

# Contenido

---

Agradecimientos .....	xxi
Introducción .....	xxiii

## PARTE I ASPECTOS GENERALES DE LA SEGURIDAD

<b>CAPÍTULO 1. El paisaje de las redes: redes de área local y redes globales .....</b>	<b>3</b>
De los PC a las redes corporativas .....	4
Computadoras personales .....	4
Redes de área local (LAN) .....	5
Redes interconectadas .....	6
Arquitecturas cliente-servidor distribuidas .....	7
Redes heterogéneas .....	7
Redes de campus, metropolitanas y de área extendida .....	8
Acceso remoto y computadoras portátiles .....	9
La empresa conectada a internet .....	10
Redes TCP/IP .....	10
Servicios de información basados en TCP/IP .....	11
Redes virtuales de área extendida .....	13
<b>CAPÍTULO 2. Amenazas de seguridad .....</b>	<b>15</b>
¿Qué son las amenazas? .....	16
Amenazas naturales y asaltos directos .....	16
Áreas débiles de la seguridad .....	17
¿Quiénes son los piratas informáticos? .....	18
La amenaza interna .....	19
Principios de un pirata informático .....	20

Métodos de ataque .....	21
Invasiones del puesto .....	22
Ataques telefónicos .....	23
Piratería de cuentas y contraseñas de usuarios .....	24
Piratería de sistemas de confianza .....	25
Escuchas electrónicas y rastreadores de conexiones .....	26
Otras áreas vulnerables .....	26
Internet y TCP/IP .....	30
Ataques y TCP/IP e Internet .....	31
Virus y caballos de Troya .....	32
Amenazas naturales .....	33
<b>CAPÍTULO 3. Contramedidas .....</b>	<b>35</b>
Definición de seguridad .....	35
Costes de seguridad .....	36
Medidas protectoras .....	37
Medidas de seguridad física .....	37
Sistemas redundantes y tolerantes a fallos .....	39
Copias de seguridad .....	39
Encriptación .....	40
Protección frente a virus .....	40
Protección del correo electrónico .....	41
Protección de las impresoras y las colas de impresión .....	42
Protección de las comunicaciones en redes .....	43
Protección de las conexiones remotas y de los usuarios móviles ....	43
Medidas de seguridad en Internet .....	45
Cortafuegos .....	45
Controles de acceso .....	46
Cuentas de usuarios .....	47
Inicios de sesión y contraseñas .....	47
Protección de directorios y archivos .....	48
Identificación avanzada .....	49
Auditoría de sistemas .....	51
Detección y tratamiento de ataques .....	52
¡Contraataques! .....	53
<b>CAPÍTULO 4. Planes de seguridad y administración .....</b>	<b>55</b>
Planificación de la seguridad .....	55
Obtención de ayuda .....	57
Temas de administración de la información y de control .....	58
Temas de acceso .....	59
Administradores .....	60

Estándares de seguridad .....	61
Educación de los usuarios .....	62
Recuperación de desastres .....	63
Planes de seguridad .....	64
Documentos de planes y procedimientos .....	65

**PARTE II**  
**Seguridad en Windows NT**

<b>CAPÍTULO 5. Visión global de la seguridad en Windows NT .....</b>	<b>73</b>
Sobre la seguridad C2 .....	74
Visión microscópica de la seguridad en Windows NT .....	75
Arquitectura Windows NT .....	76
Diseño orientado a objetos .....	78
El subsistema de seguridad de Windows NT .....	79
El proceso de inicio de sesión .....	81
Controles de acceso discrecionales .....	83
El sistema de auditoría de Windows NT .....	85
Modelos de red Windows .....	87
El modelo de trabajo en grupos .....	88
Control de accesos a nivel compartido .....	89
Control de accesos a nivel de usuario .....	90
Limitaciones de seguridad del modelo de trabajo en grupos .....	91
Dominios .....	92
Relaciones de confianza .....	94
Cuentas de usuarios y de grupos .....	95
Cuentas de usuarios .....	95
Planes de cuentas .....	97
Grupos .....	98
Derechos de usuario .....	99
Perfiles de usuario .....	100
El sistema de archivos de Windows NT (NTFS) .....	101
Compartición de recursos .....	102
Configuración de permisos .....	102
 <b>CAPÍTULO 6. Amenazas específicas y soluciones en Windows NT .....</b>	 <b>105</b>
Sobre agujeros y puertas traseras .....	106
Seguridad en el inicio de sesión .....	107
Técnica de asalto a la cuenta del Administrador .....	107
Precauciones y políticas de inicio de sesión generales .....	110
Seguridad comprometida por clientes débiles .....	111

