL CAPÍTULO.....	199
EJERCICIOS PROPUESTOS.....	200
TEST DE CONOCIMIENTOS	201

CAPÍTULO 6. SEGURIDAD EN REDES	203
6.1 ASPECTOS GENERALES	204
6.2 CORTAFUEGOS	211
6.3 LISTAS DE CONTROL DE ACCESO (ACL) Y FILTRADO DE PAQUETES	217
6.3.1 ACL en routers.....	217
6.3.2 Iptables	219
6.4 REDES INALÁMBRICAS	222
6.4.1 ¿Qué es una red inalámbrica?	225
6.4.2 Consejos de seguridad	226
6.5 REFERENCIAS WEB	231
RESUMEN DEL CAPÍTULO.....	232
EJERCICIOS PROPUESTOS.....	233
TEST DE CONOCIMIENTOS	233
CAPÍTULO 7. CRIPTOGRAFÍA.....	235
7.1 PRINCIPIOS DE CRIPTOGRAFÍA	236
7.1.1 Criptografía simétrica	239
7.1.2 Ataques criptográficos.....	240
7.1.3 Criptografía de clave asimétrica	242
7.1.4 Criptografía de clave asimétrica. Cifrado de clave pública.....	245
7.1.5 Criptografía de clave asimétrica. Firma digital	247
7.1.6 Certificados digitales.....	249
7.1.7 Terceras partes de confianza	251
7.2 FIRMA ELECTRÓNICA.....	253
7.2.1 Documento Nacional de Identidad electrónico (DNIe)	255
7.3 REFERENCIAS WEB	262
RESUMEN DEL CAPÍTULO.....	263
EJERCICIOS PROPUESTOS.....	264
TEST DE CONOCIMIENTOS	265
CAPÍTULO 8. NORMATIVA LEGAL EN MATERIA DE SEGURIDAD INFORMÁTICA	267
8.1 INTRODUCCIÓN A LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD).....	268
8.1.1 Ámbito de aplicación de la LOPD.....	270
8.1.1.1 Ámbito de aplicación temporal.....	272
8.1.2 Agencia Española de Protección de Datos (AGPD)	274
8.1.3 Niveles de seguridad.....	278
8.1.4 Órganos de control y posibles sanciones	279
8.2 INTRODUCCIÓN A LSSI, LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN.....	282

8.2.1	Ámbito de aplicación de la LSSI.....	283
8.2.2	Artículo 10.1 de la LSSI.....	284
8.2.3	Infracciones y sanciones.....	285
8.2.4	Comunicaciones comerciales.....	287
8.3	REFERENCIAS WEB.....	290
	RESUMEN DEL CAPÍTULO.....	291
	EJERCICIOS PROPUESTOS.....	291
	TEST DE CONOCIMIENTOS.....	292
	CAPÍTULO 9. AUDITORÍAS DE SEGURIDAD.....	293
9.1	AUDITORÍA DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN	294
9.2	METODOLOGÍA DE AUDITORÍA DE SEGURIDAD.....	295
9.3	REFERENCIAS WEB.....	297
	RESUMEN DEL CAPÍTULO.....	297
	EJERCICIOS PROPUESTOS.....	298
	TEST DE CONOCIMIENTOS.....	299
	ÍNDICE ALFABÉTICO	301