

Seguridad de la Información

Redes, informática
y sistemas de información

El presente libro permite conocer a fondo, de forma amena, desde la doble perspectiva teórica y práctica, los fundamentos y los aspectos más relevantes y apasionantes de la Seguridad de la Información.

La Seguridad de la Información abarca la protección tanto de los Sistemas de Información como de las Redes y de los Computadores. Se trata de un continuo desafío, ya que más que un problema tecnológico, constituye hoy en día un elemento clave que posibilita los negocios y permite que las organizaciones puedan llevar a cabo sus objetivos corporativos.

Aunque controlar y dominar los secretos de la Seguridad de la Información puede parecer reservado sólo a unos pocos, el objetivo de este libro es proporcionar un referente actual de las cuestiones clave desde la perspectiva teórica-práctica de este fascinante mundo. No sólo se busca la asimilación de la teoría a través de ejemplos sino que se implica al lector en una dinámica rica en actividades y retos, tanto cualitativos, cuantitativos como de representación gráfica.

Contenido

Prólogo

xv

1. Fundamentos de seguridad de la información	1
1.1. Importancia de la seguridad	2
1.1.1. Objetivos generales de la seguridad	2
1.1.2. Entidades implicadas en la seguridad	4
1.1.3. Fases en el ciclo de vida de seguridad de un sistema de información	5
1.1.4. Actividades en el ciclo de vida de seguridad de un sistema de información	6
1.2. Áreas de proceso de la seguridad	7
1.2.1. Riesgos	7
1.2.2. Ingeniería	8
1.2.3. Aseguramiento	9
1.2.4. Factores que motivan cambios en la seguridad	10
1.3. Servicios de seguridad	11
1.4. Elementos de gestión de la seguridad de los sistemas de información	21
1.4.1. Identificación de todos los activos del sistema	21
1.4.2. Identificación de amenazas a los activos	22
1.4.3. Identificación de vulnerabilidades	23
1.4.4. Identificación de impactos	23
1.4.5. Identificación de riesgos	24
1.4.6. Identificación de riesgos residuales	24
1.4.7. Aplicación de salvaguardas	24
1.4.8. Identificación de las limitaciones de aplicación de la seguridad	25
1.5. Estándar de seguridad ISO-7498-2	25
1.5.1. Aspectos del ciclo de vida de la seguridad	25
1.5.2. Identificación de requisitos de seguridad	27
1.5.3. Tipos genéricos de amenazas según el estándar ISO 7498-2	27
1.5.4. Clasificación de las amenazas	28
1.5.5. Políticas de seguridad genéricas	29
1.5.6. Categorías de servicios de seguridad ISO-7498-2	30
1.5.7. Mecanismos de seguridad ISO 7498-2	31
1.5.8. Categorías de mecanismos de seguridad generalizados	39
1.5.9. Relación entre servicios y mecanismos de seguridad ISO-7498-2 y entre los servicios de seguridad y las capas del modelo OSI	41
1.5.10. Categorías de gestión de la seguridad	42

