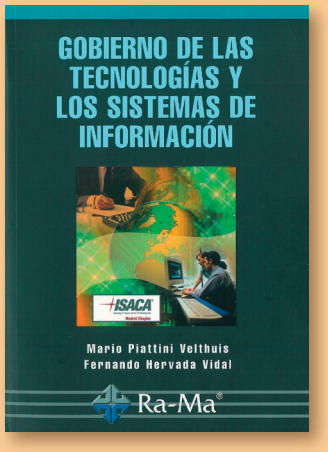


GOBIERNO DE LAS TECNOLOGÍAS Y LOS SISTEMAS DE INFORMACIÓN

Autores: J. Álvarez, M. A. Amutio, Mª M. Arcilla, D. Cabrero, E. Del Peso, L. Díaz, C.M. Fernández, E. Fernández-Medina, F. Hervada, P. López, J. Garzás, S. Gómez, P. Llaneza, R. López, J. A. Mañas, M. Mendiola, M. Piattini, L. Prats, A. Ramos, A. Rembado, S. Romero, J. Romo, L.E. Sánchez, M.Touriño y D. Villafranca
Editorial: RA-MA / Año 2007 – 456 páginas / ISBN: 978-84-7897-767-3
www.ra-ma.es

Ya era hora de que en España se dispusiera de un libro como el que a continuación se reseña. Dos expertos académicos y profesionales, **Mario Piattini**, CISA y CISM, Catedrático de Lenguajes y Sistemas Informáticos de la ESP de la Universidad de Castilla-La Mancha, donde dirige el grupo Alarcos, especializado en Calidad y Seguridad de Sistemas de Información; y **Fernando Hervada**, CISA, miembro fundador y anterior presidente de ASIA, (capítulo de Madrid de la ISACA) y actual director de la Unidad de Auditoría de Sistemas de Información de Endesa, han sido los principales instigadores para dar curso a este compendio de aportaciones propias y de otros 23 autores con el objetivo de ayudar a proporcionar a los profesionales concernidos una correcta metodología de control sobre la gobernabilidad de las TI, soportada en argumentos teóricos, buenas prácticas y resoluciones acertadas.

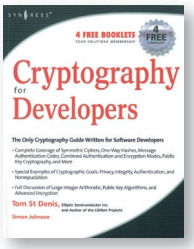
Bajo la impronta de la hoy muy activa Asociación de Auditores y Auditoría y Control de los Sistemas y Tecnologías de la Información (ASIA), este volumen aboga por el uso de una metodología de este tipo para el desempeño eficaz y eficiente de la gestión sobre los sistemas de información, que permitirá que el ejercicio de control interno (funciones de auditoría interna, intervención, inspecciones, control de gestión y seguridad) se aplique de forma profesional, clara, medible y comparable.

Estructurada en dieciocho capítulos agrupados en dos partes, la obra recoge diferentes aspectos relacionados con el gobierno de las Tecnologías y los Sistemas de Información (TSI), por lo que se ofrece una visión amplia sobre diferentes factores que se deben tener en consideración para la implantación y mejora del gobierno de las TSI, abordando los conceptos fundamentales relacionados con esta materia; analizando áreas importantes como son los recursos humanos, la gestión de riesgos, la gestión de recursos, o los aspectos jurídicos; y dando a conocer los diferentes estándares, normas y modelos aplicables. Globalmente, la mayoría de las aportaciones son de gran calidad aunque, todo hay que decirlo, algunos capítulos conforman un auténtico recital del 'buen conocimiento' y se erigen en inexcusable faro de referencia.

En la primera parte, que consta de nueve capítulos, se ofrece una visión general sobre los conceptos, las técnicas y los elementos de gobierno de las TSI. Sus firmantes contribuyen en su gran mayoría con aportaciones rigurosas y reflexivas. Los epígrafes que conforman la misma son los que siguen: 1. **El Gobierno de las Tecnologías y Sistemas de Información**, 2. **Técnicas y Planificación para el Gobierno de TSI**, 3. **El Valor y el Retorno de la Inversión de las TSI**, 4. **Aspectos Jurídicos**, 5. **Visión General del Gobierno de la Seguridad**, 6. **Implantación del Gobierno de la Seguridad de las TSI**, 7. **Gestión de Riesgos de Seguridad**, 8. **Cuadro de Mando para el Gobierno de TSI**, 9. **Modelos de Madurez para SGSI desde un Enfoque Práctico**.