Administración del sistema .....	112
Configuración de sistemas seguros .....	113
Jerarquía administrativa .....	113
Cuentas de usuarios .....	114
El sistema de archivos .....	114
Impresoras y seguridad .....	115
El Registro .....	115
Algunas configuraciones del registro .....	116
Temas de seguridad en redes .....	119
Utilidades de monitorización .....	119
Rastreadores y monitores de red .....	120
Problemas de compartición de archivos en el entorno Windows ....	121
Conexiones Web e Internet .....	122

**CAPÍTULO 7. Dominios, inicios de sesión en dominios y controles de seguridad .....** **125**

Dominios .....	126
Relaciones de confianza .....	128
Más acerca de los dominios .....	130
La base de datos del Directorio .....	133
Más acerca de las relaciones de confianza .....	134
Cómo se establece la confianza .....	135
Cuentas de dominio .....	137
Sobre grupos locales y globales .....	137
Administración de estaciones de trabajo .....	139
Configuración de dominios .....	139
Administración de dominios con el Administrador de servidores ...	140
Modelo de dominio único .....	141
Modelo de dominio maestro único .....	142
Modelo de dominio maestro múltiple .....	142
Elección de un modelo de dominio .....	143
Inicio de sesión en dominios .....	144
Planes de seguridad .....	147
Restricciones de contraseñas .....	148
Bloqueo de cuentas .....	150
Sugerencias para la seguridad en los dominios .....	152

**CAPÍTULO 8. Administración de la seguridad para grupos y usuarios .....** **155**

Terminología .....	155
El Administrador de usuarios .....	156
Herramientas del administrador de clientes de la red .....	158

Cuentas de usuarios .....	159
Propiedades de nombres de usuarios y contraseñas .....	159
Propiedades de las cuentas de usuarios .....	161
La cuenta del Administrador .....	164
La cuenta Sistema .....	166
La cuenta Invitado .....	166
Rastreo de cuentas de usuarios .....	168
Grupos .....	170
Grupos locales y globales .....	171
Los grupos locales .....	173
Los grupos globales .....	178
Creación de grupos .....	180
Derechos .....	182
Administración de entornos de usuario .....	185

**CAPÍTULO 9. La seguridad del sistema de archivos y la compartición de recursos ..... 187**

Compartición y permisos, ¿cuál es la diferencia? .....	188
¿Cómo es la seguridad en NTFS? .....	195
Compresión y encriptación .....	196
Protección física .....	197
Administración de permisos .....	198
Dónde y cómo configurar permisos .....	198
Permisos individuales .....	200
Permisos estándar .....	201
Permisos de archivos .....	203
Comparación de NTFS con otros sistemas de archivos .....	204
Permisos acumulados, herencia y propiedad .....	205
Sujetos de los permisos .....	206
Permisos por defecto .....	207
Permisos sugeridos .....	211
Permisos para Todos .....	212
Permisos para programas .....	214
Permisos de copia y movimiento de archivos .....	214
Protección de archivos del directorio raíz .....	216
Activación de alertas de accesos no autorizados .....	216
Cosas que debe saber sobre archivos borrados .....	216
Compartición de directorios y archivos .....	217
Compartición de recursos en Windows NT .....	219
Ocultación de comparticiones .....	221
Administración de comparticiones con el Administrador de servidores .....	222
Utilización de servicios SMB en Web .....	223
Uso de los servidores Web para servicios de archivos .....	223

