

AVANCES EN CRIPTOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

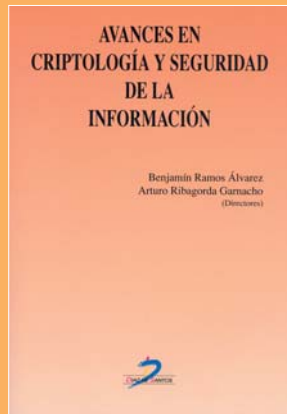
Para empezar, es de justicia reconocer que Díaz de Santos, la editorial que cobija la obra aquí glosada, siempre ha prestado atención a los temas que conforman el mundo de la seguridad de la información y la seguridad TIC. A su histórica receptividad hay que sumar el buen hacer editorial de su producción, con obras bien diseñadas, traducidas y vestidas, en las que obviamente "Avances en criptología y seguridad de la información" también hay que incluir.

Un segundo motivo de satisfacción es constatar quiénes son los directores del volumen recensionado, Arturo Ribagorda y Benjamín Ramos, que, dado sus dilatados y brillantes *curricula* académicos en la materia, no necesitan de excesivas presentaciones; muchos de quienes llevamos más de una década especializados en este campo en nuestro país, hemos enriquecido nuestro acervo gracias a las abundantes aportaciones de ambos especialistas.

Dicho esto, el volumen que nos ocupa surge como resultado recopilatorio de la octava reunión española sobre criptología y seguridad de la información, acontecida el pasado septiembre en las instalaciones de la Universidad Carlos III de Madrid, que ejerció de entidad organizadora y anfitriona.

En palabras de Ribagorda, que prologa la obra, "este volumen recoge los últimos avances en la materia, expuestos por sus propios desarrolladores, que unen a sus conocimientos una acu-

Directores: Benjamín Ramos y Arturo Ribagorda
Editorial: Díaz de Santos, S.A.
Año 2004 - 697 páginas
ISBN: 84-7978-650-7
www.diazdesantos.es/ediciones



sada vocación docente, lo que les permite plantear temas de gran actualidad con elevado rigor no exento de una gran claridad expositiva. Esperamos por tanto que este libro sea de gran utilidad a todos aquellos, profesionales o no, interesados en este fructífero, pujante y vital campo de la seguridad".

Esta cita bienal suele reunir las aportaciones periódicas –mayoritariamente españolas– del mundo académico junto con algunas conferencias de ponentes invitados de renombre en dicho campo. En esta edición, como en las anteriores, el resultado es quizá algo dispar. Algunos temas –aunque en ocasiones muy 'duros' de contenido– son de gran interés y responden al devenir actual de la seguridad TIC, pero otros acusan una excesiva bisoñez.

En cualquier caso, el haber del libro es notable y sus páginas constituyen un fiel reflejo de lo que este colectivo da de sí. Empero, es una pena constatar cuán alejados de la realidad del mundo empresarial y social están algunos investigadores, pero es lo que hay.

El contenido de la obra se vertebra en los siguientes capítulos: Criptografía, Criptoanálisis, Protocolos criptográficos y validación, Seguridad en sistemas de información, Seguridad en redes e internet, Servicios de certificación y notarización, Seguridad en DRM, y Anexos. ■

Luis Fernández

BLACK ICE. La amenaza invisible del ciberterrorismo



Autor: Dan Verton
Editorial: McGraw Hill
Serie: Telecomunicaciones
Año 2003 - 298 páginas
ISBN: 84-481-2954-7
www.mcgraw-hill.es

La premisa de partida es clara: el nuevo rostro del terrorismo (el ciberterrorismo) es consecuencia de la constatación y aprendizaje por parte de los terroristas actuales de que la seguridad nacional de una nación depende de las infra-

estructuras críticas, que a su vez dependen de ordenadores y redes informáticas. Un ataque estratégico sobre esos sistemas tendría indudablemente consecuencias devastadoras para los países y la economía de los mismos.

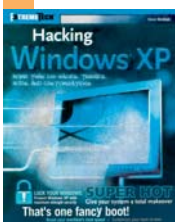
Los futuribles sobre posibles ataques, la reconstrucción de los habidos y las propuestas de acciones encaminadas a prever y paliar, en lo posible, acciones de este calado, conforman el contenido de este ameno libro de Dan Verton, periodista y antiguo oficial de inteligencia del U.S. Marine Corps.

Entre el caudal de frases lapidarias y sensatas advertencias propugnadas por el autor, valgan como botón de muestra dos ejemplos: "La

seguridad nacional de América depende de su seguridad económica y en la vanguardia de ambas hay un sistema digital débil, sin proteger y manejado por corporaciones", y "Muchos analistas y observadores de seguridad en Internet han rechazado reconocer los aspectos físicos del ciberterrorismo, la mayoría debido a una carencia de educación oficial y experiencia en aproximaciones holísticas de la seguridad".

El intercambio de información de inteligencia en tiempo real es la clave para asegurar que el futuro del terrorismo de alta tecnología no se expanda a demasiada velocidad, alertándonos de su presencia cuando sea demasiado tarde. ■

HACKING WINDOWS XP



Autor: Steve Sinchak
Editorial:
John Wiley & Sons
Año 2004 - 355 páginas
ISBN: 0-7645-6929-5
www.wiley.com

Steve Sinchak es un empresario responsable de varias compañías digitales, entre las que se encuentra TweakXP.com, que reúne una gran

base de datos de arreglos o *tweaks* de Windows XP y es lugar habitualmente visitado por los *hackers* de este sistema operativo. Partiendo de la base, como así afirma el autor, de que XP es más rápido y seguro que cualquier otra versión de Windows, el libro ofrece algunas indicaciones para personalizar, y optimizar el rendimiento y la seguridad del mismo.

Las propuestas del autor se estructuran en el manual de la siguiente manera: **I Parte: Personalice su sistema.** 1) Cómo personalizar la apariencia del arranque; 2) Personalizar la navegación de

usuario; 3) "Hackear" el escritorio; 4) Personalizar el aspecto del interfaz de Windows; 5) "Hackear" el explorador de Windows; 6) Examinar otras mejoras de Windows. **II Parte: Mejore el funcionamiento de su sistema.** 7) Analizando su sistema; 8) Agilizar el arranque del sistema; 9) Cómo hacer que su ordenador se cargue más rápido; 10) Cómo hacer que su ordenador responda mejor; 11) Aumentar la velocidad. **III Parte: Asegure su sistema.** 12) Proteja su ordenador de los intrusos; 13) Luchar contra el *spam*, el *spyware* y los virus; 14) Cómo proteger su privacidad. ■