

# Índice de contenido

<b>Introducción</b> .....	<b>xvii</b>
La importancia de la seguridad en Java .....	xviii
¿A quién va dirigido este libro? .....	xx
Cómo está organizado este libro .....	xx
Cómo empezar .....	xxii
Cómo utilizar este libro .....	xxiii
<b>Parte I Los fundamentos de la seguridad en Java</b> .....	<b>1</b>
<b>Capítulo 1. Fundamentos de la seguridad</b> .....	<b>3</b>
El modelo básico de seguridad .....	5
Criptografía .....	7
Clases de criptografía .....	7
Boletines de mensajes .....	9
Claves simétricas .....	10
Claves asimétricas .....	10
Autenticación y no repudiación .....	11
Tipos de autenticación .....	12
No repudiación .....	15
Control de acceso .....	16
Control de acceso discrecional .....	16
Control de acceso basado en funciones .....	17
Control de acceso obligatorio .....	17
Control de acceso de cortafuegos .....	17
Dominios .....	18
Auditoría .....	18
Normas y administración .....	19
Resumen .....	20
<b>Capítulo 2. Panorámica de la seguridad en Java</b> .....	<b>21</b>
Los antecedentes de la seguridad en Java .....	23
La arquitectura de seguridad de Java .....	25
La arquitectura de seguridad nuclear de Java 2 .....	26
La arquitectura de la criptografía en Java .....	28
La extensión de la criptografía en Java .....	29
La extensión de <i>sockets</i> en Java .....	29
La autenticación y el servicio de autorización en Java .....	29

El verificador de código binario . . . . .	30
El cargador de clases . . . . .	31
La arquitectura y la seguridad del cargador de clases . . . . .	32
Las interfaces del cargador de clases . . . . .	32
El administrador de seguridad . . . . .	36
Las interfaces del administrador de seguridad . . . . .	37
Los administradores de seguridad personalizados . . . . .	39
La arquitectura de criptografía de Java . . . . .	40
La arquitectura de JCA . . . . .	41
Los motores criptográficos . . . . .	43
Los proveedores de servicios criptográficos . . . . .	43
Resumen . . . . .	45
<b>Capítulo 3. Control de acceso a la seguridad de las aplicaciones</b>	
<b>Java . . . . .</b>	<b>47</b>
Permisos . . . . .	49
La arquitectura de los permisos . . . . .	49
Tipos de permisos . . . . .	50
Tipos de permisos personalizados . . . . .	58
Normas de seguridad . . . . .	59
El formato del archivo de normas de seguridad . . . . .	59
Cómo hacer referencia a las propiedades en los archivos de normas . . . . .	61
Cómo utilizar los archivos de normas de seguridad . . . . .	61
La herramienta de normas de seguridad . . . . .	62
API de normas de seguridad . . . . .	63
Control de acceso en Java . . . . .	64
La arquitectura del control de acceso . . . . .	65
Objetos protegidos . . . . .	67
Asignación de control para acceder a Security/Manager . . . . .	68
Ejemplo de control de acceso configurable . . . . .	72
Resumen . . . . .	74
<b>Capítulo 4. Seguridad de los applets . . . . .</b>	<b>75</b>
Cómo ampliar el <i>sandbox</i> . . . . .	77
El <i>sandbox</i> de JDK 1.0 . . . . .	78
El <i>sandbox</i> de JDK 1.1 . . . . .	80
Privilegio menor de JDK 1.2 . . . . .	81
Cómo especificar unas normas de seguridad para los <i>applets</i> . . . . .	81
El contenido del archivo de normas de seguridad . . . . .	82
La sintaxis de las entradas garantizadas . . . . .	83
Uso de <i>applets</i> firmados . . . . .	84
Cómo crear el archivo JAR . . . . .	84
Cómo firmar el archivo JAR . . . . .	85
Cómo especificar unas normas de <i>applets</i> firmados . . . . .	86