Nuevos sistemas de archivos .....	224
FAT32 .....	224
Sistema de archivos comunes Internet .....	225
Sistema de archivos distribuidos del Windows NT Server .....	225
<b>CAPÍTULO 10. Administración, monitorización y auditoría .....</b>	<b>227</b>
Herramientas del Administrador de clientes .....	228
Diagnóstico Windows NT .....	228
La utilidad Servidor y el Administrador de servidores .....	230
Administración de propiedades del servidor .....	232
Administración de servicios .....	234
Cambio de la cuenta de inicio para los servicios .....	238
Servicios de enlazado y desenlazado en sistemas multipropietarios .....	239
Las órdenes NET .....	241
Órdenes NET para Windows NT .....	243
Órdenes NET para clientes DOS y Windows .....	245
Órdenes TCP/IP .....	246
Visualización de actividades con el Monitor del sistema .....	248
Alertas de seguridad .....	250
Monitorización de la red .....	254
La seguridad del Monitor de red .....	256
Auditorías .....	257
Configuración de auditorías de cuentas de usuarios .....	258
Configuración de auditoría del sistema de archivos .....	259
Uso del Visor de sucesos .....	261
Técnicas para auditorías .....	263
La cuenta del auditor ficticio .....	266
<b>CAPÍTULO 11. Tolerancia a fallos y protección de datos .....</b>	<b>269</b>
Protección del sistema operativo .....	269
El Disco de reparaciones de emergencia .....	270
Errores fatales y caídas del sistema .....	270
Protección del Registro .....	271
Recuperación de un sistema operativo dañado .....	272
Tolerancia a fallos en el servidor Windows NT .....	273
Reflejado de disco .....	275
Conjuntos de bandas para discos .....	277
Seguridad mediante la duplicación del directorio .....	278
Configuración de la duplicación .....	280
Copia de seguridad de datos .....	283
Operadores de copias de seguridad .....	284
Temas de seguridad en cintas .....	285

Tipos de copias de seguridad.....	286
Métodos de rotación de cintas .....	287
La utilidad de Copias de seguridad de Windows NT .....	287
Problemas de alimentación eléctrica y soluciones .....	292
Ruidos .....	293
Equipo con mala conexión a tierra .....	293
Tensión insuficiente .....	293
Sobretensión .....	294
Zumbidos .....	294
Soluciones a los problemas de alimentación .....	294
Uso de fuentes de alimentación permanentes .....	295

**PARTE III**  
**TEMAS GENERALES DE SEGURIDAD EN LA RED**

<b>CAPÍTULO 12. Temas de seguridad Cliente/Estación de trabajo .....</b>	<b>299</b>
Clientes en el entorno de compartición de redes.....	300
Implementación de la compartición de archivos e impresoras para clientes .....	301
Desactivación de la compartición de archivos e impresoras para clientes .....	301
Sistemas de archivos comunes Internet (CIFS) .....	302
Problemas de seguridad en estaciones de trabajo cliente.....	303
Actualizaciones de seguridad que hay que conocer .....	303
Inicio de sesión Windows 95.....	304
Inseguridades en las contraseñas .....	305
Seguridad y administración de clientes de red .....	308
PC/DACS para Windows 95 .....	308
RSA Secure para Windows y Macintosh .....	309
Administración remota .....	310
Servidor de administración de sistemas Microsoft .....	313
Administración de perfiles y directivas .....	313
Perfiles .....	315
Administración de directivas .....	317
 <b>CAPÍTULO 13. Temas de seguridad Microsoft BackOffice .....</b>	 <b>321</b>
Conexiones BackOffice a Internet.....	323
Microsoft SQL Server.....	323
Seguridad del SQL Server .....	324
Acceso e integridad de la base de datos.....	325
Protección de datos .....	326

Propiedades de administración .....	327
Otras opciones de seguridad de SQL Server .....	328
Microsoft Exchange .....	330
Componentes Exchange Server .....	332
Administración del sistema .....	334
Conexiones Exchange .....	335
Seguridad en Microsoft Exchange .....	335
System Management Server .....	342
<b>CAPÍTULO 14. Temas de acceso remoto .....</b>	<b>345</b>
Servicio de acceso remoto (RAS) Windows NT .....	347
Protocolos RAS y técnicas de comunicación .....	349
Configuración del servidor RAS .....	351
Configuración de clientes RAS .....	354
Administración de servicios RAS y opciones de seguridad .....	356
Administración de permisos de usuarios .....	356
Restricción del acceso a la red .....	358
Envío de mensajes y desconexión de usuarios .....	360
Opciones de retollamada .....	360
Inicio de sesión RAS y métodos de identificación .....	361
Dónde configurar la encriptación .....	362
Protocolos de encriptación .....	363
Identificación de usuarios de doble sentido .....	364
Auditoría del servidor de accesos remotos .....	365
<b>CAPÍTULO 15. Reforzamiento de la seguridad en WAN privadas y virtuales .....</b>	<b>367</b>
Construcción de redes corporativas .....	367
Protección de WAN y accesos remotos .....	369
Temas de sucursales .....	370
WAN en el entorno Windows NT .....	371
Modelos interredes .....	374
Protocolos de seguridad WAN y encriptación .....	376
Encriptación de enlaces WAN .....	379
Otras técnicas de seguridad .....	380
Soporte RAS en WAN .....	381
Conexiones Internet con RAS .....	383
Llamada automática .....	386
Redes virtuales privadas sobre Internet .....	386
Red de área extensa segura (S/WAN) .....	388
Protocolo punto a punto canalizado (PPTP) .....	389
Internet Tunnel de DEC .....	392



