

Contenido

Agradecimientos	xvii
Introducción	xvii

PARTE I

Fundamentos de seguridad de la información

1 ¿Qué es la seguridad de la información?	3
Aptitud crítica 1.1 Defina que es seguridad de la información	4
Breve historia de la seguridad	5
Aptitud crítica 1.2 Defina la seguridad como proceso, sin sugerir productos	11
Software antivirus	12
Controles de acceso	12
Muros de fuego	12
Tarjetas inteligentes	13
Biométrica	13
Detección de intrusiones	14
Administración de políticas	14
Exploración de vulnerabilidades	15
Encriptación	15
Mecanismos de seguridad física	15
Proyecto 1 Examine las certificaciones de seguridad computacionales	15
Módulo 1 Preguntas de evaluación	16

2 Tipos de ataques	19
Aptitud crítica 2.1 Defina qué son los ataques de acceso.	20
Fisgoneo.	20
Escuchar furtivamente	21
Intercepción	22
Cómo se consuman los ataques de acceso.	22
Aptitud crítica 2.2 Defina qué son los ataques de modificación	26
Cambios	26
Inserción	26
Eliminación	26
Cómo se consuman los ataques de modificación.	27
Aptitud crítica 2.3 Defina qué son los ataques de denegación de servicio.	28
Denegación de acceso a la información.	28
Denegación de acceso a las aplicaciones.	28
Denegación de acceso a sistemas.	28
Denegación de acceso a comunicaciones	28
Cómo se consuman los ataques de denegación de servicio.	29
Aptitud crítica 2.4 Defina qué son los ataques de refutación	30
Simulación	30
Denegación de un evento.	31
Cómo se consuman los ataques de refutación	31
Proyecto 2 Examine sus vulnerabilidades	32
Módulo 2 Preguntas de evaluación	33
3 Técnicas de los hackers.	35
Aptitud crítica 3.1 Identificar las motivaciones de un hacker	36
Retos	36
Codicia	37
Propósito malintencionado	38
Aptitud crítica 3.2 Aprendizaje de las técnicas históricas de los hackers	38
Compartición abierta	39
Contraseñas deficientes	40
Fallas de programación	42
Ingeniería social.	42
Desbordamientos del búfer	44
Denegación de servicio	46
Aptitud crítica 3.3 Aprendizaje de técnicas avanzadas.	51
Rastreo de redes conmutadas.	51
Falseamiento de IP.	54
Aptitud crítica 3.4 Identificación de código malintencionado	57
Virus.	57
Caballos de Troya	58
Gusanos	58

Aptitud crítica 3.5 Identificación de los métodos de los hackers sin objetivos específicos	60
Objetivos	60
Reconocimiento	61
Métodos de ataque	63
Uso de sistemas comprometidos	64
Aptitud crítica 3.6 Identificación de los métodos de los hackers con objetivos específicos	69
Objetivos	69
Reconocimiento	69
Métodos de ataque	73
Uso de sistemas comprometidos	74
Proyecto 3 Realice el reconocimiento de su sitio	74
Módulo 3 Preguntas de evaluación	75
4 Servicios de seguridad de la información	77
Aptitud crítica 4.1 Defina confidencialidad	78
Confidencialidad de archivos	78
La confidencialidad de la información durante la transmisión	79
Confidencialidad del flujo de tráfico	80
Ataques que pueden ser evitados	81
Aptitud crítica 4.2 Defina integridad	82
Integridad de archivos	82
Integridad de la información durante la transmisión	83
Ataques que pueden ser evitados	83
Aptitud crítica 4.3 Defina disponibilidad	84
Respaldos	84
Recuperación de fallas (fail-over)	85
Recuperación de desastres	85
Ataques que pueden ser evitados	85
Aptitud crítica 4.4 Defina responsabilidad	85
Identificación y autenticación (validación)	86
Auditoría	87
Ataques que pueden ser evitados	87
Proyecto 4 Proteja su información	88
Módulo 4 Preguntas de evaluación	89

PARTE II

Trabajo preparatorio

5 Cuestiones legales en la seguridad de la información	93
Aptitud crítica 5.1 Comprenda el derecho penal de Estados Unidos de Norteamérica	94
Abuso y fraude por computadora (18 US Code 1030)	94
Fraude con tarjetas de crédito (18 US Code 1029)	95
Derechos de autor (18 US Code 2319)	95