Cómo obtener un certificado de firma .....	86
Cómo trabajar con distintos navegadores .....	87
Resumen .....	87
<b>Parte II Seguridad criptográfica .....</b>	<b>89</b>
<b>Capítulo 5. Introducción a la criptografía .....</b>	<b>91</b>
Una breve historia de la escritura secreta .....	93
Criptografía, criptoanálisis y criptología .....	96
Cifras .....	97
La cifra de César .....	97
Una cifra de sustitución sencilla .....	103
Criptografía de clave secreta .....	117
El Estándar de Encriptación de Datos (DES) .....	118
Un ejemplo de DES .....	131
DESede .....	135
Blowfish .....	136
Cifras de Rivest .....	140
Criptografía de clave pública .....	141
El algoritmo de Rives, Shamir, Adleman (RSA) .....	141
El algoritmo ElGamal .....	145
Boletines de mensajes .....	146
MD5 .....	148
SHA-1 .....	150
Codificación Base 64 .....	152
Firmas digitales .....	160
El algoritmo de Firma Digital .....	161
Certificados digitales .....	163
Resumen .....	164
<b>Capítulo 6. Administración de claves y certificados digitales .....</b>	<b>167</b>
Importancia de la administración de claves .....	169
Representación de claves .....	170
Generación de claves .....	172
La clase KeyPairGenerator .....	173
La clase KeyGenerator .....	174
El programa KeyGeneratorApp .....	175
Números aleatorios seguros y generación de claves .....	178
Traducción de claves .....	181
Acuerdo sobre claves .....	184
Administración de claves sencilla para los Protocolos de Internet (SKIP) .....	186
Soporte de JCE del acuerdo sobre claves .....	187
El almacenamiento de claves y la encriptación basada en contraseña ...	193

Diferencias en la administración de claves entre JDK 1.1 y la Plataforma Java 2 (versión JDK 1.2) .....	204
Administración de claves JDK 1.1 .....	204
Administración de claves en JDK 1.2 .....	206
keytool .....	209
Resumen .....	212
<b>Capítulo 7. Boletines de mensajes y firmas digitales .....</b>	<b>213</b>
Clases e interfaces de boletines de mensajes .....	215
MessageDigestSpi .....	215
MessageDigest .....	216
DigestInputStream y DigestOutputStream .....	219
Cómo trabajar con flujos de boletín .....	221
DigestException .....	222
Códigos de autenticación de mensajes .....	223
MacSpi .....	224
Mac .....	225
Los MAC en acción .....	226
Clases e interfaces de firma .....	227
SignatureSpi .....	227
Signature .....	228
SignedObject .....	232
Signer .....	235
SignatureException .....	235
Resumen .....	235
<b>Capítulo 8. La Extensión de Criptografía de Java .....</b>	<b>237</b>
El interior de la JCE .....	239
La JCE de Cryptix .....	241
Proveedores de seguridad e independencia de los algoritmos .....	242
Cómo se organiza un proveedor de seguridad .....	242
Clases de motor .....	243
Clases de SPI .....	243
Clases de proveedor .....	243
Cómo crear un proveedor nuevo .....	244
Cómo ampliar la clase SPI .....	244
Cómo ampliar la clase de proveedor .....	247
Cómo instalar las clases de proveedor .....	248
Cómo usar el proveedor .....	249
Resumen .....	250
<b>Capítulo 9. SSL y JSSE .....</b>	<b>251</b>
Panorámica de SSL .....	253
Panorámica de la Extensión de <i>Socket</i> Seguro de Java .....	255

Panorámica de las clases y paquetes JSSE .....	256
Proveedores JSSE .....	258
<i>Sockets</i> de servidor SSL y JSSE .....	258
Cómo obtener una factoría de <i>sockets</i> de servidor SSL .....	259
Cómo crear <i>sockets</i> de servidor SSL .....	262
La audición del <i>socket</i> de servidor SSL .....	263
Autenticación de clientes .....	265
<i>Sockets</i> de cliente SSL y JSSE .....	266
Cómo obtener una factoría de <i>sockets</i> SSL .....	266
Cómo crear <i>sockets</i> de clientes SSL .....	267
Sesiones SSL de JSSE .....	268
Resumen .....	269

### Parte III Seguridad en los sistemas distribuidos ..... 271

#### Capítulo 10. Panorámica de la seguridad empresarial distribuida ... 273

Tecnología de sistemas empresariales distribuidos .....	275
Conectividad empresarial de bases de datos .....	276
Comunicaciones empresariales .....	277
Servicios de comunicación empresarial .....	278
Componentes empresariales basados en contenedores .....	280
Seguridad en la conectividad empresarial de bases de datos .....	281
Seguridad empresarial en las comunicaciones .....	281
Seguridad RMI .....	285
Seguridad en CORBA .....	286
Seguridad de servicios empresariales de comunicaciones .....	286
Seguridad en JNDI .....	286
Seguridad en Jini .....	288
Seguridad en JMS .....	289
Seguridad en JavaMail .....	290
Seguridad de componentes empresariales basados en contenedores ...	291
Seguridad en los componentes web .....	291
Seguridad en EJB .....	292
Resumen .....	293