1.6.	Métodos para desarrollar una política de seguridad	43
1.6.1.	Análisis y valoración de riesgos	43
1.6.2.	Construcción de la política de seguridad	46
1.6.3.	Implantación de la política de seguridad	47
1.6.4.	Mantenimiento de la política de seguridad	47
1.6.5.	Implicación del componente humano	48
1.6.6.	Causas del fallo de las políticas de seguridad	48
2.	Análisis y gestión de riesgos de seguridad	53
2.1.	Análisis de riesgos de seguridad	54
2.1.1.	Razones para realizar el análisis de riesgos	54
2.1.2.	Tipos de análisis de riesgos	55
2.1.3.	Clases de riesgos	58
2.1.4.	Argumentos en contra del análisis de riesgos	59
2.1.5.	Fases del análisis de riesgos	60
2.1.6.	Técnicas alternativas de análisis de riesgos	61
2.2.	Identificación de recursos	62
2.2.1.	Recursos amenazados: tangibles e intangibles	62
2.2.2.	Activos	62
2.2.3.	Amenazas asociadas a los activos	63
2.2.4.	Factores de valoración de activos	64
2.3.	Explotación de amenazas	65
2.3.1.	Factores para la estimación de la probabilidad de explotación	68
2.4.	Medidas de protección	69
2.4.1.	Evaluación de daños	69
2.4.2.	Evaluación de riesgos en base a su importancia y a la probabilidad de que se produzca un ataque	70
2.4.3.	Análisis de costes y beneficios	70
2.4.4.	Tipos de medidas, controles y servicios de seguridad	71
2.5.	Cuestionarios de referencia en las entrevistas con los clientes	72
2.5.1.	Cuestionario para definir los activos más críticos	73
2.5.2.	Cuestionario para establecer las medidas más adecuadas	73
2.6.	Plan director de seguridad	73
2.6.1.	Elementos de un plan director de seguridad	73
2.6.2.	Aspectos que debe establecer un plan director de seguridad	74
2.7.	Gestión de riesgos de seguridad de la información	74
2.7.1.	Variables que intervienen en la gestión de riesgos	76
2.7.2.	Situaciones adversas en seguridad y elementos de riesgo	77
2.7.3.	Mecanismos para el control de riesgos	78
2.7.4.	Aspectos para construir un proceso de gestión de riesgos	79
2.8.	Identificación y cualificación de los riesgos de seguridad de la información	80
2.8.1.	Criterios de vulnerabilidad	80
2.8.2.	Criterios de impacto y uniformidad de amenazas	81
2.9.	Fases del proceso de gestión y reducción de riesgos de seguridad	82
2.9.1.	Fase 1. Identificación de los elementos y componentes del sistema	82
2.9.2.	Fase 2. Definición del ámbito y frontera del problema	82

2.9.3.	Fase 3. Identificación de los subsistemas y componentes en la frontera establecida	83
2.9.4.	Fase 4. Determinación de un cualificador de criticidad	83
2.9.5.	Fase 5. Identificación de las vulnerabilidades conocidas de cada sub-nivel de la fase-3	83
2.9.6.	Fase 6. Identificación de los controles de compensación, mecanismos, políticas y procesos existentes	84
2.9.7.	Fase 7. Cualificación de las vulnerabilidades en base a los controles de compensación existentes	84
2.9.8.	Fase 8. Completado de la matriz de cualificación del riesgo	84
2.9.9.	Fase 9. Proceso de reducción del riesgo	84
2.10.	Formulación cuantitativa de los riesgos de seguridad	85
2.10.1.	Determinación cuantitativa del riesgo	85
2.10.2.	Estructuración de la toma de decisiones basada en riesgos	85
2.11.	Gestión de la seguridad basada en riesgos	86
2.11.1.	Fases de la toma de decisiones de seguridad basada en riesgos	86
2.12.	Estándar ISO/IEC-27002 o ISO/IEC-17799 de gestión de la seguridad	89
2.12.1.	Objetivos de control según el estándar ISO-17799	90
2.12.2.	Gestión de la seguridad según el estándar ISO-17799	92
2.12.3.	Panel de indicadores para la gestión de la seguridad según el estándar ISO-17799	95
2.13.	Fases para la determinación del ROI o del ROSI	99
2.13.1.	Cálculo del EF, SLE, ARO y ALE	99
2.13.2.	Cálculo del ALE, mALE , ahorro y ROSI básico y útil	100
3.	Control de acceso: autenticación, autorización y cumplimiento	107
3.1.	Control de acceso	108
3.1.1.	Elementos del control de acceso	109
3.1.2.	Tipos de necesidades de seguridad	109
3.1.3.	Niveles de seguridad	110
3.2.	Control de acceso y modelos de seguridad	115
3.2.1.	Objetivos del control de acceso	116
3.2.2.	Mecanismo de perfiles	117
3.2.3.	Factores de los que depende el control de acceso	118
3.2.4.	Mecanismos de control de acceso	118
3.3.	Operaciones de acceso	119
3.3.1.	Matriz de control de acceso	119
3.3.2.	Principales técnicas de agregación	120
3.3.3.	Control de acceso basado en roles (RBAC)	121
3.3.4.	Operaciones de acceso Unix	122
3.4.	Los cuatro enfoques de la seguridad de un sistema de información	123
3.5.	Componentes del control de acceso	125
3.5.1.	Elementos de implantación de un control de acceso	125
3.6.	Políticas de control de acceso	126
3.6.1.	Categorías de políticas de control de acceso	128
3.7.	Mecanismo de capacidades	129

