

## MERGERS AND ACQUISITIONS SECURITY. CORPORATE RESTRUCTURING AND SECURITY MANAGEMENT

**Autores:** Edwar P. Halibozek, Dr. Gerald L. Kovacich  
**Editorial:** Elsevier. Año 2005 - 250 pág.  
**ISBN:** 0-7506-7805-4  
[www.elsevier.com](http://www.elsevier.com)

Centrado en el papel vital que juega la seguridad como elemento facilitador y de éxito de los procesos de fusión, adquisición o disgregación, el libro presenta los elementos de seguridad fundamentales que se requieren para respaldar los objetivos corporativos. Se parte de la idea de que, con frecuencia, los rápidos cambios que acompañan a estas operaciones tienen como consecuencia un aumento del riesgo, motivado por nuevas oportunidades de fraude, robo o venta de información confidencial, así como de otros activos de la empresa.

En este sentido, las directrices propuestas proporcionan una aproximación integrada sobre cómo implementar la seguridad en el desarrollo de estos movimientos estratégicos, complementándose con métodos y procesos que se pueden poner en marcha de forma inmediata y eficaz.

Las secciones y capítulos en que se enmarca el contenido de esta atinada obra son los siguientes:

**Sección I: Una introducción a las fusiones y adquisiciones. Capítulo 1: ¿Qué son las fusiones y adquisiciones? Capítulo 2: El actual entorno global de negocio: ¿se producen las adquisiciones y fusiones de forma dinámica? Capítulo 3: El papel de la Seguridad y del Responsable de Seguridad en las fusiones y adquisiciones. Sección II: Soporte previo a los procesos de fusión y adquisición. Capítulo 4: Recopilación de información y Producción de inteligencia competitiva. Capítulo 5: El porqué del soporte previo a las fusiones y adquisiciones. Capítulo 6: El papel de la Seguridad en la evaluación Due-Diligence. Sección III: Soporte posterior a las operaciones de fusión y adquisición. Capítulo 8: Soporte posterior a largo plazo de la fusión. Capítulo 9: Desposeimiento. Capítulo 10: Sumario de fusiones, adquisiciones y cambio de propiedad mediante listas de comprobación. ■**



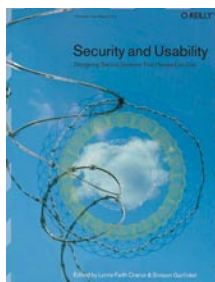
## DATA PROTECTION AND INFORMATION LIFECYCLE MANAGEMENT

**Autor:** Tom Petrocelli  
**Editorial:** Prentice Hall  
**Año 2006** – 256 páginas  
**ISBN:** 0-13-192757-4  
[www.phptr.com](http://www.phptr.com)

A modo de guía para la protección de los activos de información en la empresa, el presente volumen hace un recorrido por la tecnología, las técnicas, estrategias y mejores prácticas que se emplean en la actualidad para la salvaguardia de datos. En este sentido, el autor realiza una aproximación progresiva respecto a la protección de datos, comenzando por los aspectos más básicos, hacia otros más complejos en los que además presenta casos reales en los que distintos profesionales de las TI explican las metodologías empleadas para resolver problemas

que se pueden generar a la hora de proteger información crítica.

El índice capitular del libro es el siguiente: **1. Introducción a la protección de datos, 2. Una perspectiva general sobre la tecnología de almacenamiento, 3. Backup y recuperación, 4. Copia remota y replicación: Traslado de los datos a una localización segura, 5. Conceptos básicos de seguridad, 6. Seguridad de los sistemas de almacenamiento, 7. Protección de datos basada en políticas, y 8. Gestión del ciclo de vida de la información. ■**



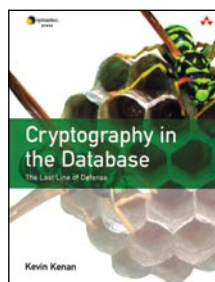
## SECURITY AND USABILITY. DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE

**Autores:** Lorrie Faith Cranor, Simson Garfinkel  
**Editorial:** O'Reilly  
**Año 2005** – 715 páginas  
**ISBN:** 0-596-00827-9  
[www.oreilly.com](http://www.oreilly.com)

Los coautores de este libro parten de la idea, extendida entre muchos profesionales, de que la seguridad y el uso funcional de los ordenadores son conceptos frecuentemente antagónicos. Bajo esta premisa, y el acuerdo generalizado entre los profesionales de la seguridad de la necesidad de diseñar sistemas seguros de fácil uso, se proponen a lo largo de los 34 capítulos de esta obra diversos casos prácticos para el diseño de sistemas robustos, expuestos por destacados investigadores y profesionales del ámbito de la seguridad TIC.

Algunos de los temas abordados en sus aportaciones son los que siguen: Cómo realinear y progresar en la seguridad y la funcionalidad mediante un atento cuidado a los principios de diseño

centrados en el usuario; una mirada en profundidad en los mecanismos para identificar y autenticar a los usuarios en sistemas tanto locales como remotos; un examen sobre los sistemas seguros (diseño de interfaces de usuario seguro, anti-phishing, PKI funcional, seguridad compartimentada y análisis etnográfico); sistemas de privacidad y anonimato (dificultades en el diseño de sistemas de privacidad, la Plataforma para las Preferencias de Privacidad (P3P), web bugs, consentimiento expreso en Internet, y aproximaciones sociales a la seguridad, entre otros); y experiencias de fabricantes como Microsoft, IBM/Lotus, Firefox, Zone Labs y Groove Networks a la hora de afrontar los retos de la "usabilidad". ■



## CRYPTOGRAPHY IN THE DATABASE. THE LAST LINE OF DEFENSE

**Autor:** Kevin Kenan  
**Editorial:** Addison-Wesley  
**Colección:** Symantec Press  
**Año 2006** – 277 páginas  
**ISBN:** 0-321-32073-5  
[www.awprofessional.com](http://www.awprofessional.com)

**Kevin Kenan**, autor de esta publicación, y responsable de Programación de Seguridad de Bases de Datos y Aplicaciones de TI dentro de Symantec, vuelca su conocimiento y experiencia profesional en este libro, acercando a los lectores el uso de la criptografía en las bases de datos y las aplicaciones como medida de protección de la información corporativa. Para ello, se presenta un modelo para el diseño y la ejecución (o la selección e integración) de un criptosistema para la protección de las bases de datos frente a

amenazas identificadas.

Organizado en cuatro grandes segmentos, el primero de ellos se dedica a la seguridad avanzada de bases de datos, el segundo detalla el diseño del criptosistema, el tercero pone énfasis en el desarrollo de las prácticas necesarias para implementar el criptosistema de forma segura, y el segmento final proporciona prácticos ejemplos con cerca de 3.000 líneas de código de libre descarga, para el diseño del mismo, incluyendo *key vaults*, administradores, patentes, motores y proveedores. ■