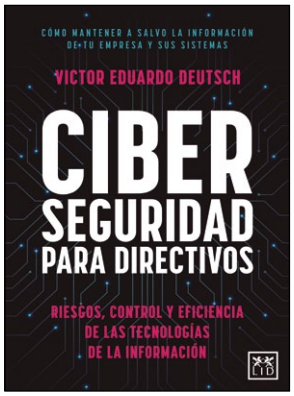
CIBERSEGURIDAD PARA DIRECTIVOS. RIESGOS, CONTROL Y EFICIENCIA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN



Autor: Víctor Eduardo Deutsch
Editorial: Lid Editorial
Año: 2022 – 212 páginas
ISBN: 978-84-113-115-95
www.lideditorial.com

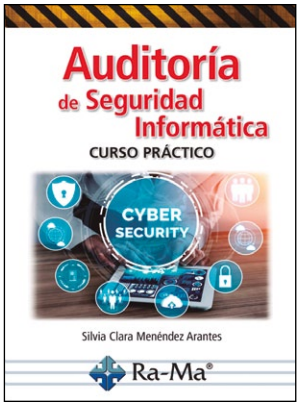
Con un lenguaje sencillo, un enfoque práctico y con abundantes casos reales, esta obra aspira a convertirse en un 'libro de cabecera' para la alta dirección, experta en gestión de riesgos tradicionales, pero con "dudas al enfrentarse a los nuevos retos digitales" por falta de formación en esta área y, también, por enfrentarse a ataques cada vez más silenciosos, inteligentes y sofisticados. Un reto para el que **Víctor Eduardo Deutsch**, con una amplia trayectoria en compañías como Telefónica o Kpmg, propone apostar por los tres pilares fundamentales de la ciberseguridad: "identificar los riesgos devenidos, establecer controles y poner en práctica los procesos y la organización necesarios para hacerlo de forma eficiente". Con ello, este libro nace con la aspiración de convertirse en una referencia para que los directivos puedan enfrentarse a los riesgos digitales con éxito "y mantener a salvo sus activos: la información de su negocio y de sus clientes y sus sistemas", destaca el autor.

CYBERINSURANCE POLICY: RETHINKING RISK IN AN AGE OF RANSOMWARE, COMPUTER FRAUD, DATA BREACHES, AND CYBERATTACKS (INFORMATION POLICY)

Autora: Josephine Wolff
Editorial: The MIT Press
Año: 2022 – 296 páginas
ISBN: 978-0262544184
mitpress.mit.edu

¿Por qué el ciberseguro no ha mejorado la ciberseguridad y qué pueden hacer los gobiernos para convertirlo en una herramienta más eficaz para la gestión del riesgo cibernético? Esta es una de las preguntas que dan pie a este interesante volumen que analiza la situación y cobertura de la industria de seguros cibernéticos. Además, ofrece un interesante resumen de su historia, desde las primeras pólizas de 'Responsabilidad de seguridad de Internet', a finales de los años 90, hasta la cobertura expansiva de la actualidad. **Josephine Wolff** ofrece así una excelente 'foto' del panorama actual del ciberseguro, comparándolo con las pólizas en otro tipo de sectores y recordando que esta figura como tal "es ineficaz para frenar las pérdidas de seguridad cibernética porque normaliza el pago de rescates en línea, mientras que el objetivo de la seguridad cibernética es el opuesto: desincentivar dichos pagos para que el *ransomware* sea menos rentable". En definitiva, este libro ofrece un análisis en profundidad de esta industria que sigue trabajando en dar con un modelado de riesgos adaptado a las nuevas tecnologías que están en constante evolución.

AUDITORÍA DE LA SEGURIDAD INFORMÁTICA

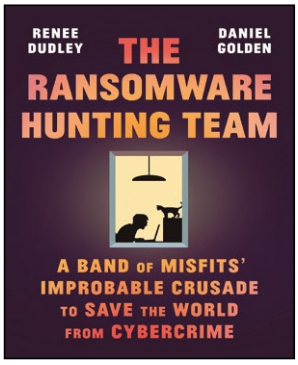


Autora: Silvia Clara Menéndez
Editorial: Ra-Ma
Año: 2022 – 220 páginas
ISBN: 978-84-18971-93-8
www.ra-ma.es

Como acostumbra la editorial Ra-Ma en su línea dedicada a ciberseguridad, este libro ofrece una excelente visión de cuáles son los procedimientos de una Auditoría Informática. A lo largo de sus capítulos el lector aprenderá a entender sus fases, metodologías y las herramientas que se precisan para realizar los diferentes tipos de auditorías. También, ofrece abundante información sobre las normativas que atañen a este ámbito, así como los estándares y procedimientos de buenas prácticas que hay que tener en cuenta a la hora de realizarlas, además del análisis y la gestión de riesgos.