3.7.1.	Operaciones con capacidades	129
3.7.2.	Características de un esquema de capacidades	130
3.8.	Mecanismo de listas de control de acceso (ACL)	130
3.8.1.	Obtención de las ACL	131
3.8.2.	Dos formas de utilización de los caracteres comodín en ACL	131
3.9.	Control de acceso sobre ficheros FTAM	132
3.9.1.	Campos de la declaración	132
3.10.	Transferencias de control de acceso	133
3.11.	Gestión de la información de control de acceso	134
3.11.1.	Permisos de control	134
3.11.2.	Certificado de atributos de privilegios	135
3.11.3.	Casos de revocación de la información de control de acceso	135
3.12.	Controles de acceso para las comunicaciones de red	136
3.12.1.	Control de encaminamiento en los niveles de red y aplicación	136
3.12.2.	Formas de especificar la calidad de servicio de protección	138
3.13.	El estándar de seguridad ISO/IEC10181	138
3.13.1.	Aspectos cubiertos por el estándar	139
3.13.2.	Entidades, tipos de información y configuraciones de autenticación según el estándar ISO/IEC-10181-2	139
3.13.3.	Objetivos primarios y secundarios del control de acceso según el ISO-10181-3	140
3.14.	Sistema de autenticación Kerberos	148
3.14.1.	Tipos de servidores en Kerberos	148
3.14.2.	Funcionamiento de Kerberos	149
3.14.3.	Productos donde se utiliza Kerberos	150
3.15.	Protocolos de seguridad de red AAA	151
3.15.1.	Funcionalidades de RADIUS	152
3.15.2.	Criterios de evaluación de protocolos AAA	153
4.	Análisis de ataques a los sistemas de información	161
4.1.	Ataques a través de Internet	162
4.1.1.	Falta de información en relación a los ataques	162
4.1.2.	Razones para considerar la amenaza de los ataques	162
4.2.	Descripción de técnicas DoS	164
4.2.1.	Ataques genéricos de inundación o <i>flood</i>	167
4.2.2.	Ataques <i>smurf</i>	170
4.2.3.	Ataques <i>nuke</i>	171
4.2.4.	Ataques DDoS (<i>Distributed Denial of Services</i>)	171
4.3.	Técnica de los árboles de ataque	171
4.3.1.	Formas de descomponer un nodo de un árbol	172
4.3.2.	Refinamiento de ataques: propiedad de transparencia referencial	172
4.3.3.	Construcción de árboles de ataque: <i>login shell, etc/passwd</i>	173
4.3.4.	Componentes de la descripción informal de un ataque	175
4.4.	Determinación cuantitativa del riesgo en un árbol de ataque	176
4.4.1.	Método para valorar riesgos	176
4.4.2.	Patrones de ataque	177

