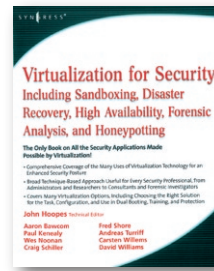


CRYPTOGRAPHY AND NETWORK SECURITY Principles and Practices

Autor: William Stallings
Editorial: Pearson
Año: 2006 – 680 páginas
ISBN 0-13-202322-9
www.pearsoned.com

El presente manual ofrece un examen detallado de los algoritmos de cifrado convencionales y de sus principios de diseño, incluyendo una disertación sobre el uso del cifrado convencional para proveer servicios de confidencialidad; a continuación proporciona un análisis exhaustivo de los algoritmos de cifrado de clave pública, además de profundizar en el uso de códigos de autenticación de mensajes y de funciones resumen, firma digital y certificados de clave pública; tras estos contenidos de índole teórica, comienza una sección eminentemente práctica, dedicada a importantes instrumentos de seguridad de redes y aplicaciones, entre las que figuran Kerberos, los certificados X.509v3, PGPS/MIME, Seguridad IP, SSL/TLS y SET; mientras que la última parte de la obra, también de aplicación práctica, aborda la seguridad en el nivel del sistema.

Es igualmente destacable que para la elaboración de esta cuarta edición de la obra, su afamado autor, en colaboración con diversos profesionales del sector, ha revisado y actualizado el contenido del libro, figurando entre las novedades introducidas una versión simplificada del Estándar de Cifrado Avanzado (*Advanced Encryption Standard* o AES) que hace más fácil su comprensión; el algoritmo *hash* seguro Whirlpool, que está basado en la utilización de un cifrador en bloque simétrico; CMAC (*Cipher-based Message Authentication Code*), un modo de operación de cifrado en bloque que proporciona mensajes de autenticación basados en el uso de un cifrador en bloque simétrico; PKI (*Public Key Infrastructure*); ataques de denegación de servicio distribuidos (DDoS); y los Criterios Comunes (*Common Criteria*) para evaluar la seguridad de la tecnología de la información. ■



VIRTUALIZATION FOR SECURITY Including Sandboxing, Disaster Recovery, High Availability, Forensic Analysis and Honeypotting

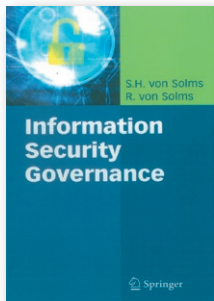
Autores: John Hoopes (editor técnico), Aaron Bawcom, Wes Noonan, Craig Schiller, Fred Shore, Andreas Turriff, Carsten Willems y David Williams
Editorial: Syngress
Año: 2009 – 357 páginas. ISBN 13: 978-1-59749-305-5
www.syngress.com

Este práctico y novedoso libro sobre las aplicaciones de seguridad que la virtualización hace posible enseña a crear un entorno aislado, o *Sandbox*, en el que poder probar aquellas aplicaciones que podrían poner en peligro la seguridad; también muestra cómo construir un *honeypot*, o cebo para descubrir *hackers* y vulnerabilidades en el entorno de producción real; e instruye al lector en las técnicas de anti-virtualización y de análisis de *malware* para poner en cuarentena y estudiar códigos dañinos en entornos seguros.

Asimismo, quienes lean esta obra estarán mejor capacitados para desplegar aplicaciones en entornos de simulación, que imitan al mundo real, para observar su comportamiento;

aprenderán la técnica del *fuzzing*, que consiste en proporcionarle a una aplicación datos semi-aleatorios para detectar posibles fallos de seguridad; y serán capaces de llevar a cabo un análisis forense, para investigar una máquina concreta sin alterar el dato original.

