



SOLDADOS SIN ROSTRO Los servicios de información, espionaje y criptografía en la Guerra Civil española

Autores: José Ramón Soler Fuensanta y Javier López-Brea Espiau
Editorial: Inédita Editores
Año: 2008 – 312 páginas
ISBN: 978-84-92400-04-1
www.inedita-editores.com

La aparición de esta obra constituye, sin duda, todo un hito. A tenor de lo difícil de su alumbramiento vaya por delante un admirado reconocimiento a sus dos autores, **José Ramón Soler y Javier López-Brea**, quienes a buen seguro han debido bregar con tremendos obstáculos para lograr obtener la información que este volumen recoge y, por ende, darle forma e imbricarla en un contexto histórico tan especialmente complejo como fue el de la Guerra Civil que asoló nuestro país.

Concita sumo interés el empeño en reconstruir –en lo posible– el complejo *puzzle* espacio temporal referido a la constitución y funcionamiento de los ser-

vicios de información de ambos bandos (SIFNE, SIM, SIPM, DEDIDE, SIEM, SIDE), que a la postre tendrían desiguales resultados en rendimiento y eficacia.

También el papel desempeñado por la colaboración de los respectivos entes y agentes aliados extranjeros en estas materias fue decisivo, no ya sólo porque ayudaron a la consolidación de los servicios de información de ambos bandos españoles, sino porque además revirtió en su propio beneficio.

Sin duda, la parte más suculenta para los lectores de SIC concernidos con estos temas es la que los autores dedican a la criptografía. Como efectivamente sentencian, España fue el perfecto

conejillo de indias para que las conocidas máquinas Enigma alemanas iniciaran su rodaje, y cuyo descifrado contribuiría pocos años más tarde a los aliados a ganar la segunda guerra mundial. Franco adquirió diez unidades en noviembre de 1936 y fue en este conflicto cuando los británicos ya trataron de romper sus códigos.

Lástima que la ocasión no propiciara la inclusión de contenidos más ‘duros’ en este epígrafe, no obstante lo cual revisten gran interés las muestras expuestas de los venerables métodos de cifrado manual “con papel y lápiz” con que se llevaban a cabo las tareas, así como los ejemplos de algunos éxitos ‘descriptados’, causantes de sonadas modificaciones del devenir bélico.

Lo dicho. Un loable trabajo divulgador de los coautores –especialistas y amantes ambos de la disciplina– en el que de manera ágil arrojan luz sobre la gestación de unos servicios de los que ya ningún país hoy podría prescindir, y por dejar constancia de unos extraordinarios especialistas, parcos en medios pero mentalmente fecundos, en los difíciles inicios de los grupos de escucha, cifra y contracifra que les tocó protagonizar. ■

Luis Fernández Delgado



AUDITORÍA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN

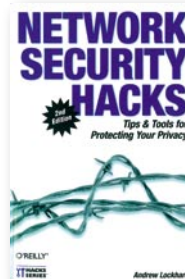
Recopiladores: Mario Piattini Velthuis, Emilio del Peso Navarro y Mar del Peso Ruiz
Editorial: Ra - Ma
Año: 2008 – 692 páginas
ISBN: 978-84-7897-849-6
www.ra-ma.es

En la elaboración de esta obra recopilatoria, que presenta de forma clara y precisa los conceptos fundamentales sobre control interno y auditoría de Tecnologías y Sistemas de Información (TSI), han colaborado más de veinte autores, entre los que figuran profesores de universidad y profesionales de prestigio en este ámbito. La audiencia a la que se dirige es bastante extensa, y no se limita a los profesionales en la materia, sino que incluye a informáticos y economistas que estén trabajando en el área de auditoría, ya sea financiera o de sistemas de información; directivos responsables de la gestión del departamento de TI, de su desarrollo y explotación; consultores informáticos; usuarios avanzados y, en general, cualquiera que tenga interés en adquirir conocimientos sobre la auditoría de TSI.

El texto se divide en dos partes. La primera comienza con la presentación del concepto de auditoría y su relación con el control interno. También se sitúa la auditoría TSI

respecto a las normas de buenas prácticas más difundidas, como COBIT, ITIL, o ISO 17799; se exponen las principales metodologías de control interno; la organización y las funciones del departamento de auditoría de TSI; la deontología del auditor y, finalmente, las principales herramientas a disposición del auditor de TSI para llevar a cabo su cometido.

Los capítulos que conforman la segunda parte analizan las áreas a las que se aplica la auditoría de TSI, empezando con la de *outsourcing*, ya que cada vez mayor número de organizaciones externaliza sus procesos y sistemas de información. Los siguientes capítulos se dedican a la auditoría física, fundamental para la seguridad tanto de las personas, como de los recursos y datos de las organizaciones; la de dirección; la de bases de datos; la de seguridad; la de redes e Internet; la de aplicaciones informáticas; la auditoría de la videovigilancia y la reglamentaria de los datos de carácter personal. ■



NETWORK SECURITY HACKS Tips and Tools for Protecting Your Privacy

Autor: Andrew Lockhart
Editorial: O'Reilly
Año: 2007 – 455 páginas
ISBN-13: 978-0-596-52763-1
www.oreilly.com

Las técnicas que utilizan los intrusos para atacar las redes están en constante evolución, por lo que los instrumentos y métodos empleados para defenderse de ellos también deben actualizarse. En este sentido, la presente obra proporciona ejemplos para detectar la presencia de intrusos, métodos para proteger la red y la información mediante el uso de soluciones de cifrado fuerte, así como acerca de la actual oferta de tecnologías de seguridad y los métodos empleados que permiten obtener información útil sobre lo que está pasando en la red.

En total son 125 las técnicas de seguridad que desgrana su autor, **Andrew Lockhart**, a través de los doce capítulos de que se compone el texto, cuyos epígrafes son: **1. Seguridad para servidores Unix**, en el que se explican técnicas avanzadas para proteger servidores Linux, FreeBSD u OpenBSD; **2. Seguridad para servidores Windows**, que cubre algunos pasos importantes que los administradores de Windows en ocasiones pasan por alto, como auditar la actividad del

sistema o eliminar agujeros de seguridad presentes en la instalación de Windows por defecto; **3. Privacidad y anonimato**, un capítulo que expone varias maneras de auto-protegerse *online*, como cifrar el correo-e o establecer contraseñas de acceso a sitios web; **4. Instalación de cortafuegos**; **5. Cifrado y seguridad de servicios**; **6. Seguridad de red**, que desvela algunas herramientas y técnicas empleadas para atacar servidores empleando la red, así como la forma de evitarlos; **7. Seguridad inalámbrica**; **8. Logging**, que enseña a crear claves de acceso de calidad; **9. Monitorización y definición de tendencias**, que presenta la forma de establecer patrones para ayudar a detectar que algo no marcha bien; **10. Túneles seguros**, que ilustra sobre cómo desarrollar VPNs y técnicas para proteger los servicios usando SSL, SSH u otros instrumentos de cifrado fuerte; **11. Detección de intrusos**, dedicado a la herramienta *Snort* y a cómo aprovechar todo su potencial; y **12. Respuesta y recuperación tras incidentes**. ■