

SEGURIDAD INFORMÁTICA PARA EMPRESAS Y PARTICULARES



Autores: Gonzalo Álvarez y Pedro Pablo Pérez
 Editorial: McGraw Hill
 Año: 2004 - 411 páginas
 ISBN: 84-4814297-7
 www.mcgraw-hill.es

La obra de **Gonzalo Álvarez** y **Pedro Pablo Pérez** –dos consultores de marcado carácter técnico–, es una aportación, otra más, al caudal de volúmenes cuya filosofía es la de ofrecer un libro ‘comprensible’ para ese universo de potenciales lectores,

conformado por particulares, profesionales liberales y pequeñas empresas en las que, no constituyendo las TI la columna vertebral de su actividad, deben bregar con la tecnología informática y escenarios IP, y por ende, se ven abocados a lidiar con algunos aspectos de la seguridad informática, sin posibilidad ni ganas de ahondar excesivamente en ellos.

Este propósito, sin duda loable, ya lo enarbola en el prólogo **J.C.G. Cuartango**, afamado especialista de las salas de máquinas cibernéticas y azote de sus aluminosis, al afirmar que resultaba patente la inexistencia de obras en castellano que abordaran el tema de la seguridad informática a un nivel intermedio. Esto no es en absoluto cierto. En los últimos cinco años no pocas editoriales han inundado el mercado con obras de similar pelaje, fueran ya de autores españoles o traducidas a nuestro idioma, cuyo nivel se orienta exactamente a la desatendida audiencia mentada por Cuartango.

Ahora bien, si esto es así, ¿por qué se recensiona en esta página una obra que parece de rango ‘ligero’ al no adecuarse al perfil de la audiencia de SIC, sí habituada a profundizar en cualesquiera temas de la seguridad TIC? Pues porque aunque no lo hayan advertido sus autores, sí se adecua bastante y porque es buena. Para entender esto basta con unos botones de muestra: a los ‘particulares’ a los que hace referencia el título del libro, ¿hasta qué punto les interesa conocer qué es un análisis de riesgos, cómo son las tripas de un IDS, si la clave privada de una firma está validada, la transparencia del SLA del MSSP o si la UNE/ISO/IEC 17799: 2002 es una opción a considerar?, porque esos asuntos también son abordados en la obra y no precisamente de forma ligera ...

Es decir, el libro trasciende, para bien, los modestos límites de conocimiento de la supuesta audiencia del mismo. Es más, constituye una excelente y bien dimensionada recopilación de temas, articulada en seis capítulos, éstos: 1) **Introducción a la seguridad de la información**; 2) **Anonimato y privacidad**; 3) **CID: Confidencialidad, Integridad, Disponibilidad**; 4) **Protección de redes**; 5) **Protección de equipos**; 6) **Auditoría, detección de intrusiones y análisis forense**. El volumen se completa con dos apéndices (**Listas de tareas de seguridad y Herramientas de seguridad**).

Por cierto, y eso sí es novedad: está más que correctamente escrito, no rechina ninguna expresión o palabra y ese mérito, justo es reseñarlo, han de compartirlo sus autores con Panda Software, uno de cuyos especialistas, **Pedro Bustamente**, ha hecho una estupenda revisión técnica del libro. ■

Luis G. Fernández

DEFEND I.T.: Security by Example



Autores: Ajay Gupta y Scott Laliberte
 Editorial: Addison Wesley
 Año 2004 - 349 páginas
 ISBN: 0-321-19767-4
 www.agprofessional.com

Dirigido tanto a profesionales TIC con interés en el área de la seguridad, como a administradores de red, y expertos en seguridad de la información, *Defend I.T.*, recoge un buen número de ejemplos prácticos de situaciones a las que habitualmente se enfrentan los profesionales de la seguridad lógica, todos ellos analizados desde la metodología del caso. De este modo, el libro se fragmenta en cinco partes: **Basic Hacking**, que recorre algunas técnicas básicas de ataque empleadas por los *hackers*, como *mapping* de red, ataques a sistemas comprometidos por brechas en la arquitectura, y ataques de denegación de servicio (DoS); **Current Methods**, que presta atención a cuestiones críticas de actualidad, como la seguridad en redes inalámbricas, las nuevas amenazas de código malicioso, o los problemas derivados de los fallos de comunicación

entre una consultora de seguridad y su cliente; y **Additional Items on the Plate**, que aborda algunas otras materias que son responsabilidad del profesional de la seguridad TIC, como la selección de un sistema de detección de intrusiones (IDS), planes de recuperación ante desastres, elaboración de una política de seguridad oficial, y los detalles relativos a la asunción de la norma americana HIPAA, que regula las transmisiones de datos personales sanitarios a través de soportes telemáticos o virtuales. Finalmente, las últimas dos secciones de este volumen se refieren, por un lado, a los métodos más clásicos de ataques a las redes, recogidos en un apartado titulado **Old School**; y a la aplicación de técnicas de análisis forense, abordada a lo largo de tres casos diferentes, englobados bajo el título **Computer Forensics**. ■

PLANES DE CONTINGENCIA. La continuidad del “negocio” en las organizaciones



Autor: Juan Gaspar Martínez
 Editorial: Díaz de Santos
 Año 2004 - 220 páginas (incluye CD)
 ISBN: 84-7978-647-7
 www.diazdesantos.es/ediciones

Esta obra de **Juan Gaspar** –un auténtico veterano de la seguridad TIC en nuestro país– resume toda una carrera centrada en la materia. Muy pocos profesionales podrán hacer gala de un conocimiento tan intenso como el que el autor hace en su obra. Desde una óptica ciertamente clásica, realiza un recorrido por las diversas fases para la elaboración de un Plan de Contingencia, o lo que es lo mismo, un conjunto de estrategias y procedimientos preventivos y reactivos que permiten un rápido retorno a una situación suficientemente normalizada para que la actividad de la organización recupere un nivel aceptable después de una interrupción no prevista de sus sistemas de información. En este sentido, las fases propuestas están inspiradas

en los principios difundidos por el *Business Continuity Institute* británico, para la gestión de la continuidad del “negocio” corporativo, y se desarrollan a lo largo de ocho capítulos: 1. **Iniciación y gestión del proyecto**, 2. **Análisis de riesgos**, 3. **Análisis de impacto**, 4. **Desarrollo de las estrategias de continuidad**, 5. **Operaciones de respuesta ante la emergencia**, 6. **Desarrollo e implementación de los planes de continuidad de negocio**, 7. **Entrenamiento, pruebas y mantenimiento**, 8. **Estrategias de comunicación y gestión de la crisis**. Asimismo, el libro se completa con dos anexos, uno relativo a **Legislación y Normativa**, y otro titulado **Consideraciones económicas. Análisis coste/beneficio**. ■