4.5.	Árbol de ataque de alto nivel	179
4.5.1.	Análisis de las ramas del árbol de ataque	180
4.5.2.	Refinamiento del árbol de ataque	181
4.6.	Modelos de ataques	182
4.6.1.	Áreas de defensa de los mecanismos de control de riesgo	183
4.6.2.	Alertas de seguridad	184
4.7.	Denegación de servicios de red	186
4.7.1.	Amenazas de comportamiento anómalo de <i>routers</i>	186
4.7.2.	Mecanismos de prevención de ataques DoS	186
4.7.3.	Tecnología de encaminamiento	189
4.8.	Defensa contra ataques DoS en redes: técnica del <i>hop integrity</i>	192
5.	Sistemas de gestión de seguridad de la información. Métricas, cuadros de mando y criterios de evaluación	199
5.1.	Sistema de gestión de seguridad de la información	200
5.2.	Métricas de seguridad de la información	201
5.2.1.	Recogida de datos de métricas de seguridad	203
5.2.2.	Factores que influyen en el éxito de un plan de métricas de seguridad de un sistema de información	204
5.2.3.	Enfoques para métricas de seguridad	207
5.2.4.	Parámetros que intervienen en la definición de métricas de seguridad	211
5.2.5.	Factores de evolución de las métricas de seguridad	211
5.2.6.	Etapas del desarrollo de métricas de seguridad	212
5.2.7.	Detalles a identificar en una métrica de seguridad	213
5.3.	Clasificación de las métricas de seguridad	214
5.3.1.	Métricas genéricas	214
5.3.2.	Métricas para la seguridad organizacional	215
5.3.3.	Métricas de seguridad de los objetivos técnicos	218
5.3.4.	Métricas de seguridad de los objetivos de seguridad	219
5.3.5.	Métricas de seguridad de los controles aplicados al sistema de información	219
5.3.6.	Métricas de seguridad del factor tiempo de aplicación del control	220
5.3.7.	Métricas de seguridad según el tipo de público al que van dirigidas	220
5.4.	Cuadros de mando de seguridad. Buen gobierno de la seguridad	221
5.4.1.	Funciones de los cuadros de mando de seguridad	222
5.4.2.	Niveles de un cuadro de mando	223
5.4.3.	Métricas de seguridad de los cuadros de mando	224
5.4.4.	Cuadros de mando y aportaciones de la seguridad al valor del negocio	225
5.5.	Modelo de madurez de capacidades para la seguridad	226
5.5.1.	Dimensiones del modelo de madurez: dominio y capacidad	228
5.5.2.	Niveles de madurez de un plan de seguridad	229
5.5.3.	Clasificación de los objetivos de madurez	231
5.5.4.	Áreas de proceso en cada nivel de madurez	231
5.5.5.	Métricas para el modelo de madurez	232
5.5.6.	Prácticas de base y áreas de proceso del modelo de madurez	232
5.5.7.	Prácticas genéricas del modelo de madurez	234

5.5.8.	Características comunes de los modelos de madurez	235
5.5.9.	Escala de niveles de capacidades de un modelo de madurez	236
5.6.	Criterios de evaluación para medir la seguridad. Estándares	236
5.6.1.	Estándar TCSEC	237
5.6.2.	Estándar ITSEC/ITSEM	242
5.6.3.	Comparativa del ITSEC frente al TCSEC	245
5.6.4.	Criterios comunes CC ISO/IEC 15408	248
6.	Planificación de contingencias y continuidad de negocios	255
6.1.	Procesos de gestión del riesgo y planificación de contingencias	256
6.1.1.	Factores de atenuación de contingencias	256
6.2.	Categorías de planes de contingencias	259
6.2.1.	Plan de continuidad de negocios o BCP (<i>Business Continuity Plan</i>)	260
6.2.2.	Plan de recuperación de negocios o plan de reanudación de negocios o BRP (<i>Business Recovery Plan</i>)	260
6.2.3.	Plan de continuidad de las operaciones o COOP (<i>Continuity Of Operations Plan</i>)	260
6.2.4.	Plan de contingencias de TIC o plan de continuidad del soporte o SCP (<i>Support Continuity Plan</i>)	261
6.2.5.	Plan de comunicación de crisis o CCP (<i>Crisis Communication Plan</i>)	262
6.2.6.	Plan de respuesta a ciberincidentes o CRP (<i>Cyber-Incidents Response Plan</i>)	262
6.2.7.	Plan de recuperación de desastres o DRP (<i>Disaster Recovery Plan</i>)	262
6.2.8.	Plan de emergencia de ocupantes u OEP (<i>Occupant Emergency Plan</i>)	262
6.2.9.	Plan de gestión de eventos de crisis o C/EM (<i>Crisis Event Management</i>)	263
6.3.	Estrategias de contingencias en el ciclo de vida del desarrollo de un sistema TIC	263
6.4.	Contingencias en sitios web	266
6.4.1.	Medidas de contingencia en sitios web	266
6.4.2.	Clases de balanceo de carga en web	268
6.4.3.	Técnicas de copias de seguridad (<i>backup</i>)	270
6.4.4.	Estrategias SAN, NAS e iSCSI	270
6.5.	Estrategia multidimensional para mejorar la seguridad	271
6.5.1.	Dimensión de prevención	271
6.5.2.	Dimensión de detección	273
6.5.3.	Dimensión forense	273
6.5.4.	Dimensión de respuesta	274
6.6.	Continuidad de los negocios	274
6.6.1.	Continuidad de negocios de comercio electrónico	276
6.7.	Especificación de la confianza	277
7.	Cumplimiento con las leyes. Privacidad y anonimato. Servicios de investigación y responsabilidad	285
7.1.	Reglamento de medidas de seguridad (RMS-LOPD)	286
7.1.1.	Ficheros automatizados y datos sensibles en papel	288