Intercepción (18 US Code 2511)	96
Acceso a la información electrónica (18 US Code 2701)	96
Otros decretos penales	97
Ley Patriota	97
Ley de seguridad nacional	99
Aptitud crítica 5.2 Comprenda las leyes estatales	99
Aptitud crítica 5.3 Comprenda las leyes de otros países	100
Australia	100
Brasil	101
India	101
República Popular de China	101
Reino Unido	101
Aptitud crítica 5.4 Comprenda las cuestiones relacionadas con la acción judicial	102
Recopilación de evidencias	102
Establecer contacto con autoridades judiciales	103
Aptitud crítica 5.5 Comprenda las cuestiones civiles	104
Cuestiones laborales (de empleados)	104
Responsabilidad legal hacia abajo	105
Aptitud crítica 5.6 Comprenda las cuestiones de privacidad	106
Información del consumidor o cliente	106
Ley de responsabilidad y portabilidad de seguro médico	107
Componentes direccionables vs. requeridos	107
Requerimientos de la regla de seguridad	108
Ley de modernización de los servicios financieros de Graham-Leach-Bliley	110
Proyecto 5 Entable acción judicial contra el infractor	112
Módulo 5 Preguntas de evaluación	113
6 Políticas	115
Aptitud crítica 6.1 Comprenda por qué las políticas son importantes	116
Definición de lo que debería ser la seguridad	116
Incluir a todos en el mismo nivel	116
Aptitud crítica 6.2 Defina varias políticas	117
Políticas de información	117
Políticas de seguridad	119
Políticas de uso de las computadoras	123
Política del uso de Internet	124
Política de e-mail (correo electrónico)	125
Procedimientos de administración de usuarios	126
Procedimiento de administración del sistema	127
Política de respaldos	128
Procedimiento de respuesta a incidentes	129
Procedimiento de administración de la configuración	132
Metodología del diseño	133
Planes para la recuperación de desastres	134

Aptitud crítica 6.3 Cree una política apropiada	136
Definición de lo que es importante	136
Definición de un comportamiento aceptable	137
Identificación de las personas involucradas	137
Definición de los perfiles apropiados	137
Desarrollo de la política	137
Aptitud crítica 6.4 Política de despliegue	138
Ganar la aceptación	138
Educación	138
Implementación o instrumentación	139
Aptitud crítica 6.5 Utilice eficazmente la política	139
Nuevos sistemas y proyectos	139
Sistemas y proyectos existentes	139
Auditorías	139
Revisiones de la política	140
Proyecto 6 Desarrolle una política para el uso de Internet	140
Módulo 6 Preguntas de evaluación	141
7 Administración de riesgos	143
Aptitud crítica 7.1 Defina riesgo	144
Vulnerabilidad	144
Amenaza	145
Amenaza + Vulnerabilidad = Riesgo	149
Aptitud crítica 7.2 Identifique el riesgo para una organización	150
Identificación de las vulnerabilidades	151
Identificación de las amenazas reales	152
Comprobación de las contramedidas	152
Identificación del riesgo	153
Aptitud crítica 7.3 Evalúe el riesgo	154
Dinero	154
Tiempo	156
Recursos	156
Reputación	156
Negocios perdidos	157
Metodología para evaluación de riesgos	157
Proyecto 7 Identificación de riesgos electrónicos para su organización	158
Módulo 7 Preguntas de evaluación	159
8 Proceso para la seguridad de la información	161
Aptitud crítica 8.1 Realice una evaluación	163
Red	165
Seguridad física	167

