



SEGURIDAD DE LA INFORMACIÓN Redes, informática y sistemas de información

Autor: Javier Areitio Bertolín
Editorial: Paraninfo
Año 2008 – 592 páginas
ISBN: 8497325028 - **EAN:** 9788497325028
www.thomsonparaninfo.com

Se suele afirmar que cada vez sabemos más y más de menos y menos, lo que por inferencia nos aboca a pensar que asintóticamente llegaremos a saber todo de nada. Efectivamente, desde el Renacimiento la Humanidad no ha vuelto a tener personajes de conocimiento enciclopédico; y no obstante ser esto inevitable en cierta medida, no es menos cierto que sus efectos empezaban a ser devastadores para el progreso de la ciencia y de la técnica. Todo ello no es nuevo, y ya nuestro filósofo José Ortega y Gasset lo denunció clarívidamente en su magnífico opúsculo “La Barbarie del «especialismo»” comprendido en su obra “La Rebelión de las Masas”. Resumiendo su tesis en un único párrafo extraído de la misma: el especialista “sabe” muy bien su mínimo rincón del universo; pero ignora de raíz todo el resto (sic).

Esta tendencia se acusa también en el propósito de la mayor parte de los libros publicados hoy en día que tratan, principalmente los escritos en lengua inglesa, de temas ultra especializados. El ejemplo extremo lo tenemos en las obras compiladas por un editor experto en una materia y consistentes en un compendio de capítulos monográficos escritos por varios super especialistas, consagrados cada uno a un átomo de conocimiento.

Viene todo ello a propósito de los, proporcionalmente, escasos títulos de libros versados en nuestra disciplina de la seguridad que tienen vocación omnicompreensiva. Ciertamente esto no ocurre en las obras escritas en nuestra lengua donde las más especializadas abarcan un amplio campo de nuestra materia. Sin deseo de ser exhaustivo en las citas, es el caso –en la criptografía–, del magnífico y profundo: *Criptografía Digital. Fundamentos y Aplicaciones* (Pastor, J y Sarasa, M. A. Colección Textos Docentes. Zaragoza, 1998) o del más breve pero no menos interesante: *Introducción a la Criptografía* (Caballero Gil, P. Ra-Ma. Textos Universitarios, 1996), o –en redes e internet– del imprescindible: *Seguridad en Redes Telemáticas* (Carracedo, J.), o –en planes de contingencia– del muy profesional *Planes de contingencia. La continuidad del negocio en las organizaciones*. (Gaspar, J. Díaz de Santos. 2004), etc. Todos ellos de inexcusable referencia para todos los que escribimos en español.

Sin embargo, se echaba en falta algún libro actual que comprendiera varias áreas de la seguridad, algo que no ocurría desde el lejano 1994 (*Seguridad y Protección de la Información*. Morant, J. L. et al. Editorial Centro de Estudios Ramón Areces, 1993. 1ª reimpresión 1997) y este es el hueco que viene a llenar el libro que ahora reseñamos: *Seguridad de la Información. Redes, Informática y Sistemas de Información*, escrito por el profesor Javier Areitio y publicado este año por Paraninfo. Aunque sólo fuera por esta intención globalizadora, y no lo es, ya

merecería que nos felicitáramos por la aparición de esta obra y agradeceríamos a su autor el esfuerzo, a todas luces ímprobo, de su elaboración.

Como se acaba de comentar, el texto pretende compendiar casi todos los ámbitos de la seguridad, desde los aspectos de gestión hasta los técnicos, incluyendo una breve incursión por el campo legal. Pero es probablemente no ya este afán de tratar casi todas las facetas, sino sobre todo de agotar cada una de ellas, lo que hace que a veces algunos elementos de la seguridad se vean en más de un capítulo o sección y, lo que es peor, en ocasiones, bien es cierto que escasas, se describan tan ampliamente que resulten algo confusos.

Con todo, y seguramente para hacer el volumen manejable, olvida algunos temas, como la seguridad física, cuyos aspectos de protección frente a radiaciones radioeléctricas (protección Tempest), así como frente a sustracciones o discontinuidades del suministro eléctrico (por no citar las manidas contramedidas frente a incendios o inundaciones) merecen una redoblada atención debido en gran parte al interés que suscita la defensa de las infraestructuras críticas.