7.2.	Niveles de seguridad definidos en el RMS según el tipo de datos	288
7.2.1.	Medidas técnicas y organizativas a adoptar según nivel de seguridad definidas en el RMS	289
7.3.	LSSI-CE	293
7.4.	Anonimato de las comunicaciones electrónicas. <i>Cookies</i>	294
7.4.1.	Tecnologías de anonimato de comunicaciones	294
7.4.2.	Privacidad del usuario. <i>Cookies</i>	299
7.5.	Servicio de investigación: <i>computer forensic</i>	303
7.5.1.	Elementos que se buscan mediante <i>computer forensic</i>	306
7.5.2.	Incidentes tratados por <i>computer forensic</i>	307
7.5.3.	Investigación de ataques que han tenido éxito	309
7.6.	Evidencias en <i>computer forensic</i>	310
7.6.1.	Fases de la investigación en análisis forense	310
7.6.2.	Proceso de recogida de evidencias en <i>computer forensic</i>	311
7.6.3.	Dificultades que aparecen en <i>computer forensic</i>	312
7.6.4.	Recogida de evidencias en una red corporativa	312
7.7.	Principios legales y técnicos en <i>computer forensic</i>	316
7.8.	Servicio de responsabilidad: auditoría de seguridad	317
7.8.1.	Funciones de auditoría de seguridad	317
7.8.2.	Información registrada en cada evento	319
7.8.3.	Recogida de información de auditoría	319
7.8.4.	Clasificación de requisitos de auditoría en TCSEC	320
7.8.5.	Almacenamiento de registros de auditoría	321
7.8.6.	Saturación en el proceso de recogida de datos de auditoría	322
7.8.7.	Monitorización y reconocimiento de amenazas	323
8.	Tecnologías de seguridad	327
8.1.	Tecnología de cortafuegos (<i>firewall</i>)	328
8.1.1.	Clasificación de los cortafuegos	331
8.1.2.	Funciones de los cortafuegos	335
8.1.3.	Configuración de los cortafuegos	337
8.1.4.	Limitaciones de los cortafuegos	338
8.1.5.	Formas de eludir a los cortafuegos	339
8.1.6.	Autenticación en los cortafuegos	340
8.1.7.	Arquitectura de los cortafuegos según el nivel de riesgo de seguridad	341
8.1.8.	Gestión de un cortafuegos	342
8.1.9.	Amenazas a los cortafuegos	342
8.2.	Sistemas de detección y prevención de intrusiones (IDS-IPS)	345
8.2.1.	Arquitecturas fundamentales de detección de intrusiones	350
8.2.2.	Componentes de los IDS	356
8.2.3.	Tipos de IDS según su forma de reaccionar	356
8.2.4.	Tipos de IDS según su composición interna	357
8.2.5.	Limitaciones, problemas y soluciones de los sistemas de detección de intrusiones de red	357
8.2.6.	Componentes de un sistema de detección y respuesta a intrusiones	360
8.2.7.	Consortio IDSC . Formato IDMEF del IETF	360

