



EL PLAN DE CONTINUIDAD DE NEGOCIO

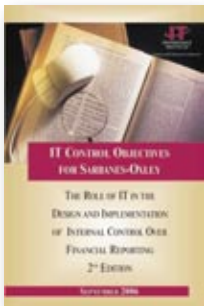
Guía práctica para su elaboración

Autor: Juan Gaspar Martínez
 Editorial: Díaz de Santos
 (Incluye CD-Rom)
 Año 2006 – 224 páginas
 ISBN: 84-7978-778-3
www.diazdesantos.es/ediciones

Juan Gaspar Martínez, experto profesional donde los haya –no en vano acumula un pedigrí de más de 23 años en diversos ramos de la seguridad–, es el autor de esta guía que presenta un esquema de trabajo sencillo para elaborar un plan de continuidad de negocio en las organizaciones. Para ello, el volumen no sólo pretende que el responsable de la elaboración del plan realice el planteamiento, sino que además asuma el comienzo y desarrollo de mismo, para lo cual la obra incluye un útil CD que proporciona impresos y modelos prediseñados para poder llevarlo adelante.

La secuencia de sus 11 capítulos plantea los objetivos que debe tener un plan de continuidad de negocio y sus definiciones previas para, posteriormente, abordar el análisis de su

impacto en la organización. También trata los elementos críticos de este plan de negocio en función del impacto que sufrirían las diferentes áreas de una organización, determinando qué funciones deberían ser atendidas en primer lugar. Otros temas abordados son: la estrategia de continuidad, en función de las características de cada empresa y de su grado de criticidad; los equipos o grupos de personas que se encargan de las actividades para conseguir un proceso de recuperación efectivo; y el plan de acción a seguir si se produce un desastre, así como la vuelta a la normalidad una vez solventado. Lástima que cuando este libro vio la luz aún no se oteaba en el horizonte el advenimiento del pre-estándar BS 25999 sobre gestión de continuidad de negocio, destinado a ser guía nuclear en estas lides. ■



IT CONTROL OBJECTIVES FOR SARBANES-OXLEY

The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting 2nd Edition

Editorial: IT Governance Institute
 Año 2006 – 128 páginas
 ISBN: 1-933284-76-5
www.itgi.org

En abril de 2004, el IT Governance Institute (ITGI) publicó la primera edición de *IT Control Objectives for Sarbanes-Oxley* (SOX), que proporcionaba a los CIOs, responsables de TI y profesionales de control y seguridad asesoramiento, aproximaciones y orientación para el soporte de controles objetivos internos relacionados con las TI para el reporte financiero.

Desde entonces, esta obra ha sido ampliamente utilizada por empresas de todo el mundo, y dado que durante este tiempo también se ha avanzado en el aprendizaje sobre estas cuestiones y sobre la necesidad de un acercamiento a los programas de cumplimiento de SOX basados en el riesgo, el ITGI ha decidido revisar y actualizar la obra

proporcionando orientación adicional en áreas de mayor importancia para el control interno sobre la información financiera, tras las modificaciones de la SEC (*Securities and Exchange Commission*) y PCAOB (*Public Company Accounting Oversight Board*) relativas a los controles a nivel de entidad, un acercamiento basado en el riesgo y la aplicación de controles y evaluación de deficiencias, además de aportar las lecciones aprendidas sobre el cumplimiento de TI con la SOX. La obra incluye, además, un sumario de casos prácticos para compartir las experiencias del cumplimiento de empresas mundiales, indicando los pasos para la obtención de beneficios o evitar los fallos más comunes. ■



ENCICLOPEDIA DE LA SEGURIDAD INFORMÁTICA

Autor: Álvaro Gómez Vieites
 Editorial: Ra-Ma
 Año 2006 – 664 páginas
 (Incluye CD-Rom)
 ISBN: 84-7897-731-7
www.ra-ma.es

Este libro pretende abordar desde un punto de vista global la problemática de la seguridad de la información, aglutinando los aspectos técnicos, organizativos y el entorno legal, de ahí que vaya dirigido a un público muy diverso. Las 7 partes en las que está dividida la obra y sus 28 capítulos dan una idea de lo extenso de la misma, recogiendo el testigo de no pocos libros similares anteriormente publicados, centrados en adicionar sucesivamente los diferentes segmentos que conforman este epígrafe de la protección TI.

La primera parte indaga en aspectos básicos como qué se entiende por seguridad informática, consecuencias de su falta, la detección y respuesta ante incidentes o la ingeniería social. En la segunda, se estudian las vulnerabilidades de los sistemas y las redes y en la tercera se

abordan los aspectos relacionados con la identificación y autenticación de los usuarios. El cuarto y quinto bloque abundan, respectivamente, en los sistemas y técnicas criptográficas, como la firma electrónica, y en los aspectos técnicos para implantar medidas de seguridad en las redes de ordenadores, analizando el papel de los cortafuegos o los sistemas de detección de intrusos (IDS). Los aspectos relacionados con la seguridad en la navegación en páginas web y correo-e son tratados en la sexta parte, mientras que la última se centra en los asuntos relacionados con el entorno legal y normativo que afectan a la seguridad informática. Todos estos temas, se completan con guías prácticas y contenidos técnicos que se ofrecen en el CD que incluye la obra. Por cierto, ¿todavía a estas alturas alguien sigue poniendo 'encriptación'? ■



PROFESSIONAL PEN TESTING FOR WEB APPLICATIONS

Autor: Andres Andreu
 Editorial: Wiley
 Año 2006 – 522 páginas
 ISBN: 0-471-78966-6
www.wrox.com

Como es sabido, las pruebas de penetración sirven para alcanzar un equilibrio que permita al sistema estar adecuadamente protegido sin dejar de ser totalmente funcional. Este manual, eminentemente técnico, proporciona la información suficiente para que el lector pueda convertirse en un perfecto simulador de ataques con el fin de burlar las características de seguridad de una aplicación web, de forma que esas características puedan ser evaluadas con precisión y se puedan establecer las precauciones de seguridad adecuadas.

A lo largo de sus 11 capítulos y 4 apéndices *Professional Pen Testing*

muestra las técnicas de vigilancia que un *hacker* usa cuando apunta hacia un sistema para atacarlo; cómo auditar los servicios web para evaluar las áreas de mayor exposición y riesgo; cómo analizar los resultados y traducirlos a documentación útil para poner remedio; o técnicas para realizar prácticas de ataques antes de llevar a cabo un proyecto real. Dada la complejidad y minuciosidad de los asuntos tratados, la obra se dirige particularmente a programadores, desarrolladores web y profesionales de la seguridad informática que quieran empezar a familiarizarse con la seguridad de las aplicaciones web y saber cómo auditarla. ■