Políticas y procedimientos	168
Precauciones	169
Concientización	170
Personas	171
Carga de trabajo	171
Actitud	172
Cumplimiento	172
Negocios	172
Resultados de la evaluación	173
Aptitud crítica 8.2 Desarrolle las políticas	173
Selección del orden de políticas a desarrollar	174
Actualización de políticas existentes	175
Aptitud crítica 8.3 Implementación de la seguridad	176
Sistemas de informes de seguridad	176
Sistemas de autenticación	177
Seguridad en Internet	178
Sistemas de detección de intrusiones	178
Encriptación	179
Seguridad física	180
Personal	180
Aptitud crítica 8.4 Emprenda una capacitación de concientización	181
Empleados	181
Administradores	181
Desarrolladores	181
Ejecutivos	182
Personal de seguridad	182
Aptitud crítica 8.5 Realice auditorías	182
Auditorías para el cumplimiento de las políticas	183
Evaluaciones periódicas y de nuevos proyectos	183
Pruebas de penetración	183
Proyecto 8 Desarrolle un programa de concientización de la seguridad	184
Módulo 8 Preguntas de evaluación	185
9 Mejores prácticas para la seguridad de la información	187
Aptitud crítica 9.1 Comprenda la seguridad administrativa	188
Políticas y procedimientos	188
Recursos	189
Responsabilidad	191
Educación	193
Planes de contingencia	195
Planes de un proyecto de seguridad	197
Aptitud crítica 9.2 Comprenda la seguridad técnica	199
Conectividad en red	199

Protección del código malintencionado	200
Autenticación	201
Monitoreo	202
Encriptación	203
Reparación (corrección) de sistemas	204
Respaldo y recuperación	204
Seguridad física	205
Aptitud crítica 9.3 Haga uso del ISO 17799	207
Conceptos clave del estándar	207
Cómo puede usarse este estándar	208
Proyecto 9 Realice un análisis de deficiencias	208
Módulo 9 Preguntas de evaluación	209

PARTE III

Tecnologías de seguridad

10 Muros de fuego	213
Aptitud crítica 10.1 Defina los tipos de muros de fuego	214
Muros de fuego de capa de aplicación	214
Muros de fuego de filtrado de paquete	216
Híbridos	218
Aptitud crítica 10.2 Desarrolle la configuración de un muro de fuego	218
Arquitectura #1: Sistemas con acceso a Internet al exterior del muro de fuego	219
Arquitectura #2: Muro de fuego simple	220
Arquitectura #3: Muros de fuego dobles	221
Aptitud crítica 10.3 Diseñe un conjunto de reglas para un muro de fuego	223
Proyecto 10 Examine las diferencias entre tipos de muros de fuego	224
Módulo 10 Preguntas de evaluación	225
11 Redes Privadas Virtuales (Virtual Private Networks, VPN)	227
Aptitud crítica 11.1 Defina las redes privadas virtuales	228
Aptitud crítica 11.2 Despliegue VPN de usuario	230
Beneficios de las VPN de usuario	231
Problemas con las VPN de usuario	232
Administración de las VPN de usuario	233
Aptitud crítica 11.3 Despliegue VPN de sitio	234
Beneficios de las VPN de sitio	235
Problemas con las VPN de sitio	235
Administración de las VPN de sitio	236
Aptitud crítica 11.4 Comprenda las técnicas estándar de la VPN	237
Servidor VPN	238
Algoritmos de encriptación	239

Sistema de autenticación	241
Protocolo de VPN	241
Aptitud crítica 11.5 Comprenda los tipos de sistemas VPN	242
Sistemas de hardware	243
Sistemas de software	243
Sistemas basados en la Web	244
Proyecto 11 Examine las diferencias entre tipos de muros de fuego	244
Módulo 11 Preguntas de evaluación	245

12 Encriptación	247
Aptitud crítica 12.1 Comprenda los conceptos básicos de encriptación	248
Términos de encriptación	249
Ataques en contra de la encriptación	249
Aptitud crítica 12.2 Comprenda la encriptación de clave privada	250
¿Qué es la encriptación de clave privada?	251
Códigos de sustitución	251
Libretas de un solo uso (“One-Time Pads”)	252
Estándar de encriptación de datos (Data Encryption Standard, DES)	252
DES Triple (Triple DES, TDES)	255
Encriptación de contraseña	256
La encriptación estándar avanzada (Advanced Encryption Standard, AES): Rijndael	257
Otros algoritmos de clave privada	257
Aptitud crítica 12.3 Comprenda la encriptación de clave pública	259
¿Qué es la encriptación de clave pública?	259
Intercambio de clave Diffie-Hellman	260
RSA	261
Otros algoritmos de clave pública	263
Aptitud crítica 12.4 Comprenda las firmas digitales	264
¿Qué es una firma digital?	264
Funciones condensadoras seguras	265
Aptitud crítica 12.5 Comprenda la administración de claves	266
Creación de clave	266
Distribución de clave	267
Certificación de clave	268
Protección de la clave	268
Revocación de la clave	270
Aptitud crítica 12.6 Comprenda la confianza en el sistema	270
Jerarquía	270
Web	273
Proyecto 12 Diseñe un sistema de encriptación	274
Módulo 12 preguntas de evaluación	275

