

CONTENIDO

Introducción	XV
Capítulo 1	
Generalidades sobre la administración de una red de computadoras	1
1.1. Introducción	3
1.2. Funciones de la administración de redes de computadoras	5
1.2.1. Configuración y administración	5
1.2.2. Fallas	11
1.2.3. Contabilidad (administración de los usuarios)	13
1.2.4. Desempeño	14
1.2.5. Seguridad	15
1.3. Servicios de una red de computadoras	17
1.3.1. DHCP	18
1.3.2. DNS	19
1.3.3. Telnet	21
1.3.4. SSH	22
1.3.5. FTP y TFTP	23
1.3.6. WWW: HTTP y HTTPS	26
1.3.7. NFS	30
1.3.8. CIFS	33
1.3.9. E-mail: SMTP, POP, IMAP y SASL	34
1.4. Análisis y monitoreo	41
1.4.1. Protocolo de administración de red (SNMP)	43
1.4.2. Analizadores de protocolos	44
1.4.3. Planificadores	46
1.4.4. Análisis de desempeño de la red: tráfico y servicios	48
1.5. Seguridad básica	49
1.5.1. Los elementos de seguridad	49
1.5.2. Medidas de seguridad lógica con relación al usuario	52
1.5.3. Medidas de seguridad física para el control de acceso a las redes	56
1.5.4. Tipos de riesgos	58
1.5.5. Tipos de ataques y vulnerabilidades	61



1.5.6 Control de acceso, respaldos, autenticación y elementos de protección perimetral	63
1.5.7. Seguridad en NetBIOS	65
1.5.8. Herramientas de control y seguimiento de accesos	65
1.6. Conclusiones	67

Capítulo 2

Administración de una red de computadoras	75
2.1 Introducción	77
2.2. Funciones de la administración de redes de computadoras	78
2.3. Modelo de gestión ISO	81
2.4. Plataformas de gestión de una red de computadoras	83
2.4.1. OpenView	84
2.5. Aplicaciones de la gestión de redes convergentes	86
2.5.1. La gestión y tecnología en redes	87
2.6. Modelos de gestión de redes de computadoras y sus servicios	89
2.6.1. Modelo funcional OSI-NM	89
2.7. Los objetivos de las redes en el mercado y su importancia en las empresas	93
2.7.1. Aplicación de las redes en la actualidad	94
2.7.2. Aplicación de las redes al trabajo	94
2.7.3. Ejemplo de una aplicación del sistema operativo Android en redes de telefonía móvil	96
2.8. Conclusiones	98
2.9. Banco de preguntas para la certificación de CISCO	99
Prácticas	105

Capítulo 3

Seguridad informática	143
3.1. Introducción	145
3.2. Principios y fundamentos de la teoría de la seguridad informática	148
3.3. Objetivos de la seguridad de la información e informática	151
3.4. Políticas de seguridad	154
3.4.1. Grupo de elaboración de políticas para la seguridad informática	157
3.4.2. Niveles de seguridad	158
3.4.3. Esquemas y modelos de seguridad	160



3.5. Procedimientos de seguridad informática	163
3.5.1. Estándares de seguridad informática	166
3.6. Arquitectura de seguridad de la información	167
3.7. Vulnerabilidades en la seguridad informática	170
3.8. Riesgos en la seguridad informática	171
3.8.1. Gestión de riesgos	173
3.8.2. Análisis de riesgos	177
3.8.3. Enfoques cualitativos y cuantitativos	179
3.9. Exposición de datos	184
3.10. Conclusiones	185

Capítulo 4

La gestión de la seguridad informática en redes de computadoras	189
4.1. Introducción	191
4.2. Especificación de los principales mecanismos de seguridad	192
4.2.1. Criptografía: algoritmos simétricos, asimétricos e híbridos	192
4.2.2. Cortafuegos	204
4.2.3. Redes privadas virtuales (VPN)	208
4.2.4. Creación e infraestructura de redes virtuales	210
4.2.5. Ventajas y desventajas de las VPN	211
4.2.6. Intranets y extranets en VPN	213
4.2.7. Sistema de detección de intrusos (IDS)	215
4.3. Seguridad por niveles	217
4.3.1. Seguridad a nivel aplicación	217
4.3.2. Seguridad a nivel transporte	218
4.3.3. Seguridad a nivel de enlace	219
4.4. Identificación de ataques y de respuestas con base en las políticas de seguridad	222
4.5. Sistemas unificados de administración de seguridad	225
4.6. Seguridad en las redes inalámbricas	228
4.6.1. Política de seguridad inalámbrica	229
4.6.2. Pasos prácticos para una seguridad inalámbrica	229
4.7. Autenticación y sistemas biométricos	230
4.8. Nuevas tecnologías en seguridad	234
4.9. Auditoría al sistema de seguridad integral	237



4.10. Modelos de seguridad informática: militar y comercial (el caso estadounidense)	239
4.11. Principios de la seguridad informática en el ámbito legal	245
4.11.1. Marco legal en México de servicios electrónicos relacionados con seguridad	246
4.12. Conclusiones	251

Capítulo 5

Administración de la seguridad informática	255
5.1. Introducción	257
5.2. Auditorías y evaluación de la seguridad informática	259
5.3. Evaluación de la seguridad informática implantada	260
5.4. Problemas en los programas de control de la seguridad informática	261
5.5. Mejores prácticas de integridad de los sistemas de información	264
5.6. Conclusiones	273
5.7. Banco de preguntas para la certificación de CISCO	274

Capítulo 6

La administración estratégica de la seguridad informática	285
6.1. Introducción	287
6.2. El inventario y la clasificación de activos de la seguridad informática	288
6.3. Diagnósticos de la seguridad informática	301
6.4. Revisión y actualización de procedimientos en seguridad informática	303
6.5. Recuperación y continuidad del negocio en caso de desastres (DRP/BCP/BCM)	306
6.5.1. Conceptos y terminología usados en la continuidad del negocio	308
6.5.2. Metodología para el desarrollo de continuidad del negocio	309
6.5.3. Herramientas de software para el desarrollo y mantenimiento del DRP/BCP/BCM	310
6.5.4. Factores de éxito de la continuidad del negocio	314
6.6. Servicios administrados (seguridad en la nube)	316
6.6.1. Seguridad en la nube	317
6.7. Servicios administrados (seguridad en la nube)	319
6.7.1. Ley Federal de protección de datos	321
6.7.2. Gobernanza de Internet	323
6.8. Conclusiones	325
Prácticas	327



Capítulo 7

Situación actual de las redes de computadoras	401
7.1. Introducción	403
7.2. El inventario y la clasificación de activos de la seguridad informática	404
7.2.1. Integración segura de MANET a redes de infraestructura	404
7.2.2. Evaluación de extensiones de seguridad para DNS	406
7.2.3. Virtualización de redes	407
7.2.4. Cableado estructurado, estándares y nuevos componentes	408
7.3. Últimas tendencias en redes	410
7.3.1. El Internet de las cosas	414
7.3.2. La realidad aumentada	417
7.3.3. Web 3.0	423
7.3.4. Web 4.0	425
7.3.5. Drones	427
7.4. Conclusiones	430
Glosario	435
Índice analítico	439