<b>CAPÍTULO 16. Seguridad corporativa.....</b>	<b>395</b>
NetWare en el entorno Windows NT.....	396
Servicios Cliente y Pasarela para NetWare .....	397
Compartición de archivos e impresoras para NetWare (FPNW) .....	398
Administrador del servicio de directorio para NetWare (DSMN)...	399
Examinar y trabajar con sistemas NetWare.....	399
Seguridad a nivel de usuario en entornos NetWare .....	401
Temas de inicio de sesión y contraseñas .....	404
Seguridad en los entornos Windows NT y UNIX.....	405
Compartición de archivos UNIX/Windows NT .....	406
Seguridad en los servicios Macintosh .....	409
Servicios para la seguridad Macintosh .....	410
Seguridad en el inicio de sesión.....	412
Microsoft SNA Server .....	413
Propiedades del Microsoft SNA Server.....	413
Administración y seguridad .....	416
Administración de la seguridad corporativa .....	417
Administrador de seguridad corporativa de Axent (ESM).....	418
RAS Enterprise de Technologic Software.....	419

**PARTE IV**

**Estrategias de defensa para redes públicas**

<b>CAPÍTULO 17. Temas de seguridad Internet y TCP/IP.....</b>	<b>423</b>
Conexión a internet .....	424
Herramientas de muestreo.....	427
SATAN (Herramienta del administración de seguridad para análisis de redes) .....	428
SAFEsuite de Internet Security Systems .....	429
Escuchas en la red .....	432
Monitor de red Windows NT .....	435
IP-Watcher de En Garde Systems .....	435
Netcat: un rastreador/escáner.....	438
Otros ataques.....	439
Falsificaciones .....	439
Ataques a encaminadores.....	441
Problemas de protocolo en aplicaciones Internet.....	442
<b>CAPÍTULO 18. Cortafuegos y servidores proxy.....</b>	<b>447</b>
Estrategias defensivas.....	448
Clasificación de cortafuegos .....	452

Planes de cortafuegos .....	455
Más acerca de encaminadores de filtrado .....	457
Puertos y filtrado de puertos .....	458
¿Cómo son de seguros los encaminadores de filtrado? .....	460
Cortafuegos de gama alta .....	461
Implementaciones de cortafuegos .....	462
La cache del servidor proxy .....	466
Socks .....	466
Cortafuegos comerciales .....	467
Black Hole de Milkyway Networks .....	468
FireWall/Plus de Network-1 .....	471
Eagle NT de Raptor Systems .....	471
Cortafuegos Would-Be .....	473
Cortafuegos a medida Windows NT .....	474
Variaciones .....	478
<b>CAPÍTULO 19. Microsoft Proxy Server .....</b>	<b>481</b>
Más acerca de los servicios proxy .....	484
Instalación y configuración del Proxy Server .....	486
Ejecución de la configuración .....	489
Configuración del Proxy Server .....	490
Identificación de clientes .....	491
Permisos para Proxy Server .....	492
Uso de la cache del Proxy Server .....	492
Filtrado con el Proxy Server .....	493
Servicio Conectores de Windows remotos (RWS) .....	494
Configuración RWS .....	496
Configuración de clientes .....	497
<b>CAPÍTULO 20. Protección de Microsoft Internet Information Server .....</b>	<b>499</b>
Protocolos y estándares Web .....	500
El modelo Web cliente-servidor .....	502
Más acerca de HTTP .....	503
Estructuras de directorio del servidor Web .....	504
Configuración y administración .....	505
Servicios de suscripción e inicio de sesión anónimos .....	511
Administración de cuentas de usuario en el servidor Web .....	513
Más acerca de la cuenta de usuario anónimo .....	513
Petición del inicio de sesión en la cuenta del usuario .....	514
Controles de inicio de sesión .....	515
Controles de acceso a directorios .....	516

