

# Contenido

## **CAPÍTULO 1**

<b>Introducción a la seguridad de la información . . . . .</b>	<b>19</b>
Enrique Daltabuit Godás	
Manejo de la información . . . . .	19
Tecnologías naturales de la información . . . . .	23
Tecnología humana de la información . . . . .	24
Seguridad de la información . . . . .	26
<b>El órgano de la información . . . . .</b>	<b>30</b>
Desarrollo del cerebro . . . . .	30
Mecanismo de producción del lenguaje . . . . .	40
Mecanismo de captación del lenguaje . . . . .	42
Sistema visual . . . . .	43
<b>Comunicación . . . . .</b>	<b>44</b>
Aparición del lenguaje . . . . .	47
Percepción del lenguaje . . . . .	48
Producción del lenguaje . . . . .	49
<b>Evolución de la comunicación . . . . .</b>	<b>50</b>
Estructura fonética del lenguaje . . . . .	53
Precursores de la era de la información . . . . .	57
<b>Consecuencias de la escritura . . . . .</b>	<b>58</b>
<b>La era digital . . . . .</b>	<b>59</b>
Información en formato binario . . . . .	59
<b>Referencias . . . . .</b>	<b>70</b>

<b>CAPÍTULO 2</b>	
<b>Problemática de la seguridad y conceptos básicos . . . . .</b>	<b>75</b>
Leobardo Hernández Audelo	
Enrique Daltabuit Godás	
Introducción . . . . .	75
Primeros problemas de seguridad informática . . . . .	76
Historia del cómputo . . . . .	76
Evolución temprana del cómputo . . . . .	77
Computadoras multiusuario . . . . .	80
Primera revolución: la computadora personal . . . . .	81
Problemas de seguridad de la PC . . . . .	82
Segunda revolución: Internet . . . . .	86
Problemas de seguridad en Internet . . . . .	87
Tercera revolución: ubicuidad . . . . .	91
Vulnerabilidades, amenazas y ataques . . . . .	93
Servicios de seguridad . . . . .	97
Arquitectura de seguridad OSI . . . . .	100
Descripción de servicios de seguridad . . . . .	101
Implementación de los servicios . . . . .	104
Referencias . . . . .	107
<b>CAPÍTULO 3</b>	
<b>Criptografía . . . . .</b>	<b>109</b>
Leobardo Hernández Audelo	
Introducción . . . . .	109
Criptología . . . . .	110
Criptografía . . . . .	111
Información cifrada . . . . .	112
La historia . . . . .	112
Épocas en criptografía . . . . .	114
Criptografía moderna . . . . .	115
Bases de la criptografía . . . . .	118

Reglas de Kerckhoff . . . . .	120
Criptografía simétrica o de clave secreta. . . . .	122
Transposición, sustitución y producto . . . . .	122
Cifrado por bloques . . . . .	123
Cifrados de flujo . . . . .	124
Criptografía asimétrica o de clave pública . . . . .	125
Reto de Diffie & Hellman . . . . .	125
Sistemas de clave pública. . . . .	128
Sistema RSA . . . . .	130
Referencias. . . . .	131
<b>CAPÍTULO 4</b>	
<b>Aplicaciones criptográficas. . . . .</b>	<b>133</b>
Leobardo Hernández Audelo	
Introducción. . . . .	133
Protocolos . . . . .	134
Definición de protocolo. . . . .	134
Notación. . . . .	135
Tipos de protocolos . . . . .	135
Protocolos criptográficos para implementar servicios de seguridad	138
Confidencialidad con DES . . . . .	139
Autenticación con DES . . . . .	139
Integridad con DES . . . . .	140
Problemas con criptografía simétrica . . . . .	140
Confidencialidad con RSA. . . . .	141
Autenticación con RSA . . . . .	141
Confidencialidad, autenticación e integridad con RSA . . . . .	142
Soluciones y problemas de la criptografía asimétrica. . . . .	143
Firmas digitales. . . . .	145
Firmas digitales y funciones de dispersión (Hash). . . . .	150
Algoritmo ElGamal . . . . .	151
Algoritmo DSA (Digital Signature Algorithm) . . . . .	154
Protocolos para utilización de firmas digitales . . . . .	158

Certificados digitales .....	161
Definición.....	161
Autoridades certificadoras .....	162
Validación de certificados .....	166
Certificados digitales X.509 y estándares PKCS .....	170
Listas de revocación .....	174
Aplicaciones de los certificados digitales .....	176
Conclusión .....	187
Protocolos de acuerdo e intercambio de claves .....	188
Problema del acuerdo e intercambio de clave.....	188
Problema de la administración de claves .....	189
Claves de sesión y protocolos de establecimiento de clave .....	191
Protocolos de autenticación e intercambio de clave .....	197
Protocolos de autenticación.....	197
Protocolos de autenticación e intercambio de clave .....	200
Aplicaciones de la criptografía simétrica y funciones	
Hash a la verificación de integridad y autenticidad .....	203
Códigos para integridad y autenticación de mensajes .....	203
Generación de códigos de verificación	
de integridad/autenticación de mensajes .....	206
Referencias.....	211
<b>CAPÍTULO 5</b>	
<b>Administración de la seguridad .....</b>	<b>213</b>
Enrique Daltaubuit Godás	
José de Jesús Vázquez	
Introducción.....	213
Misión de seguridad .....	213
Consenso .....	215
El método Delphi .....	216
Políticas de seguridad.....	221
Criterios de la OCDE.....	221
Posturas .....	225
Beneficios.....	226
Proceso del diseño de políticas .....	227

