

IT RISK. Turning Business Threats Into Competitive Advantage

Autores: George Westerman y Richard Hunter
 Editorial: Harvard Business School Press
 Año 2007 - 220 páginas
 ISBN-13: 978-1-4221-0666-2
www.HBSPress.org

Los incidentes TI se pagan caros: dañan la reputación corporativa, muestran los puntos débiles de los equipos directivos de la firma que lo padece y desencadenan tanto pérdidas de beneficios como de competitividad. Por eso, gestionar bien el riesgo es una necesidad cada vez más acuciante en el seno de cualquier organización, aunque no todas estén preparadas para hacerlo correctamente. *IT Risk* enseña a suplir esta carencia explicando cómo los directivos de las compañías y los responsables de TI han de trabajar juntos para gestionar el riesgo desde la seguridad y la responsabilidad. Además, está repleto de ejemplos prácticos y consejos para mejorar la capacidad de reacción de la

empresa ante desastres.

Sus autores, **George Westerman** y **Richard Hunter**, a lo largo de los nueve capítulos de que consta el texto, definen los tres pilares sobre los que se apoya una gestión eficiente del riesgo. El primero de ellos son los principios, personas, procesos de soporte y controles, que permiten a los ejecutivos gestionar el riesgo en el orden correcto. La segunda es un programa de actuación bien diseñado, que incluya una visión global del conjunto, para permitir a las compañías identificar y priorizar los peligros. Y la tercera consiste en concienciar a todos y cada uno de los empleados de los peligros que entraña la tecnología, para que actúen con cautela y prudencia. ■



SECURING AJAX APPLICATIONS

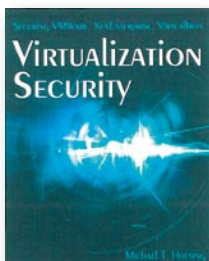
Autor: Christopher Wells
 Editorial: O'Reilly
 Año: 2007- 233 páginas
 ISBN _ 10: 0-596- 52931-7
www.oreilly.com

El propósito de *Securing Ajax Applications* es explorar esta nueva generación de desarrolladores web y los problemas de seguridad que plantean, mostrando las técnicas básicas de seguridad y examinando vulnerabilidades con JavaScript, XML, JSON, Flash y otras tecnologías. La obra de Wells hace especial hincapié en la importancia de localizar “agujeros” peligrosos, y propone formas de cubrirlos antes de que se conviertan en un problema más serio; ya que Ajax, pese a sus muchas bondades, también proporciona a los *hackers* nuevas oportunidades de apropiarse de datos ajenos o interferir en los intercambios de información entre varios usuarios.

Esta es, por tanto, una obra destinada a programadores que quieren

aprender a hacer más seguras las aplicaciones Ajax y a saber reaccionar con prontitud cuando se produce un ataque. Asimismo, también es aconsejable para desarrolladores y arquitectos de sistemas, pues a éstos les interesa compartir y consumir contenidos de manera segura.

Los epígrafes que conforman la misma son los que siguen: 1. **La Red cambiante**, 2. **La seguridad de la Red**, 3. **Haciendo seguras las tecnologías de la Red**, 4. **Protegiendo el servidor**, 5. **Unos cimientos débiles**, 6. **Haciendo seguros los servicios de la Red**, 7. **Construyendo APIs seguras**, 8. **“Mashup” (remezclar)**. Este último término hace referencia a la facilidad de construir nuevas aplicaciones utilizando APIs abiertas. ■



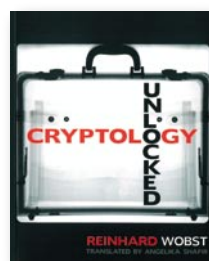
VIRTUALIZATION SECURITY. Securing VMWare, XenEnterprise, VirtualIron

Autor: Michael T. Hoelsing
 Editorial: Wiley
 Año 2008 - 408 páginas
 ISBN: 978-0-470-17706-8
www.wiley.com

El emergente entorno virtual que empieza a envolver las infraestructuras informáticas de las corporaciones de todo el planeta está planteando serios problemas de seguridad y, por lo novedoso del tema, pocos profesionales de la protección TI han escrito todavía sobre ello. A este reducido grupo pertenece **Michael T. Hoelsing**, autor de este libro –que verá la luz comercial en la primavera de 2008– en el que, además de detallarse en qué consiste la virtualización, se profundiza en cómo proporcionar un estatus de seguridad a las instalaciones existentes, además de examinar las capacidades de los instrumentos de virtualización de VMWare, XenEnterprise y VirtualIron.

Sin duda, la obra debiera erigirse en referencia obligada de directores y auditores de seguridad de la información, arquitectos de redes y consultores. Igualmente, también puede resultar de gran utilidad para todos aquellos responsables de redes y administradores de sistemas que pretendan evitar un informe desfavorable por parte de los primeros.

El volumen proporciona material de fondo para comprender la historia de la virtualización, su importancia en el mundo de los negocios o sus raíces. Asimismo, se adentra en los problemas de seguridad que un entorno virtual plantea y describe y evalúa las herramientas Ecora, Nessus, CIS, LSAT, junto con el *script* del autor. ■



CRYPTOLOGY UNLOCKED

Autor: Reinhard Wobst
 Editorial: Wiley
 Año 2007- 540 páginas
 ISBN: 978-0-470-06064-3
www.wiley.com

Cryptology Unlocked es una obra innovadora que abarca desde los métodos de cifrado más sencillos hasta las complejas investigaciones del algoritmo moderno, empleando para ello un peculiar estilo no-matemático. De este modo profundiza en conceptos como el cifrado, el criptoanálisis (algoritmos clásicos y modernos), los protocolos criptográficos o los estándares digitales, además de adentrarse en los peligros de romper los códigos.

Comienza con una introducción en la que su autor, el matemático **Reinhard Wobst**, explica por qué es importante la criptografía. Le siguen siete capítulos cuyo orden es el siguiente: 2. **El cifrado desde los romanos hasta la II Guerra Mundial**,

3. **Criptoanálisis en profundidad**, 4. **Hitos en el desarrollo: DES, RSA**, 5. **La vida después de DES: nuevos métodos, nuevos ataques**, 6. **Protocolos de cifrado**, 7. **Aplicaciones prácticas**, y 8. **Cifrado, política y negocios**.

Su lectura revela aspectos de sumo interés como son las premisas básicas para diferenciar entre un buen algoritmo, seguro y difícil de romper, y uno inseguro; hasta qué punto los servicios secretos pueden o no leer todo tipo de mensajes; el efecto que el cifrado tuvo en la II Guerra Mundial; los riesgos de seguridad que se ocultan detrás de los estándares digitales móviles GSM y UMTS; y las implicaciones diarias para firmas digitales y códigos PIN. ■