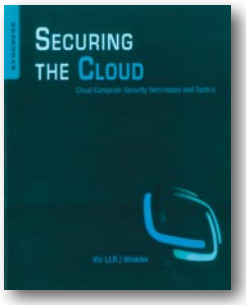
SEGURIDAD POR NIVELES

Autor: Alejandro Corletti Estrada
Editorial: DarFE Learning Consulting
Año: 2011 – 708 páginas
www.darFE.es

Esta obra de más de 700 páginas del prolífico **Alejandro Corletti** desarrolla diversos temas de interés para profundizar en la seguridad de la información desde la perspectiva de los niveles del modelo OSI, presentándolo desde el modelo de capas TCP/IP, e incorporando ejercicios, herramientas y prácticas. El libro, prologado y presentado, respectivamente, por **Arturo Ribagorda Garnacho** y **Jorge Ramió Aguirre**, destacados conocedores y divulgadores del ámbito de la Seguridad TIC en España, está disponible bajo licencia "Copyleft" para su libre descarga y difusión sin fines de lucro.

Su estructura se desarrolla en dos partes: Conceptos y protocolos por niveles; y Seguridad por niveles. En la primera (Capítulos del 1 al 8: "Introducción", "Principios de análisis de la información", "El Nivel Físico", "El Nivel de Enlace", "El Nivel de Red", "El Nivel de Transporte", "El Nivel de Aplicación", y "Algunos conceptos más") se realiza un profundo análisis de los diferentes protocolos de comunicaciones que aplican en cada capa, y se incorporan ejercicios prácticos, herramientas –en su mayor parte de código abierto– y demostraciones para cada una de las temáticas. En la segunda parte se analiza el conjunto de medidas que en ese nivel es conveniente tener en cuenta; y a ella se suman cuatro anexos: "Aspectos a considerar para la certificación de una red", "Consideraciones a tener en cuenta en un CPD", "Política de seguridad", y "Metodología Nessus–snort".

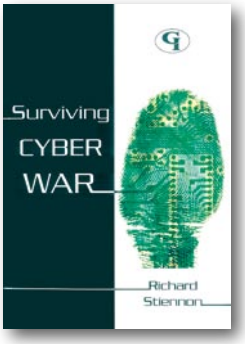


SECURING THE CLOUD Cloud Computer Security Techniques and Tactics

Autor: Vic (J.R.) Winkler
Editorial: Syngress Publications
Año: 2011 – 290 páginas
ISBN: 978-1-59749-592-9
www.syngress.com

Estructurado en 10 capítulos, este volumen aborda la problemática de seguridad que rodea a la masiva implementación de tecnología *cloud*, que, según el autor, puede adolecer de una cierta pérdida de control y falta de confianza en la transición. Después de detallar las grandes fortalezas y ventajas de la protección en la nube, que ofrece flexibilidad, adaptabilidad, escalabilidad y resiliencia, el libro también se acerca a las debilidades que rodean a esta forma de protección corporativa, con ataques que pueden hacer foco en la infraestructura o en las redes de comunicaciones, datos o servicios. El autor propone en este sentido un marco robusto y seguro capaz de proteger los activos de negocio aprovechando al máximo esta tecnología, ya sea en su versión pública, privada, híbrida, *SaaS* o *IaaS*, y poniendo el foco en las consideraciones de seguridad como servicio, el *backup* de los datos y la recuperación ante desastres.

El libro de **Vic (J.R.) Winkler** aborda, a lo largo de su estructura capitular, aspectos como las arquitecturas de *cloud computing*; las cuestiones normativas, de riesgo y seguridad; las mejores prácticas y las estrategias clave; el desarrollo de nubes internas; la selección de proveedores externos; el sistema de seguridad de la información; y la operación de la nube, entre otros.

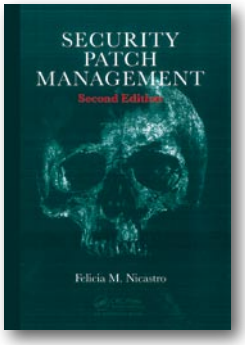


SURVIVING CYBERWAR

Autor: Richard Stiennon
Editorial: Government Institutes
Año: 2010 – 170 páginas
ISBN: 978-1-60590-674-4
www.govinstpress.com

Richard Stiennon, autor del *blog* de seguridad ThreatChaos.com y conocido profesional y analista del sector de la Seguridad TI, examina en este volumen con profundidad los recientes ciberataques que han tenido lugar alrededor del mundo y discute sus implicaciones, ofreciendo soluciones a las vulnerabilidades que hicieron posible esos ataques, explicando cómo prepararse para futuras eventualidades de este tipo. El libro también se acerca a la preparación de los diversos planes de defensa, ya sea para naciones, empresas e, incluso, individuos que busquen optimizar su protección frente a herramientas tan extendidas como el correo electrónico, *blogs*, redes sociales, etc.

Surviving Cyberwar se divide en 15 capítulos y en ellos, entre otras cosas, se acerca a la figura de los analistas de seguridad, como el caso del estadounidense **Shawn Carpenter** y su investigación de la amenaza *Titan Rain*, una de las más invasivas a las que se ha enfrentado Estados Unidos; a las políticas del Pentágono en estos escenarios; a las cambiantes causas de los distintos conflictos; a casos de ataques significativos, como los sufridos en Estonia y Georgia; y a las distintas repercusiones de estas amenazas.



SECURITY PATCH MANAGEMENT

Autora: Felicia M. Nicastro
Editorial: CRC Press
Año: 2011 – 270 páginas
ISBN: 978-1-4398-2499-3
www.crcpress.com

La historia de los códigos secretos o el arte de escribir en clave (criptografía) de la mano de las matemáticas es el objeto de estudio de este libro, que repasa los primeros métodos de cifrado de egipcios y mesopotámicos y se adentra en los secretos de la técnica utilizada por griegos y romanos, verdaderos impulsores del conflicto entre los guardianes del secreto, los criptógrafos, y quienes pretenden desvelarlo, los criptoanalistas. La historia avanza hasta el siglo VIII, donde el sabio árabe al-Kindi descubrió una herramienta de descifrado, el análisis de frecuencias, a la que se respondió siglos más tarde con la codificación mediante la cifra polialfabética. Llegaron después versiones más sofisticadas de criptoanálisis, con las matemáticas como telón de fondo, de la estadística a la aritmética modular, pasando por la teoría de los números; y el gran punto de inflexión se alcanzó con el diseño de las primeras máquinas de codificación y descodificación, y los primeros ordenadores, donde la transmisión de la información ya se basó en un sistema binario de unos y ceros.

Esta obra de divulgación, que se completa con una bibliografía básica y con un índice analítico para facilitar la consulta, intenta acercarse a la seguridad de los mensajes en esta época de virus, piratas informáticos y superordenadores, donde parece que vuelven a ser las matemáticas quienes resuelven el conflicto, gracias esta vez a la idiosincrasia de los números primos.