SiC

Revista
Ciberseguridad, seguridad de la información y privacidad

www.revistasic.com

Nº 103

Febrero 2013 - Año XXII

PROYECTOS
- Atacama
- Fraternidad Muprespa

MÉTRICAS E INDICADORES
- De ciberseguridad
- En el ENS
- En seguridad gestionada

EN CONSTRUCCIÓN
¿Cómo medir lo que no ocurre?

CIBERSEGUROS
Medición, valoración y cobertura de riesgos TI

SITUATIONAL AWARENESS
Conciencia situacional en ciberdefensa

ESTRATEGIA
Cisco: reinventando la seguridad para las redes de hoy

La hora de medir, valorar y... comparar

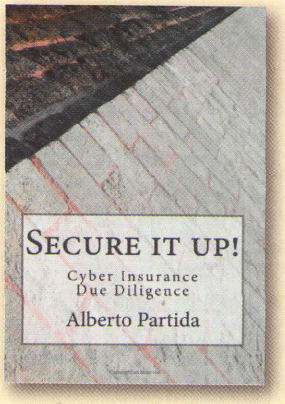
ENTREVISTA

Marty Meyer
Presidente
CORERO NETWORK SECURITY

Laboratorio SiC

- VÍNTEGRIS VinCert 2.1
- NETASQ 9.0 sobre *appliance* U800S

Bibliografía



SECURE IT UP!

Autor: Alberto Partida
Editorial: CreateSpace Independent Publishing Platform
Año: 2012 – 314 páginas
ISBN: 978-1478314752
www.createspace.com

Alberto Partida es bien conocido de los lectores de SIC. Colaborador de la revista con su afamada sección *Visita Recomendada*, y con una solvente trayectoria como especialista de seguridad TIC en los ámbitos financieros, además de prolífico conferenciante y escritor, vuelve a aportar una obra de considerable interés.

Si en su primer libro (itsecuriteers, 2010), Partida revelaba cómo crear un equipo de seguridad de la información que se alineara con los objetivos de negocio, en su segundo y recién aparecido volumen, **Secure it up!**, el autor proporciona información cualitativa y cuantitativa capaz de justificar los beneficios que la adopción de medidas de seguridad de la información y de gestión de riesgos conlleva a las organizaciones, facilitando al mismo tiempo los procesos *cyber-insurance* de diligencia debida.

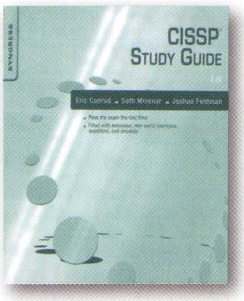
Según expone Partida en su libro, la consecuencia natural de la revolución experimentada en el volumen y tratamiento de la información que se inició en los años 90 inauguró una era de grandes beneficios empresariales. Sin embargo, si también ha ido en aumento el riesgo asociado, no así la percepción del mismo, resultando insuficientes los controles aplicados para proteger los activos críticos de una organización, los cuales, en última instancia, *"son todos los activos de una empresa solo por su propia existencia"*. En este sentido, la conclusión para el autor es que *"el ejercicio de identificación de activos nos deja donde empezamos: el papel de la gestión de riesgos de TI es la protección de todos los activos de TI"*.

En este contexto, únicamente la seguridad de la información es relevante en el contexto de su integración con los programas de gestión de riesgos empresariales (ERM, *Enterprise Risk Management*). Tras combinar un análisis exhaustivo de la literatura existente y los resultados de distintos estudios para dar forma a su argumento, del trabajo de Partida se derivan tres beneficiosas consecuencias: valor para los accionistas, mejor cumplimento y nuevas oportunidades de negocio.