Algunas políticas necesarias . . . . .	228
Procedimientos . . . . .	231
Lecciones del libro naranja . . . . .	233
Information Technology Security Evaluation Criteria (ITSEC) . . . . .	238
Listas de precauciones . . . . .	240
Análisis de riesgos . . . . .	247
Otros enfoques . . . . .	263
Análisis cuantitativo . . . . .	267
Modelos de madurez . . . . .	281
Directrices gerenciales de COBIT . . . . .	281
ISM3 1.0 . . . . .	289
MMSI . . . . .	295
Normatividad sobre políticas de seguridad informática . . . . .	302
Principios generales . . . . .	302
Consistencia de políticas . . . . .	320
Criterios normativos modernos (Criterios comunes) . . . . .	329
Perfil de protección . . . . .	331
Referencias . . . . .	339
<b>Capítulo 6</b>	
<b>Control de acceso . . . . .</b>	<b>343</b>
Enrique Daltaubuit Godás	
Introducción . . . . .	343
Protección perimetral . . . . .	345
Autenticación . . . . .	348
Identificación y autenticación . . . . .	350
Registro . . . . .	350
Identificación . . . . .	351
Autenticación . . . . .	351
Uso de los autenticadores . . . . .	383
Control de acceso discrecional . . . . .	384
Control de acceso por mandato . . . . .	386
Control de acceso obligatorio . . . . .	390

Aplicación al control de acceso físico .....	393
Debilidad del control de acceso obligatorio para preservar la confidencialidad .....	393
Compartimientos .....	397
Políticas de apoyo .....	398
Estándares actuales .....	399
Referencias .....	422
<b>CAPÍTULO 7</b>	
<b>Detección de intrusos .....</b>	<b>425</b>
Guillermo Mallén Fullerton	
Introducción .....	425
Control de accesos .....	427
Métodos de detección de intrusos .....	429
Bitácoras .....	429
Monitoreo y análisis de la actividad de los usuarios .....	430
Detección de ataques conocidos .....	431
Monitoreo del tráfico en la red .....	431
Verificación de la integridad de los archivos críticos del sistema	431
Auditoría de la configuración del sistema y sus vulnerabilidades	432
Sistemas realmente seguros .....	432
Intrusos .....	433
Expectativas en cuanto a la seguridad .....	435
Bitácoras .....	436
Analizadores de bitácoras .....	437
Análisis <i>a posteriori</i> .....	439
Monitoreo y análisis de la actividad de los usuarios .....	443
Problemática de la implantación .....	444
Reconocimiento de ataques conocidos .....	446
Monitoreo del tráfico en la red .....	447
Verificación de la integridad de los archivos críticos del sistema	450
Auditoría de la configuración del sistema y sus vulnerabilidades	451
Referencias .....	452

**CAPÍTULO 8**

<b>Código malicioso</b> .....	<b>455</b>
Guillermo Mallén Fullerton	
Introducción.....	455
Virus.....	459
El tamaño del problema .....	459
La teoría de los virus .....	462
Definición de virus informático .....	464
Ejemplos de virus .....	471
Segunda definición .....	475
Virus reales.....	477
Consecuencias de las infecciones por virus informáticos.....	479
Las generaciones de virus .....	483
Generadores de virus y cajas de herramientas .....	486
Los virus en Internet .....	487
Medidas contra los virus .....	489
El futuro .....	491
Historia de los virus .....	492
Ataques de penetración .....	498
Ataques de denegación de servicios .....	502
Programas de espionaje .....	503
Caballos de Troya .....	505
Bombas de tiempo .....	505
El problema de las combinaciones .....	506
Referencias.....	506

**CAPÍTULO 9**

<b>Seguridad en sistemas operativos</b> .....	<b>507</b>
Guillermo Mallén Fullerton	
Introducción.....	507
Normas de seguridad en sistemas operativos .....	520
División D: protección mínima .....	523
División C: protección discrecional .....	524
División B: protección obligatoria .....	526
División A: protección verificada .....	530