8.3.	Tecnología de <i>honeypots</i>	361
8.3.1.	Niveles de implicación de un <i>honeypot</i>	362
8.3.2.	Localizaciones de un <i>honeypot</i>	365
8.3.3.	Riesgos por el uso de <i>honeypots</i>	367
8.4.	Tecnología PKI . Infraestructuras de clave pública para la emisión de certificados digitales	368
8.4.1.	Componentes de una PKI	370
8.4.2.	Ventajas e inconvenientes del uso las PKI	371
8.4.3.	Configuraciones de las PKI	371
8.4.4.	Autoridades de certificación puente	376
8.4.5.	Utilización de los directorios LDAP en las PKI	379
8.4.6.	Arquitecturas de conexión entre autoridades de certificación basadas en PKI	379
8.5.	Sistema IBC basado en identidad: IBE y <i>pairing</i>	380
8.5.1.	Fases de los sistemas IBC	381
8.5.2.	Limitaciones de la firma en sistemas IBC	381
8.5.3.	Mecánica de funcionamiento del IBE	382
8.5.4.	PKG	383
8.6.	Solución a la problemática del repudio	384
8.6.1.	Fases del no repudio	384
8.6.2.	Servicio de no repudio del emisor	386
8.6.3.	Servicio de no repudio de entrega	388
9.	Análisis y síntesis de funcionalidades criptográficas simétricas	395
9.1.	Introducción	396
9.1.1.	Evolución histórica de la Criptografía	396
9.1.2.	Herramientas criptográficas	401
9.1.3.	Tipos de cifradores	402
9.1.4.	Secreto y autenticidad	402
9.1.5.	Tipos de seguridad de los criptosistemas	403
9.1.6.	Razones para la no ocultación del diseño de un criptosistema	403
9.1.7.	Requisitos de Kerckhoff	404
9.1.8.	Esteganografía y esteganografía	404
9.2.	Criptoanálisis	408
9.2.1.	Campos de investigación utilizados en el criptoanálisis	409
9.2.2.	Tipos de ataques a un criptosistema mediante criptoanálisis	410
9.3.	Técnicas criptográficas básicas de cifrado	412
9.3.1.	Sustitución	412
9.3.2.	Cifradores de transposición o permutación	413
9.3.3.	Cifradores de producto. Cajas <i>P</i> directas, expandidas y comprimidas. Cajas <i>S</i>	415
9.4.	Criptosistemas simétricos de tipo cifradores por sustitución monoalfabéticos	416
9.4.1.	Cifradores con desplazamiento puro	419
9.4.2.	Cifradores con decimación pura	420
9.4.3.	Cifradores afines o de sustitución afín	420
9.4.4.	Cifradores afines generalizados o mixtos	423

9.4.5.	Criptanálisis de cifradores simétricos de sustitución monoalfabética	423
9.5.	Criptosistemas simétricos de sustitución polialfabética	425
9.5.1.	Cifrador de Beaufort	425
9.5.2.	Cifrador de Vigenère	426
9.5.3.	Método de Kasiski para determinar la longitud de una clave de un criptosistema simétrico polialfabético	427
9.5.4.	Cifradores de flujo, Vernam y de bloque	427
9.6.	Cifrador de sustitución poligráfica tipo Hill	428
9.6.1.	Requisitos de la matriz de la clave	431
9.6.2.	Cifrador tipo Hill afín	433
9.6.3.	Ataque a cifradores tipo Hill	434
9.6.4.	Cifrador tipo <i>PlayFair</i> basado en digramas	434
9.6.5.	Cifrador tipo ADFGVX	436
9.7.	Diseño de un criptosistema simétrico	438
9.7.1.	Funcionamiento de los procesos de cifrado y descifrado	438
9.7.2.	Criptanálisis basado en texto en claro elegido	439
9.7.3.	Criptanálisis basado en texto en claro conocido	440
9.8.	Criptosistema simétrico basado en dos PRNG	441
9.8.1.	Secuencia del generador PRNG ₁	442
9.8.2.	Secuencia del generador PRNG ₂	443
9.9.	Generadores de números aleatorios	445
9.9.1.	Generadores de números pseudoaleatorios (PRNG)	445
9.9.2.	Postulados de aleatoriedad de Golomb	446
9.9.3.	Requisitos de los generadores de claves	451
9.9.4.	Consideraciones sobre números aleatorios y pseudoaleatorios	453
9.9.5.	Bloques de construcción de PRNG	455
9.10.	Gestión de claves criptográficas ISO/IEC 11770	459
9.10.1.	Mecanismos de establecimiento de clave utilizando Criptografía simétrica	460
9.10.2.	Mecanismos de establecimiento de clave utilizando Criptografía asimétrica	462
10.	Análisis y síntesis de funcionalidades criptográficas asimétricas	471
10.1.	Introducción	472
10.2.	Herramientas matemáticas en criptografía	474
10.2.1.	Algoritmo EA para valores enteros	474
10.2.2.	Algoritmo EEA para valores enteros	474
10.2.3.	Algoritmo EEA para polinomios	477
10.2.4.	Teorema del resto chino (CRT). Algoritmo de Gauss	479
10.3.	Criptosistema asimétrico basado en mochilas estilo M-H (Merkle-Hellman)	481
10.3.1.	Criptograma y descifrado del texto en claro con mochilas.	484
10.4.	Criptosistema estilo D-H (Diffie-Hellman)	487
10.4.1.	Criptosistema estilo D-H (Diffie-Hellman) clásico sobre el conjunto de números enteros Z_p	487
10.4.2.	Criptosistema estilo D-H basado en funciones de traza sobre un campo de Galois de característica tres GF (2 ³)	488

