



LA PROTECCIÓN DE DATOS EN LOS CENTROS DE ENSEÑANZA Recomendaciones para cumplir el régimen jurídico

Autores: Antonio Sánchez-Crespo y Elena Pérez Gómez
Editorial: Aranzadi
Año: 2008 – 460 páginas
ISBN: 978-84-8355-305-3

Esta es una obra concebida para promover, entre los centros de enseñanza, la cultura de la protección de los datos de carácter personal; para que todas las personas que trabajan en ellos dominen cuestiones como cuáles son las implicaciones del principio de seguridad o en qué consisten los derechos de acceso, rectificación, cancelación y oposición.

En su edición ha participado Sánchez-Crespo Abogados y consultores, y sus autores, **Antonio Sánchez-Crespo López** y **Elena Pérez Gómez**, son dos reputados consultores jurídicos que han plasmado en estas páginas los conocimientos adquiridos en más de cuarenta auditorías de centros de enseñanza de diversos niveles educativos, tamaños y Comunidades Autónomas; complementando así,

con un punto de vista práctico, las recomendaciones que la Agencia Española de Protección de Datos ha lanzado al sector en su Plan Sectorial de Oficio a la Enseñanza Reglada No Universitaria.

Es asimismo destacable que la autora del prólogo, **Rosa M^a García Ontoso**, ejerció como Directora de la Agencia de Protección de Datos de la Comunidad de Madrid entre 1997 y 2001, y asegura en el mismo que *“habremos conseguido extender la cultura de la protección de datos cuando seamos capaces de formar a los niños, enseñándoles a no dar sus datos de carácter personal cuando se les soliciten, y tengamos todos en cuenta que los mismos hay que pedirlos a los padres o tutores”*. ■



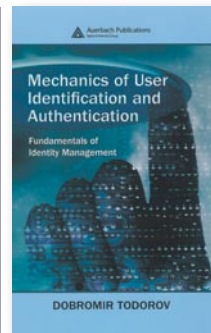
MANUAL DE BUENAS PRÁCTICAS 2007 Guía para instaurar Buenas Prácticas Globales en Gestión de Continuidad de Negocio

Autor: The Business Continuity Institute (BCI)
Editorial: ISMS Forum Spain, Asociación Española para el Fomento de la Seguridad de la Información
Año: 2007 – 114 páginas
www.ismsforum.es

Inspirado en las experiencias académicas, técnicas y empíricas de los miembros del Business Continuity Institute (BCI), y a instancias del ISMS Forum español, el presente manual ofrece, en castellano, una visión general de las buenas prácticas en lo que se refiere al ciclo de vida de la Gestión de Continuidad de Negocio (GCN), desde el reconocimiento inicial de la necesidad de desarrollar el programa, hasta el mantenimiento constante de un proceso maduro del mismo. Por tanto, está dirigido a gestores de riesgo, auditores y legisladores con conocimiento práctico de los principios de GCN, y no se considera una guía para debutantes.

El manual se basa en la edición del mismo de 2005, aunque en ésta,

su más reciente versión, apoya el lanzamiento del BS 25999-1 A *Code of Practice for Business Continuity Management* (Código de Buenas Prácticas para la Gestión de Continuidad de Negocio) de la British Standards Institution (BSI), y puede considerarse una guía para la puesta en práctica del mismo. No obstante, como existen otros estándares en vigor que muchos profesionales necesitan entender, la edición de 2007 también tiene en cuenta los requisitos de NFPA1600 (Estados Unidos y Canadá), HB221 (Australia), APS 232 (Australia) y FSA (Reino Unido). En cuanto a la estructura de la obra, los seis capítulos que la componen se corresponden con las versiones anteriores y también con la nomenclatura BS25999. ■



MECHANICS OF USER IDENTIFICATION AND AUTHENTICATION Fundamentals of Identity Management

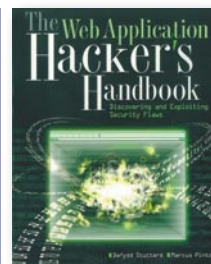
Autor: Dobromir Todorov
Editorial: Auerbach Publications
Año: 2007 – 728 páginas
ISBN: 978-1-4200-5219
www.auerbach-publications.com

El presente volumen informa en profundidad sobre algo tan esencial para la seguridad de la información como es la identificación y la autenticación de usuarios, aspecto que, según el autor del texto, **Dobromir Todorov**, era necesario, debido a la escasez de obras existentes sobre la materia, y a que la mayoría de ellas no están estructuradas, lo que a veces desemboca en malentendidos que perjudican tanto a los usuarios finales como a los profesionales de la seguridad. *Mechanics of User Identification and Authentication* incluye también numerosos casos prácticos, diagramas y capturas de pantalla que muestran el funcionamiento interno de diferentes tecnologías y mecanismos de autenticación.

La información que contiene el texto se reparte en cinco bloques. El primero de ellos, **Conceptos de Autenticación e Identificación de Usuarios**, presenta cómo es el panorama de la seguridad

actualmente y cuáles son las amenazas específicas para la autenticación de usuarios; también incluye una correcta introducción a la criptografía con los conceptos y términos necesarios para comprender cómo funciona la autenticación de usuarios.

Por su parte, los capítulos 2, **Arquitectura de identificación de usuarios UNIX** y 3, **Arquitectura de Identificación de Usuarios Windows**, proporcionan un nivel considerable de conocimiento técnico sobre todos los aspectos de la autenticación de usuarios en los dos sistemas operativos más populares actualmente. Finalmente, los capítulos cuatro y cinco, titulados respectivamente **Autenticación de Accesos a Servidores y Aplicaciones** y **Autenticación de Acceso a la Infraestructura**, familiarizan al lector con los diseños y desarrollos de diferentes protocolos de autenticación de usuarios. ■



THE WEB APPLICATION HACKER'S HANDBOOK Discovering and Exploiting Security Flaws

Autores: Dafydd Stuttard y Marcus Pinto
Editorial: Wiley
Año: 2008 – 727 páginas
ISBN: 978-0-470-17077-9
www.wiley.com

Como su propio nombre indica, esta obra es una guía práctica para descubrir cómo se explotan los fallos de seguridad en las aplicaciones web, por lo que este volumen se orienta a todos aquellos interesados en averiguar las prácticas usuales que se llevan a cabo para *hackear* una aplicación web a fin de robar datos sensibles. Es un libro de gran utilidad para profesionales responsables del desarrollo y administración de aplicaciones web, puesto que, como en la introducción dicen sus autores, **Dafydd Stuttard** y **Marcus Pinto**, la mejor manera de defenderse del

enemigo es saber cómo opera.

El denso manual se compone de 20 capítulos, cuyos tres primeros, de carácter introductorio, describen el estado actual de la seguridad de las aplicaciones web y las tendencias que indican la evolución que se espera seguirán en el futuro. No obstante, el grueso del texto gira en torno a las tareas clave que hay que realizar para llevar a cabo un *hackeo*, desde el rastreo de la funcionalidad de las aplicaciones, atacando el corazón de sus mecanismos defensivos, hasta la búsqueda metódica de fallos en seguridad. ■