En todo caso, lo primero que destaca es la secuencia de los capítulos, que partiendo de los dedicados a la gestión (análisis y gestión de riesgos, ataques a los sistemas, sistemas de gestión de la seguridad, contingencias) sigue con los centrados en las técnicas de la seguridad para concluir con dos capítulos de exposición de los sistemas criptográficos simétricos y asimétricos. Ello hace que en la mayor parte de los temas nos encontremos con términos y conceptos criptográficos aún no definidos, y mucho menos tratados, lo que se intenta soslayar con notas a pie de página o incisos en el desarrollo de los apartados donde esto ocurre. Aunque ello no plantee mayor problema a los versados en la materia puede suponer un obstáculo a los neófitos en ella. Como no cabe duda de que esta estructuración tan poco habitual debe de tener algún motivo, hubiese sido deseable haberlo manifestado en el “Prólogo” del libro.

Estas mismas dificultades debidas a la ordenación de la obra se reflejan en una de las facetas más elogiadas del libro, los epígrafes que con el nombre de “cuestiones y preguntas” y “problemas resueltos” dan fin a cada uno de los capítulos. Todos estos epígrafes, incluso los ubicados en los capítulos de gestión (como se ha dicho situados al principio del libro), incluyen ejercicios criptográficos muy elaborados y de cierta complejidad de resolución, cuya inclusión en estos capítulos no se alcanza a entender.

Igualmente, es chocante que el capítulo III, que estudia el control de accesos, se coloque entre los que exponen aspectos de gestión, cuando su posición lógica, al menos aparentemente, hubiese sido junto con los más técnicos.

Entrando en el fondo de la obra, comienza la misma con un capítulo (“Fundamentos de la seguridad de la información”) en el que, como su nombre sugiere, se introducen tanto las facetas administrativas y de organización como las técnicas que se irán desarrollando a lo largo de la obra. El capítulo II (“Análisis y Gestión de Riesgos”) es uno de los más extensos, lo que le permite tratar el tema desde diversos puntos de vista y todos con gran amplitud. El III (“Control de accesos: autenticación, autorización y cumplimiento”), estudia muy correcta y extensamente dichos controles, ahondando en los estándares correspondientes, el protocolo Kerberos y brevemente la triple A. Sin embargo, extraña la casi nula atención prestada a la autenticación de usuarios, a pesar de lo que se puede inferir en el título. En efecto, casi ni se tratan las contraseñas, y nada los sistemas biométricos, ni los basados en reto respuesta mediante la firma digital.

El capítulo IV (“Análisis de ataques a los sistemas de información”), se centra exclusivamente en los ataques de DoS, destacando favorablemente la inclusión de varios apartados acerca de la interesante técnica de los árboles de ataque. El V (“Sistemas de gestión de la seguridad de la información”) sobresale por su exposición de los cuadros de mando y de los modelos de madurez, ambos aspectos muy poco presentes, a pesar de su importancia, en los manuales al uso. El VI (“Planificación de contingencias y continuidad del negocio”), descuellan por su tratamiento exhaustivo de los distintos tipos de contingencia incluyendo las que pueden afectar a los sitios *web*.

Los aspectos legales y otros conexos se presentan en el capítulo VII (“Cumplimiento con las leyes. Privacidad y anonimato. Servicios de investigación y responsabilidad”), aunque proporcionalmente al resto de los temas se presta muy poca atención a los legales, a los que se dedican sólo 10 páginas, atendiendo mucho más a las técnicas de la informática forense, que tanto auge están experimentando en los últimos años.

El último bloque, estrictamente técnico, se extiende por los capítulos VIII (“Tecnologías de seguridad”), IX (“Criptografía simétrica”) y X (“Criptografía asimétrica”). En el primero, se exponen un gran número de tecnologías: cortafuegos, IDS, señuelos, PKI,... destacando positivamente entre todos los sistemas IBC (*Identity Based Cryptography*), raramente hallados hasta ahora en la bibliografía más común. Por lo que respecta a los dos últimos, el tratamiento es muy completo, no dejando huecos sin cubrir: sistemas clásicos, generadores pseudoaleatorios, gestión de claves, criptoanálisis, RSA, D-H, ECC, etc.

Finalmente, el apartado “Bibliografía”, es un catálogo generalmente muy bien escogido de los libros más representativos de la materia. No obstante, sorprende la ausencia de referencias a libros en español (con excepción de los artículos del autor) cuando sin embargo a estas alturas del siglo, nuestro acervo bibliográfico no es ni mucho menos el páramo desierto que podría pensar algún inadvertido lector al repasar esta sección.

En resumen, una obra de amplio espectro en la materia que interesará al especialista por la amplitud con que se exponen todos los temas y será de obligada referencia en nuestra disciplina. ■

ARTURO RIBAGORDA GARNACHO
Universidad Carlos III de Madrid