En adición a lo anterior, con ayuda de este texto el lector reducirá el tiempo de recuperación de desastres haciendo que los sistemas de *backup* y de restauración sean más simples, rápidos y eficientes; podrá utilizar múltiples sistemas operativos sobre una misma máquina, tanto de forma nativa como en un entorno virtual; y le proporcionará a los usuarios acceso seguro a áreas potencialmente comprometidas. ■



INFORMATION SECURITY GOVERNANCE

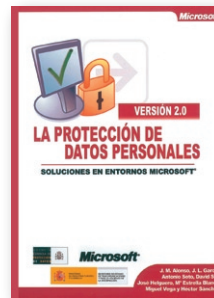
Autores: S.H. von Solms y R. Von Solms
Editorial: Springer
Año: 2009 – 134 páginas
ISBN: 978-0-387-79983-4
www.springer.com

La obra aquí reseñada pretende mostrar cómo gobernar de manera efectiva la seguridad de la información, y para ello, los hermanos von Solms empiezan definiendo la seguridad de la información como la disciplina utilizada para proteger la información, y el gobierno de la seguridad de la información como el entorno dentro de la empresa, que hace posible esta protección, y que implica a todos los miembros de la compañía, desde el presidente del Consejo de Dirección hasta cualquiera de los usuarios finales.

En la obra se explica también la relación que mantiene el gobierno de la seguridad de la información con el gobierno corporativo y con el gobierno de las TI, haciendo hincapié en que el gobierno de la seguridad de la información forma parte de todo buen gobierno corporativo, y que el Consejo Directivo de la compañía debe ser el último res-

ponsable de la gestión de la seguridad de la información.

A continuación se presenta un modelo de gobierno de seguridad de la información basado en las *best practices* COBIT e ISO 27002; y constituido por los siguientes componentes: la arquitectura de la política de seguridad de la información; el cumplimiento y el control en el gobierno de la seguridad de la información; la gestión de riesgos en el gobierno de la seguridad de la información; la planificación de la seguridad de la información y su función en una empresa; y la importancia de la educación, la formación, y la concienciación, en materia de seguridad, de todos los miembros de una organización, para mantener la información corporativa a salvo. Finalmente, se proporciona una metodología para establecer un buen programa de gobierno de seguridad de la información en la compañía. ■



PROTECCIÓN DE DATOS PERSONALES Soluciones en entornos Microsoft

Autores: J.M. Alonso, J.L. García, A. Soto, D. Suz, J. Helguero, M^a E. Blanco, M. Vega y H. Sánchez
Publicado por: Microsoft Ibérica
Año: 2009 – 388 páginas
Depósito Legal: M-14799-2009

Con prólogos de **María Garaña**, presidenta de **Microsoft Ibérica**; **Artemi Rallo**, director de la **Agencia Española de Protección de Datos (AEPD)**; y **Sebastián Muriel**, director general de **Red.es**, la presente publicación, de carácter exclusivamente informativo, tiene por objeto ayudar a los responsables de Sistemas y Seguridad, a desempeñar con eficacia la labor de proteger la información y, para ello, acerca al lector tanto el conocimiento práctico de la ley, como las configuraciones tecnológicas de la plataforma Microsoft más adecuadas a cada nivel de protección exigido.

Según lo dicho, la obra está dividida en dos partes: la primera, de carácter legal, muestra los límites en el tratamiento de datos personales, ilustrando al lector

sobre las obligaciones básicas que establece la LOPD, los derechos de los titulares de los datos, los tratamientos especiales, o las infracciones y sanciones entre otros aspectos; mientras que la segunda parte, de tipo técnico, explica cómo adaptar la plataforma Microsoft a los requisitos técnicos de la ley en materia de protección de datos; a través de cinco capítulos que versan sobre: la seguridad en sistemas Microsoft, la aplicación de la seguridad del reglamento de desarrollo de la LOPD en los sistemas Microsoft, la aplicación de dichas medidas de seguridad reglamentarias en SQL Server, la implementación de la LOPD sobre SQL Server (SQL Server 2005-2008) y la política de seguridad. ■