#### Capítulo 11. Bases de datos y seguridad en las bases de datos ... 295

¿Qué es una base de datos? .....	297
Base de datos relacionales .....	298
Cómo trabajar con claves .....	298
Lenguaje Estructurado de Consulta (SQL) .....	298
Acceso remoto a bases de datos .....	299
Controladores ODBC y JDBC .....	299
Cómo conectarse a base de datos con el paquete <code>java.sql</code> .....	303
Cómo configurar una conexión de base de datos .....	304

Cómo ejecutar instrucciones SQL .....	306
El programa StatementApp .....	307
Temas de seguridad relativos a las bases de datos .....	312
Cómo proteger las conexiones de base de datos .....	313
Cómo proteger la conexión del usuario .....	322
Auditoría .....	327
Cómo escanear la base de datos .....	328
Resumen .....	328
<b>Capítulo 12. El Servicio de Autenticación y Autorización de Java ...</b>	<b>329</b>
Panorámica de JAAS .....	331
Sujetos JAAS .....	332
Relaciones de sujeto .....	333
Cómo crear sujetos .....	334
Cómo manipular los atributos de sujeto .....	335
Especialización de las credenciales de sujeto .....	337
Autenticación con JAAS .....	337
Configuración e inicialización de los módulos de conexión .....	337
El proceso de autenticación .....	342
Manipulación de retrollamadas .....	344
La autorización con JAAS .....	348
Formato de archivo de normas de seguridad de JAAS .....	349
Cómo usar los archivos de normas de seguridad de JAAS .....	350
Cómo llevar a cabo acciones vitales para la seguridad .....	351
Abstracciones de autorización de la seguridad en JAAS .....	352
Normas de seguridad estándar de Java con permisos de JAAS .....	355
Resumen .....	356
<b>Capítulo 13. Seguridad en CORBA .....</b>	<b>359</b>
Panorámica de la seguridad en CORBA .....	362
Paquetes de seguridad de CORBA .....	363
Arquitectura de la seguridad en CORBA .....	364
Interfaces de seguridad nucleares de CORBA .....	366
Autenticación .....	369
Delegación .....	374
Autorización .....	375
Auditoría .....	377
No repudiación .....	378
Encriptación .....	381
Normas de seguridad .....	384
Administración de la seguridad .....	386
Resumen .....	386
<b>Capítulo 14. Seguridad empresarial de los JavaBeans .....</b>	<b>389</b>
Panorámica de la seguridad EJB .....	391
Controles de acceso EJB programáticos estándar .....	392

Controles de acceso EJB declarativos estándar .....	396
Controles de acceso EJB específicos del fabricante .....	402
Identidad y autenticación EJB específica del fabricante .....	404
Comunicaciones, delegación y auditoría EJB seguras .....	408
Seguridad en la conexión EJB .....	408
Delegación de principales EJB .....	409
Auditoría de la seguridad EJB .....	409
Resumen .....	409
<b>Capítulo 15. JSP y la seguridad de los servlets Java .....</b>	<b>411</b>
La Interfaz de Pasarela Común .....	413
Comunicación de programas de servidor web a CGI .....	413
Mantenimiento del estado de la sesión .....	414
Cookies .....	415
Reescritura URL .....	415
Campos de formularios ocultos .....	416
Temas de seguridad en la programación del lado del servidor .....	416
Interceptación de la información sobre el estado de la sesión .....	416
Falsificación de la información sobre el estado de la sesión .....	417
Desbordamiento de <i>buffer</i> .....	417
Validación de datos .....	418
Secuencia de páginas .....	418
Interrupción de la sesión .....	419
Notificación de la información .....	419
Residuos de navegador .....	420
Autenticación del usuario .....	420
Conexión de información sensible .....	420
Privilegio menor .....	421
<i>Servlets Java</i> .....	421
¿Por qué los <i>servlets</i> ? .....	422
La API Servlet .....	422
Cómo funcionan los <i>servlets</i> .....	422
Ejemplos de <i>servlets</i> .....	437
Seguridad en los <i>servlets</i> .....	441
Páginas de JavaServer .....	448
Resumen .....	448
<b>Parte IV Apéndices .....</b>	<b>449</b>
<b>Apéndice A. Defectos pasados en la seguridad de Java .....</b>	<b>451</b>
JavaScript (febrero de 1996) .....	453
Ataque DNS (febrero de 1996) .....	453
Error en la implementación del cargador de clases (marzo de 1996) .....	454
Fallo en la implementación del verificador (marzo de 1996) .....	455