Selección de niveles de seguridad . . . . .	530
Los niveles de seguridad y la práctica cotidiana . . . . .	532
Configuración de seguridad de sistemas Linux/Unix . . . . .	535
Principios básicos . . . . .	535
Pasos para instalar un sistema seguro. . . . .	541
Referencias. . . . .	545
<b>CAPÍTULO 10</b>	
<b>Herramientas y protocolos . . . . .</b>	<b>547</b>
Leobardo Hernández Audelo	
Introducción. . . . .	547
Sistema de nombres de dominio (Domain Name System-DNS) .	548
Antecedentes . . . . .	548
Definición y estructura . . . . .	549
Servidor de nombres . . . . .	550
Ataques a DNS. . . . .	554
Redes virtuales privadas (VPN) . . . . .	564
Definición y concepto . . . . .	564
Elementos de una conexión VPN . . . . .	565
Conexiones VPN . . . . .	566
Propiedades de una VPN . . . . .	567
Conexiones VPN Internet e intranet . . . . .	569
Administración de VPN. . . . .	573
Protocolo de Túnel Punto a Punto (PPTP). . . . .	574
Seguridad de VPN . . . . .	578
Problemas comunes de VPN. . . . .	586
SET (Secure Electronic Transaction) . . . . .	587
Introducción . . . . .	587
Características de SET. . . . .	588
El protocolo SET . . . . .	588
PGP. . . . .	591
Introducción . . . . .	591
La historia PGP . . . . .	591
Elementos principales de PGP . . . . .	592



Algoritmos que usa PGP . . . . .	599
Cifrado de paquetes PGP . . . . .	603
Vulnerabilidades . . . . .	605
Distribuciones PGP. . . . .	605
Sistemas de detección de intrusos. . . . .	607
Introducción . . . . .	607
Funcionamiento de IDS . . . . .	607
Características de un IDS . . . . .	610
Problemas asociados a IDS. . . . .	612
Ejemplos de IDS . . . . .	614
Referencias. . . . .	617
<b>CAPÍTULO 11</b>	
<b>Seguridad en redes . . . . .</b>	<b>619</b>
Leobardo Hernández Audelo	
Enrique Daltabuit Godás	
Introducción. . . . .	619
Internet. . . . .	620
Modelo ISO-OSI del funcionamiento de redes . . . . .	622
Redes locales . . . . .	623
Redes amplias . . . . .	624
Protocolos de encaminamiento . . . . .	626
Intranets . . . . .	627
Cortafuegos . . . . .	628
Decisiones de diseño . . . . .	630
Preocupaciones y problemas con cortafuegos. . . . .	631
Tipos de cortafuegos. . . . .	633
Utilización de compuertas . . . . .	637
Cortafuegos tipo compuerta de doble domicilio . . . . .	642
Integración de módems con cortafuegos . . . . .	646
Requerimientos y configuración de cortafuegos . . . . .	647
Administración de identidades . . . . .	650
TCP/IP: el lenguaje de Internet . . . . .	658
TCP (Transfer Control Protocol) . . . . .	663

UDP (User Datagram Protocol) . . . . .	664
ICMP (Internet Control Message Protocol) . . . . .	664
<b>Estructura de puertos TCP y UDP . . . . .</b>	<b>665</b>
El súper servidor de Internet . . . . .	665
Amenazas a la seguridad en redes de computadoras. . . . .	668
Denegación de servicio (interrupción) . . . . .	669
Suplantación (Spoofing o fabricación) . . . . .	670
Espionaje (monitoreo o interceptación). . . . .	670
Modificación . . . . .	670
Análisis de tráfico . . . . .	671
Canales secretos . . . . .	671
<b>Precauciones elementales. . . . .</b>	<b>671</b>
Niveles de seguridad . . . . .	671
Conocer al enemigo . . . . .	673
Identificar las hipótesis . . . . .	673
Controlar los secretos . . . . .	674
Recordar el factor humano. . . . .	674
Conocer las debilidades. . . . .	675
Limitar el alcance de los accesos . . . . .	675
Entender el ambiente . . . . .	675
Limitar la confianza . . . . .	675
Recordar la seguridad física . . . . .	676
Vigilar los cambios . . . . .	676
<b>Servicios de seguridad en redes . . . . .</b>	<b>676</b>
Confidencialidad . . . . .	677
Integridad. . . . .	679
Autenticación y no repudio . . . . .	680
Disponibilidad . . . . .	681
<b>Seguridad de los enlaces . . . . .</b>	<b>681</b>
Criptografía y seguridad en redes. . . . .	681
Confidencialidad . . . . .	681
Integridad . . . . .	682
Autenticación . . . . .	682
Control de acceso . . . . .	682
Cifrado de enlaces. . . . .	682

Cifrado de punta a punta . . . . .	684
SILS (Standard for Interoperability LAN Security) . . . . .	685
Retos de la criptografía en la seguridad en redes . . . . .	686
Seguridad en IP (IPsec) . . . . .	687
SSH (Secure SHell) . . . . .	700
Seguridad en Web . . . . .	705
Protección de los dispositivos de red . . . . .	719
Control de acceso a los dispositivos . . . . .	729
<b>Seguridad en cómputo móvil . . . . .</b>	<b>737</b>
<b>Redes inalámbricas . . . . .</b>	<b>741</b>
Conexiones Punto a Punto . . . . .	741
Espectro distribuido . . . . .	745
<b>Referencias . . . . .</b>	<b>759</b>
<b>Índice temático . . . . .</b>	<b>763</b>
<b>Autores . . . . .</b>	<b>773</b>