10.4.3. Criptosistema D-H basado en la utilización de polinomios de Chebyshev	489
10.5. Criptosistema asimétrico estilo RSA (Rivest–Shamir–Adleman)	491
10.5.1. Variantes del criptosistema estilo RSA	494
10.6. Criptosistema asimétrico estilo E-G (El-Gamal)	496
10.6.1. Criptosistema estilo E-G generalizado sobre un campo finito $\mathbf{GF}(2^m)$	497
10.7. Criptosistema probabilístico asimétrico estilo Rabin	500
10.7.1. Criptosistema estilo Rabin con clave escalar unicomponente	503
10.7.2. Criptosistema estilo Rabin con clave pública de dos componentes (N , B)	504
10.8. Protocolos de conocimiento nulo (ZK)	508
10.8.1. Protocolo criptográfico ZK estilo FFS (Feige-Fiat-Shamir)	510
10.8.2. Esquema de identificación ZK estilo GQ	512
10.8.3. Protocolo criptográfico ZK estilo Schnorr	513
10.9. Criptosistema asimétrico o de clave pública basado en tres tablas	515
10.10. Funciones criptográficas unidireccionales <i>hash</i>	516
10.10.1. Criptoanálisis de funciones <i>hash</i> no seguras	518
10.10.2. Síntesis de una función <i>hash</i> a partir de un algoritmo de cifrado asimétrico como el RSA	518
10.11. Firmas electrónicas o digitales	519
10.12. Seguridad semántica. Criptosistemas asimétricos estilo Paillier	522
10.13. Otros protocolos criptográficos	524
10.13.1. Protocolo del lanzamiento de monedas a ciegas a través de Internet	526
10.14. Compartición de secretos	527
10.14.1. Esquema estilo Shamir para el reparto de secretos	529
10.14.2. Esquema de reparto o compartición de secretos con dispersión de información	531
10.14.3. Compartición de secretos verificable	533
10.15. Números pseudoaleatorios en criptografía	534
10.15.1. Postulados de Golomb	536
10.16. Criptografía asimétrica basada en curvas elípticas (ECC)	538
10.16.1. Criptosistema asimétrico D-H basado en ECC	538
10.16.2. Criptosistema asimétrico de cifrado y descifrado basado en curvas elípticas sobre $\mathbf{GF}(p)$	541
10.16.3. Síntesis de un criptosistema estilo E-G basado en curvas elípticas	543
10.16.4. Operaciones sobre curvas elípticas	544
10.16.5. Comparación de ECC con otros criptosistemas asimétricos. Aspectos de estandarización	549
10.16.6. PRNG basados en ECC	550

Bibliografía **555**

Índice terminológico **561**