Por su parte, la segunda sección del volumen de Ra-Ma aporta abundantes capítulos cuyos autores brillan a gran altura abordando los estándares, normas y modelos aplicables al gobierno de TSI: 10. **Panorámica General sobre Normas de Seguridad de TI**, 11. **Norma ISO 27001.- Gestión de la Seguridad**, 12. **Las Métricas de Seguridad de la Información**, 13. **Norma ISO 17799. Código de Buenas Prácticas para los SGSI**, 14. **COSO**, 15. **COBIT 4**, 16. **ITIL y La norma UNE-ISO/IEC 20000**, 17. **Sarbanes-Oxley**, 18. **Basilea II: Reto y Oportunidad para la Auditoría de Sistemas**.

Es pretensión de los autores que la obra, patrocinada por Telefónica y S21sec, suscite el interés de directores generales (CEO), directores de informática (CIO), y directores de seguridad de los sistemas de información (CISO), auditores, especialistas en seguridad y control de sistemas de información, así como profesionales del departamento de informática en general que estén trabajando en el área de desarrollo de sistemas de información. A tenor de su contenido, altamente recomendable –cuando no imprescindible–, esta obra coral está destinada a erigirse en referencia clásica de una moderna comprensión del gobierno TSI. ■ **SIC**

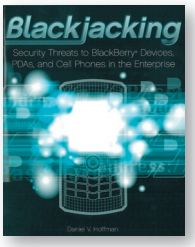


CRYPTOGRAPHY FOR DEVELOPERS

Autores: Tom St Denis y Simon Johnson
Editorial: Syngress
Año 2007 – 423 páginas
ISBN: 978-1-59749-104-4
www.syngress.com

El presente texto tiene como objetivo guiar a los desarrolladores, habitualmente no especialistas en la materia, en la resolución de problemas criptográficos que se les pueden plantear a la hora de implementar criptosistemas. El autor, un reconocido desarrollador de software y autor de la serie de librerías públicas sobre cifrado LibTom, ha planificado este manual de una forma práctica, incluyendo las suficientes referencias técnicas y académicas, pero omitiendo algunos puntos sobre la materia excesivamente especializados, y remitiendo para ello a otros volúmenes bien conocidos como *Handbook of Applied Cryptography* o *Foundations of Cryptography*, ya glosados en SIC.

Así, el libro comienza con un capítulo introductorio sobre criptografía, que da paso a un conjunto de otros ocho en los que individualmente se tratan diferentes categorías de problemas y se tratan las respectivas áreas de esta disciplina. De este modo, el índice capitular es el siguiente: 2. **Codificación de ASN.1**, 3. **Generación de números aleatorios**, 4. **Estándares de cifrado avanzado**, 5. **Funciones *Hash***, 6. **Algoritmos de código de autenticación de mensajes**, 7. **Modos de autenticación y cifrado**, 8. **Aritmética de números enteros grandes**, y 9. **Algoritmos de Clave Pública**.■



BLACKJACKING. Security Threats to BlackBerry Devices, PDAs, and Cell Phones in the Enterprise

Autor: Daniel V. Hoffman
Editorial: Wiley
Año 2007 – 292 páginas
ISBN: 978-0-470-12754-4
www.wiley.com

Aunque tradicionalmente la seguridad de los dispositivos móviles no ha sido del todo prioritaria para las compañías a pesar de tratarse de terminales portátiles con información crítica corporativa y de clientes, este escenario sin duda está cambiando. En un momento en el que el Gobierno francés ha reiterado el veto en el uso de la Blackberry entre sus miembros y altos funcionarios del Estado ante el "riesgo real" de interceptación de información confidencial a cargo de terceros (apuntándose directamente a la Agencia de Seguridad Nacional norteamericana), el autor de este libro, **Daniel V. Hoffman,** un *hacker* ético certificado CISSP, CEH y CWNA, realiza un análisis sobre las técnicas de *blackjacking*, término que hace referencia al secuestro y ataque de dispositivos Blackberry, agendas electrónicas y teléfonos inteligentes.

En este sentido, la primera parte del volumen se dedica a proporcionar los fundamentos para entender las amenazas a estos dispositivos y los terminales en sí, así como los cambios en la estrategia de seguridad corporativa que deberían implementarse. La segunda parte se centra en concreto en los dispositivos BlackBerry y en las amenazas dirigidas a los mismos, así como los *exploits* más comunes, y aborda de forma detallada la protección de estos dispositivos. Finalmente, la tercera y cuarta parte del libro disponen de una estructura temática similar a la segunda, pero aproximándose esta vez al uso de las PDAs y los teléfonos móviles. ■