Filtrado de direcciones IP .....	517
Seguridad en el canal cliente-servidor .....	518
Microsoft Internet Explorer 3.0 .....	520
<b>CAPÍTULO 21. Temas de seguridad comercial en Internet .....</b>	<b>523</b>
Dónde conseguir información comercial en Internet .....	524
Temas de seguridad Internet .....	524
Técnicas criptográficas .....	526
Firmas digitales e integridad de los mensajes .....	527
Autoridades de certificación .....	528
Pago al contado .....	529
Micropagos .....	530
Administración de derechos de copia .....	531
Servicios Microsoft Merchant .....	531
Internet Shopper .....	532
Componentes de los servicios Merchant de la parte del servidor ....	532
Microsoft Internet Security Framework .....	533
CryptoAPI .....	535
Servicios de seguridad de alto nivel .....	536
Información adicional .....	540

**PARTE V**  
**Apéndices**

<b>APÉNDICE A. Seguridad e inicio de sesión en Windows NT .....</b>	<b>543</b>
Modelo de seguridad Windows NT .....	544
Inicio de sesión e identificación .....	545
Tipos de inicio de sesión e identificación .....	545
Inicio de sesión local y en dominio .....	546
Detalles de la secuencia de inicio de sesión .....	547
Inicio de sesión y acceso remoto .....	548
Seguridad en las contraseñas y procedimientos de identificación .....	552
La base de datos SAM .....	552
Procedimiento de identificación .....	553
<b>APÉNDICE B. Criptografía y comunicación privada .....</b>	<b>555</b>
Protección de las comunicaciones privadas .....	556
Sobres digitales .....	559
Firmas digitales e integridad de mensajes .....	559
El criptosistema de clave pública RSA .....	561

Técnicas criptográficas .....	563
Funciones de un sentido (OWF) y puertas de escape .....	563
Cifradores y algoritmos hash .....	564
Microsoft CryptoAPI .....	567
<b>APÉNDICE C. Virus, caballos de Troya y otras amenazas .....</b>	<b>569</b>
Virus y otras amenazas .....	570
Otras amenazas .....	571
Cómo ocurre una infección .....	573
Detección y prevención .....	574
Planes de control de virus .....	574
Programas de detección de virus .....	575
Virus en el entorno Windows NT .....	576
Virus del Registro de arranque maestro (MBR) y del registro de arranque .....	576
Virus DOS y Windows 3.1 en sesiones DOS en Windows NT .....	577
Virus que se ejecutan en entornos Windows NT .....	578
Antivirus Scanner de Norton para Windows NT .....	578
<b>APÉNDICE D. Paquetes de evaluación de la seguridad .....</b>	<b>581</b>
Utilidades del kit de recursos de Windows NT de Microsoft .....	581
Un sistema experto: Kane Security Analyst .....	582
DumpACL de Somarsoft .....	587
Internet Scanner de Internet Security Systems .....	591
<b>APÉNDICE E. Pasos para la evaluación de la seguridad NT .....</b>	<b>593</b>
Cumplimiento de C2 .....	593
Evaluación estándar .....	594
Planes de cuentas y restricciones .....	595
Cuentas de usuarios .....	595
Grupos .....	597
Derechos de los usuarios .....	599
Archivos, carpetas, permisos y comparticiones .....	600
Control de virus y caballos de Troya .....	602
Auditorías y registros de sucesos .....	602
Tolerancia a fallos, copias de seguridad y SAI .....	603
<b>APÉNDICE F. Temas de seguridad en el Registro .....</b>	<b>605</b>
Seguridad y protección del Registro .....	606
Cambio de los permisos de las claves .....	607

Auditoría .....	609
Copias de seguridad y restauración de claves .....	610
Configuraciones de alta seguridad del Registro .....	611
Información adicional de seguridad para el Registro .....	611
Permisos relajados del Registro, por Frank Ramos de Somarsoft ...	612
<b>APÉNDICE G. Puertos en el entorno TCP/IP .....</b>	<b>615</b>
<b>Indice .....</b>	<b>627</b>