



## THE NEW SCHOOL OF INFORMATION SECURITY

**Autores:** Adam Shostack y Andrew Stewart  
**Editorial:** Addison-Wesley  
**Año:** 2008 – 238 páginas  
**ISBN-13:** 978-0-321-50278-0  
[www.informit.com/aw](http://www.informit.com/aw)

En esta obra se propone a los profesionales de la seguridad TIC una forma de trabajar innovadora que los autores han denominado "Nueva Escuela", la cual sostiene que la toma de decisiones de seguridad debe ser totalmente racional, fundamentada en minuciosos análisis e investigaciones; y también que los responsables de esta disciplina tomarán mejores decisiones si aprenden de otras materias científicas, como la economía, la sociología o la psicología. Es de reseñar que en España ya hay destacados profesionales muy receptivos a este enfoque moderno y multidisciplinar.

Según Shostack y Stewart, otra diferencia entre la escuela tradicional y la por ellos propuesta es que, para la nueva, la seguridad de la información ha dejado de ser, principalmente, una cuestión de tecnología. De hecho, en

la obra se afirma que las empresas que más invierten en productos de seguridad no son necesariamente las que mejor responden cuando se producen incidentes. Sobre este asunto, el del gasto del presupuesto para protección, el texto enseña a evaluar los factores psicológicos y sociológicos y a emplear las técnicas de valoración económica adecuadas para decidir en qué se debe invertir, en qué no y cuánto. En adición a lo anterior, la obra muestra cómo sacar partido de la detección de las fugas de información, las cuales permiten descubrir las deficiencias de los sistemas de seguridad para subsanarlas; siendo otro aspecto destacado por los autores que el trabajo en solitario es poco eficiente, por lo que la industria de la seguridad en su conjunto debe colaborar para poder evolucionar.



## 1998 – 2008 – UNA AL DÍA Diez años de seguridad informática

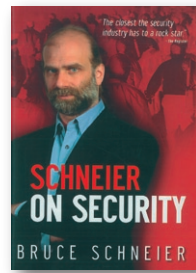
**Autor:** Sergio de los Santos  
**Editorial:** Creative Commons - Hispasec Sistemas  
**Año:** 2008 – 274 páginas  
**ISBN:** 978-1-4092-4380-9  
[www.hispasec.com](http://www.hispasec.com)

Para conmemorar el décimo aniversario de "Una al día", sin duda la iniciativa recopiladora más popular en formato digital de noticias de seguridad TIC en español –y precursora de lo que hoy es Hispasec Sistemas y el portal de dicho nombre–, uno de los artífices del mismo ha publicado el texto objeto de reseña.

Estructurada en capítulos –cada uno de los cuales corresponde a un año entre 1998 y 2008–, todos comienzan con un recorrido breve, para su contextualización, por acontecimientos relevantes sucedidos en esos periodos de tiempo y, a continuación, se tratan datos y noticias más destacados relativos al ámbito de la seguridad TIC, para después incluir algunos de los boletines tal cual fueron publicados. La obra recoge en total una selección cercana al centenar de estos boletines, al objeto de proporcionar una

visión global de esa parcela de la seguridad en un determinado año.

Cada uno de estos once capítulos contiene, además, una breve entrevista a algún personaje –todos ellos aún vigentes– que fue importante en el campo de la seguridad informática durante el año referido, como **Juan Salom**, Jefe del Grupo de Delitos Telemáticos de la U.C.O. de la Guardia Civil; **Jorge Ramíó**, coordinador de CriptoRed; **Héctor Sánchez**, responsable del área de Seguridad de Microsoft Iberia entre 2001 y 2003; **Bruce Schneier**, criptógrafo y 'gurú' de la seguridad, además de CTO de BT Counterpane; **Mikel Urizarbarrena**, fundador de Panda Security; o **Eugene Kaspersky**, presidente y fundador de Kaspersky Labs. Asimismo, el libro incluye documentación aneja y está salpicado de anécdotas referentes a "Una-al-día" y a Hispasec.



