

# Contenido

---

<b>Descripción del libro</b> .....	<b>XI</b>
Qué ofrece este libro .....	XI
Qué no incluye este libro .....	XII
Por qué este libro .....	XIV
Motivos para escribir este libro .....	XIV
Nota del autor .....	XV
Organización de este libro .....	XVI
<b>1. Necesidad de seguridad</b> .....	<b>1</b>
Buenas y malas noticias .....	1
Definición de la seguridad en computadoras personales .....	3
¿Qué está en juego? .....	13
¿Necesita realmente este libro? .....	15
Ataques, amenazas y temores .....	18
Cuestiones de seguridad .....	20
Hipótesis de trabajo .....	26
Resumen .....	26
<b>2. Las bases</b> .....	<b>27</b>
Personas, personas y personas .....	27
Copias de seguridad, copias de seguridad y copias de seguridad .....	29
Llaves y cerraduras .....	30
Conexión de la computadora .....	37
Seguridad en el arranque .....	51
Resumen .....	59

<b>10. La amenaza de los virus</b> .....	<b>389</b>
Buenas y malas noticias .....	389
Qué son los virus .....	393
De dónde vienen .....	397
Conocimiento de los virus .....	400
Escritores de virus .....	403
Ejemplos de virus .....	408
Medidas defensivas .....	417
Técnicas defensivas .....	431
Hardware antivirus .....	433
Software antivirus .....	433
Más programas antivirus .....	439
En caso de infección .....	448
Resumen .....	450
<b>11. Piratería del software y sus peligros</b> .....	<b>451</b>
Piratería del software .....	451
Por qué la gente defrauda .....	459
Historia de la protección contra copias .....	462
Mirones y entrometidos .....	473
Formateado, borrado y recuperación .....	479
Acceso después del borrado .....	487
Resumen .....	494
<b>12. Seguridad en redes y comunicaciones</b> .....	<b>497</b>
Los combatientes .....	497
El campo de batalla .....	500
Ideas básicas y terminología sobre redes .....	506
Situación actual de las redes .....	515
Aspectos hardware de la seguridad en la red .....	519
Redes y tolerancia a fallos .....	525
Aspectos software de la seguridad en la red .....	531
Seguridad en redes Novell .....	538
Conexiones telefónicas .....	548
Conexión micro-gram computadora .....	552
Enlaces rápidos .....	554
Puntos débiles .....	555
Resumen .....	556
<b>13. Piratas y otros factores humanos</b> .....	<b>557</b>
El problema de las personas .....	557
La solución de las personas .....	560
Piratas .....	562
El intrusismo y la ley .....	564

<b>7. Control del acceso a la computadora</b> .....	<b>217</b>
Control del acceso a la instalación .....	217
Llaves físicas .....	219
Gestión de las llaves físicas .....	220
Dispositivos de autenticación .....	221
Ausencia temporal del puesto de trabajo .....	231
Escuchas electrónicas .....	232
Archivos por lotes para control de inicialización .....	240
Uso de la orden ASK .....	242
La orden ANSWER .....	245
Uso de REPLY.COM .....	247
Seguridad en CONFIG.SYS .....	252
Problemas con discos de arranque .....	253
Un diseño seguro .....	253
Otros métodos hardware .....	260
Resumen .....	264
<b>8. Control del acceso a los archivos</b> .....	<b>267</b>
El papel del control de acceso a archivos .....	267
Un escenario de acceso a archivos .....	270
Protección gratuita con clave de acceso .....	274
Análisis de los archivos .....	278
Aspectos técnicos del cifrado .....	288
Selección y administración de claves de acceso .....	310
Controles de acceso comerciales para sistemas DOS .....	318
Comentario: el debate secreto-intimidad .....	324
Resumen .....	326
<b>9. Copia de seguridad de archivos</b> .....	<b>327</b>
El dilema de la copia de seguridad .....	327
Estrategias de copia de seguridad .....	330
Copia de seguridad en disquetes .....	339
Datos, archivos y copia de seguridad en cinta .....	344
Dispositivos intercambiables de alta capacidad .....	348
Almacenamiento óptico .....	352
CD-ROM .....	354
Factores de coste .....	355
Evaluación de software de copias de seguridad .....	357
Ordenes de copia de seguridad en el DOS .....	358
La restauración .....	365
Las órdenes COPY .....	370
Otros productos para copia de seguridad en DOS .....	377
Copia de seguridad en Macintosh .....	379
Seguridad del software .....	385
Resumen .....	387

<b>3. Primeros pasos</b> .....	<b>61</b>
Protección básica de archivos .....	61
Protección durante la ausencia .....	66
Protección mediante clave de acceso .....	69
Recuperación y prevención de desastres a nivel de disco .....	79
<b>4. Análisis y planificación</b> .....	<b>93</b>
Terminología del riesgo .....	93
Metodología .....	96
Realización de la evaluación de riesgos .....	101
Preguntas a hacer .....	112
Evaluación de la probabilidad .....	121
Evaluación del valor .....	124
Política de seguridad .....	126
Plan de contingencia .....	126
Volver a empezar .....	127
Sistemas comerciales de análisis y planificación .....	128
Resumen .....	137
<b>5. Seguridad para hardware</b> .....	<b>139</b>
Ejemplo de seguridad .....	139
Dispositivos de fijación .....	140
Alimentación y control interno .....	144
Protección frente a daños .....	146
Marcado de los equipos .....	147
Seguridad del perímetro .....	148
Protección del sistema completo .....	157
Carteles de advertencia .....	158
Introducción a los archivos por lotes .....	160
Rango de productos .....	168
Resumen .....	168
<b>6. Mantenimiento en funcionamiento de las computadoras</b> .....	<b>169</b>
Alimentación de la computadora .....	170
Fusibles, tierras y diferenciales .....	176
Regulación del suministro eléctrico .....	182
El problema del ruido .....	187
Acondicionadores de corriente .....	193
Precauciones a la hora de comprar .....	193
Garantía del suministro eléctrico .....	194
Asistencia software .....	207
Baterías incluidas .....	207
¿La aldea global? .....	209
Seguros para computadoras .....	211
Resumen .....	215

Protección contra el intrusismo .....	565
Resumen .....	567
<b>14. Conclusiones y desarrollos futuros .....</b>	<b>569</b>
Resumen general .....	569
Una aproximación por niveles .....	574
El siguiente frente .....	575
Conclusión .....	579
<b>Apéndice A. Seguridad en línea .....</b>	<b>581</b>
<b>Apéndice B. Un catálogo de virus .....</b>	<b>599</b>
<b>Índice .....</b>	<b>613</b>