13 Detección de intrusiones	277
Aptitud crítica 13.1 Defina los tipos de sistemas de detección de intrusiones (Intrusion Detection Systems, IDS)	279
IDS basado en anfitrión (Host-Based IDS, HIDS)	280
IDS basado en red (Network-Based IDS, NIDS)	283
¿Es mejor cierto tipo de IDS?	285
Aptitud crítica 13.2 Establezca un IDS	285
Definición de las metas del IDS	285
Elección de lo que hay que monitorear	287
Elección de la manera de responder	290
Configuración de límites	294
Implementación del sistema	296
Aptitud crítica 13.3 Administre un IDS	296
Comprensión de lo que puede informarle un IDS	297
Investigación de eventos sospechosos	300
Aptitud crítica 13.4 Comprenda la prevención de las intrusiones	304
Cómo pueden evitarse las intrusiones con el uso de IDS	304
Cuestiones relacionadas con la prevención de intrusiones	305
Proyecto 13 Despliegue un IDS de red	306
Módulo 13 Preguntas de evaluación	307

PARTE IV

Aplicaciones prácticas de implementaciones específicas de la plataforma

14 Cuestiones de seguridad en Unix	311
Aptitud crítica 14.1 Configuración del sistema	312
Archivos de arranque	312
Servicios permitidos	313
Archivos de configuración del sistema	316
Reparaciones o correcciones (“parches” o <i>patches</i>)	322
Aptitud crítica 14.2 Realice la administración de usuarios	322
Agregar usuarios al sistema	323
Eliminar usuarios del sistema	325
Aptitud crítica 14.3 Realice la administración del sistema	325
Auditar un sistema	325
Archivos de registro o de bitácora	326
Archivos ocultos	326
Archivos SUID y SGID	327
Archivos escribibles por cualquier persona (“World-Writable”)	327
Búsqueda de señales sospechosas	327
Proyecto 14 Audite un sistema Unix	331
Módulo 14 Preguntas de evaluación	333

15	Cuestiones de seguridad de servidores: Windows 2000/Windows 2003 server	335
	Aptitud crítica 15.1 Establezca el sistema	336
	Parámetros para la política de seguridad local	336
	Configuración del sistema	341
	Cuestiones especiales de configuración para Windows 2003	347
	Aptitud crítica 15.2 Administre a los usuarios	350
	Agregar usuarios al sistema	350
	Establecer permisos de archivo	352
	Eliminar usuarios del sistema	352
	Aptitud crítica 15.3 Administre el sistema	353
	El comando secdit	354
	Auditoría de un sistema	357
	Archivos de registro (bitácora)	358
	Búsqueda de señales sospechosas	358
	Aptitud crítica 15.4 Utilice el directorio activo (Active Directory)	361
	Instalación y configuración seguras	362
	Administración	362
	Seguridad y política de grupo (Group Policy, GP)	363
	Usuario de AD y administración de grupo	371
	Proyecto 15 Haga uso de secdit para administrar las configuraciones de seguridad de Windows 2000	372
	Módulo 15 Preguntas de evaluación	373
16	Arquitectura de Internet	375
	Aptitud crítica 16.1 Aprenda qué servicios ofrecer	376
	Correo	376
	Correo electrónico (e-mail) encriptado	376
	La Web	377
	Acceso interno a Internet	377
	Acceso externo a los sistemas internos	378
	Servicios de control	379
	Aptitud crítica 16.2 Aprenda qué servicios no ofrecer	380
	Aptitud crítica 16.3 Desarrolle una arquitectura de comunicaciones	381
	Acceso de línea simple	381
	Acceso de línea múltiple para un ISP simple	382
	Acceso de línea múltiple hacia múltiples ISP	386
	Aptitud crítica 16.4 Diseñe una "zona desmilitarizada" (Demilitarized Zone, DMZ)	388
	Definición de la DMZ	389
	Sistemas a colocar en la DMZ	389
	Arquitecturas DMZ apropiadas	391
	Aptitud crítica 16.5 Comprenda la traducción de direcciones de red (Network Address Translation, NAT)	395
	¿Qué es la traducción de direcciones de red?	395