## SCHNEIER ON SECURITY

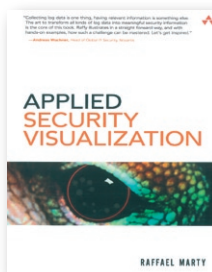
**Autor:** Bruce Schneier  
**Editorial:** Wiley  
**Año:** 2008 – 328 páginas  
**ISBN:** 978-0-470-39535-6  
[www.wiley.com](http://www.wiley.com)

El volumen reseñado consiste en una recopilación de ensayos y artículos publicados por **Bruce Schneier**, tecnólogo de seguridad y experto en criptografía, entre junio de 2002 y junio de 2008, en diferentes medios de comunicación, tanto impresos como electrónicos, entre los que se incluye *Crypto-Gram*, la *newsletter* electrónica mensual del mediático autor.

Los textos abordan la seguridad de la información desde variopintas perspectivas, que abarcan tanto las tecnologías y las políticas, como el funcionamiento de la seguridad en el mundo real. En este sentido, realiza diferentes aproximaciones, abarcando tanto aspectos específicos, como las tarjetas de identificación personal nacionales, o la seguridad aérea; como tendencias más genéricas, que prestan

atención al creciente entorno de complejidad o al comportamiento humano. Especialmente en este último punto, el autor subraya la importante interacción entre las tecnologías de seguridad y las personas, y conceptos adyacentes como las economías de la seguridad y la psicología de la seguridad.

El libro estructura el conjunto de los artículos en torno a los siguientes capítulos: **1. Terrorismo y Seguridad; 2. Política de Seguridad Nacional; 3. Desplazamientos en avión; 4. Privacidad y Vigilancia; 5. Tarjetas de Identificación y Seguridad; 6. Seguridad en procesos electorales; 7. Seguridad y Desastres; 8. Economías de la Seguridad; 9. Psicología de la Seguridad; 10. Negocio de la Seguridad; 11. "Ciberdelitos" y "Ciberguerra"; 12. Seguridad de Sistemas y de la Información.**



## APPLIED SECURITY VISUALIZATION

**Autor:** Raffael Marty  
**Editorial:** Addison-Wesley  
**Año:** 2009 – 523 páginas  
**ISBN-13:** 978-0-321-51010-5  
[www.awprofessional.com](http://www.awprofessional.com)

Esta publicación realiza un enfoque directo sobre el presente estado del arte de las técnicas de visualización de la información, a partir de las cuales se puede entender en mayor profundidad lo que ocurre en la red en cada momento. A partir de estas técnicas se pueden descubrir patrones ocultos de los datos, identificar vulnerabilidades y ataques emergentes, y responder con decisión y mediante contramedidas más efectivas que los métodos convencionales.

En este sentido, el libro busca proporcionar de forma didáctica información que permita al lector: comprender las fuentes de información que son esenciales para una visualización efectiva; elegir las técnicas y los gráficos más apropiados para sus datos de TI; transformar datos complejos en representaciones visuales claras; iterar los gráficos para obtener un conocimiento más profundo que ayude en la toma de decisiones; valorar tanto

las amenazas al perímetro de la red como las causadas por el personal interno; utilizar la visualización para gestionar con éxito riesgos y mandatos de cumplimiento; auditar visualmente los aspectos organizativos y técnicos de la información y de la seguridad de red; y comparar y sacar partido de los instrumentos más idóneos para visualizar la seguridad.

Para que el lector pueda asimilar todos estos conocimientos de manera ordenada, han sido distribuidos en los siguientes capítulos: **1. Visualización; 2. Fuentes de Datos; 3. Representar Datos Visualmente; 4. De Datos a Gráficos; 5. Análisis de Seguridad Visual; 6. La Amenaza del Perímetro; 7. Cumplimiento; 8. La Amenaza Interna y 9. Herramientas para Visualizar Datos.** El libro contiene, además, numerosos ejemplos prácticos y viene acompañado por un CD que incluye DAVIX, una recopilación de herramientas gratuitas para visualización de la seguridad.