En lo que respecta al segundo de ellos, el autor concluye que la experiencia demostrada en seguridad, como proteger una página web con SSL o demostrar la ausencia de infracciones y vulnerabilidades graves, se está convirtiendo en un factor crítico para las organizaciones en la creación de marca y confianza. La revolución que se aproxima, según vislumbra Partida, propone un giro desde la gestión de riesgos basada en activos a la gestión de riesgos basada en amenazas. Y es que la sofisticación de exitosas campañas de ataque, como las protagonizadas por Flame-Duqu-Stuxnet, ha llevado a las empresas a darse cuenta de que la simple aplicación de herramientas tradicionales de protección no es suficiente para detener determinados ataques.

En este contexto de nuevas vulnerabilidades, la gestión de riesgo basada en amenazas está cada vez más presente. Como se reconoce que los atacantes encontrarán, de un modo u otro, la forma de entrar en los sistemas, es preciso entonces hacer un giro desde la aproximación tradicional de la identificación de activos críticos a proteger, para focalizarse en la identificación de los agentes de amenaza, catalogando sus capacidades e intenciones.

Pero cambiar a un régimen de gestión de riesgos basado en la amenaza supone la existencia previa de un enfoque de gestión de riesgos que combine el trabajo en el campo de los riesgos de negocio con el mundo de la seguridad de la información. Justo lo que este libro propone.

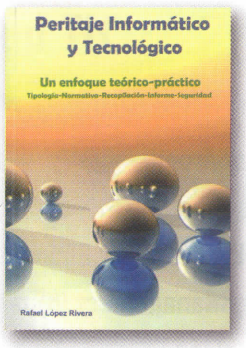


CISSP STUDY GUIDE

Autores: Eric Conrad, Seth Misenar y Joshua Feldman
Editorial: Syngress
Año: 2012 – 577 páginas
ISBN: 978-1-59749-961-3
www.syngress.com

En esta su segunda edición, esta guía para la certificación CISSP proporciona un método completo y efectivo de estudio para preparar los exámenes CISSP, conteniendo únicamente lo que realmente se necesita para aprobar los *tests*. Uno de los consejos que se extraen de sus páginas es el de aprenderse a conciencia los acrónimos que se utilizan en el libro y las palabras que representan, prestando mucha atención tanto al glosario como al índice, ampliamente detallados. Este libro, que también proporciona dos exámenes prácticos, e incluye preguntas al final de cada capítulo para ir haciendo un seguimiento gradual del aprendizaje.

El volumen está dividido en 11 capítulos: **1.-** Introducción; **2.-** Control de acceso; **3.-** Seguridad de telecomunicaciones y de red; **4.-** Gobierno de seguridad de la información y gestión del riesgo; **5.-** Seguridad en el desarrollo de software; **6.-** Criptografía; **7.-** Arquitectura y diseño de seguridad; **8.-** Seguridad de operaciones; **9.-** Planes de continuidad de negocio y de recuperación ante desastres; **10.-** Legal, Regulaciones, Investigaciones y Cumplimiento; y **11.-** Seguridad en entornos físicos.



PERITAJE INFORMÁTICO Y TECNOLÓGICO

Autor: Rafael López Rivera
Año: 2012 – 314 páginas
ISBN: 978-84-616-0895-9
www.peritoit.com

"Me he permitido la licencia de escribir el libro que me hubiera gustado encontrar cuando me inicié en esta fascinante profesión". Con estas palabras sintetiza el autor el objetivo de su trabajo: proporcionar a los profesionales de las tecnologías de la información TI y de las nuevas tecnologías los conocimientos adecuados sobre la profesión de perito; procedimientos, uso de metodología, normativas, legislación, estándares, buenas prácticas, etc.

Bajo un enfoque teórico-práctico, el volumen de López Rivera intenta clarificar los conceptos y consolidar las bases necesarias para el ejercicio de esta profesión en sus diferentes especialidades y situaciones operativas. Está compuesto por seis bloques temáticos: Generalidades y tipologías; Normativa legal; Recopilación de evidencias; Elaboración del informe; Seguridad Informática; y Tipologías de desempeños.