Direcciones de clase privada	396
NAT estática	396
NAT dinámica	397
Aptitud crítica 16.6 Diseñe redes asociadas	398
Uso de las redes asociadas	399
Configuración	399
Cuestiones de direccionamiento	400
Proyecto 16 Cree una arquitectura de Internet	401
Módulo 16 Preguntas de evaluación	402
17 Necesidades de seguridad en el comercio electrónico	403
Aptitud crítica 17.1 Comprenda los servicios del comercio electrónico	404
Diferencias entre los servicios de comercio electrónico y los servicios regulares de DMZ	405
Ejemplos de servicios de comercio electrónico	406
Aptitud crítica 17.2 Comprenda la importancia de la disponibilidad	407
Cuestiones de negocio a consumidor (Business-to-Consumer)	408
Cuestiones de negocio a negocio (Business-to-Business)	408
Tiempo global	409
Comodidad del cliente	409
Costo del tiempo de inactividad	410
Solución del problema de disponibilidad	410
Aptitud crítica 17.3 Implemente la seguridad por el lado del cliente	411
Seguridad en las comunicaciones	412
Guardar la información en el sistema del cliente	412
Refutación	413
Aptitud crítica 17.4 Implemente la seguridad por el lado del servidor	414
Información almacenada en el servidor	414
Protección del servidor contra un ataque	415
Aptitud crítica 17.5 Implemente la seguridad de la aplicación	419
Diseño apropiado de la aplicación	420
Técnicas adecuadas de programación	421
Mostrando el código al mundo	422
Administración de la configuración	422
Aptitud crítica 17.6 Implemente la seguridad del servidor de las bases de datos	423
Ubicación de las bases de datos	423
Comunicación con el servidor de comercio electrónico	424
Protección de acceso interno	425
Aptitud crítica 17.7 Desarrolle una arquitectura de comercio electrónico	426
Ubicación y conectividad del servidor	426
Disponibilidad	428
Exploración de vulnerabilidades	428
Información de auditoría y detección de problemas	428

Proyecto 17 Diseña una arquitectura de comercio electrónico	429
Módulo 17 Preguntas de evaluación	430
18 Seguridad inalámbrica	431
Aptitud crítica 18.1 Comprenda la tecnología inalámbrica actual	432
Arquitecturas estándar	433
Seguridad de las transmisiones	433
Autenticación	435
Aptitud crítica 18.2 Comprenda las cuestiones de seguridad en un entorno inalámbrico	438
Detección de WLAN	438
Escucha furtiva	438
Ataques activos	440
Cuestiones legales potenciales	440
Aptitud crítica 18.3 Despliegue de manera segura un entorno inalámbrico	441
Seguridad del punto de acceso	441
Seguridad de las transmisiones	442
Seguridad de la estación de trabajo	442
Seguridad del sitio	443
Proyecto 18 Implementación de una LAN inalámbrica	443
Módulo 18 Preguntas de evaluación	444
A Respuestas a las preguntas de evaluación	445
Módulo 1: ¿Qué es la seguridad de la información?	446
Módulo 2: Tipos de ataques	446
Módulo 3: Técnicas de los Hackers	447
Módulo 4: Servicios de seguridad de la información	448
Módulo 5: Cuestiones legales en la seguridad de la información	448
Módulo 6: Políticas	449
Módulo 7: Administración de riesgos	450
Módulo 8: Proceso para la seguridad de la información	450
Módulo 9: Prácticas óptimas para la seguridad de la información	451
Módulo 10: Muros de fuego	452
Módulo 11: Redes privadas virtuales	452
Módulo 12: Encriptación	453
Módulo 13: Detección de intrusiones	453
Módulo 14: Cuestiones de seguridad en Unix	454
Módulo 15: Cuestiones de seguridad del servidor Windows 2000/2003	455
Módulo 16: Arquitectura de Internet	456
Módulo 17: Necesidad de seguridad en el e-comercio	457
Módulo 18: Seguridad inalámbrica	457
Índice	459