En definitiva, una obra de referencia, no por su novedad, pero sí por su excelente síntesis explicando los conceptos y definiciones básicas de una auditoría en metodologías como OSSTMM, OSINT, OWISAM, OWASP, PTES, así como profundizando en la utilidad de diferentes herramientas como Nmap, Wireshark, Nessus u otras de este tipo, además de recomendar cómo realizar informes teniendo en cuenta, también, las actuales normativas que atañen al entorno de la ciberseguridad.

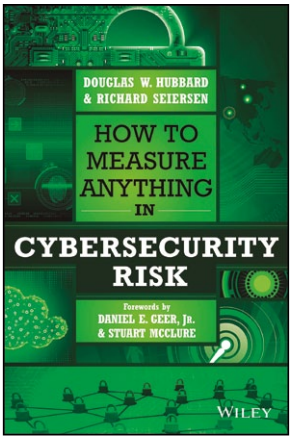
THE RANSOMWARE HUNTING TEAM: THE IMPROBABLE ADVENTURES OF THE MISFITS WHO ARE TRYING TO SAVE THE WORLD FROM CYBERCRIME



Autores: Renee Dudley y Daniel Golden
Editorial: Farrar, Straus and Giroux
Año: 2022 – 368 páginas
ISBN: 978-0374603304
us.macmillan.com

Apasionante *thriller* tecnológico a través del trabajo que realiza una "banda de excéntricos inadaptados que se enfrentan a las mayores amenazas de ciberseguridad de nuestro tiempo". Entretenido y rico en datos, sus autores muestran el trabajo de ficción, pero fruto de una investigación en profundidad, de un grupo de especialistas con altas capacidades que deciden ayudar a empresas, hospitales y administraciones a enfrentarse a las devastadoras consecuencias del *ransomware* y "evitar que millones de víctimas paguen miles de millones de dólares a los delincuentes". "Trabajando en su tiempo libre desde dormitorios y oficinas traseras, este equipo ofrece sus servicios pro bono a aquellos a quienes el FBI, otras agencias gubernamentales y el sector privado no quieren o no pueden ayudar". Por eso, la obra se muestra como una interesante simbiosis de películas como 'Los fisgones', series como 'El equipo A', que tanto han gustado, protagonizadas por expertos 'fuera del sistema', que ayudan a resolver grandes problemas a todo tipo de personas y empresas. En definitiva, un refrescante chapuzón en lo que se sumerge al lector en las bambalinas de la ciberseguridad y el trabajo de los que luchan contra el cibercrimen en su día a día.

HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK

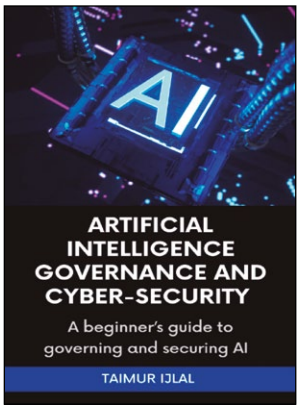


Autores: Douglas W. Hubbard y Richard Seiersen
Editorial: John Wiley & Sons Inc
Año: 2022 – 304 páginas
ISBN: 978-1119085294
www.wiley.com

¿Qué pasaría si el mayor riesgo de ciberseguridad fuera el propio método de evaluación de riesgos? Bajo este inquietante paradigma, los autores de este libro ponen en valor y recomiendan "soluciones reales, con éxito, a partir de la aplicación del lenguaje cuantitativo del análisis de riesgos a la seguridad de la información", destacan.

Al igual que obras anteriores como 'Cómo medir cualquier cosa', **Douglas Hubbard** "simplifica la complejidad de cuantificar la incertidumbre y arroja luz sobre asuntos con pocos datos u objetivos aparentemente intangibles", a los que **Richard Seiersen** aporta un enfoque de ciberseguridad para "brindar orientación autorizada", que permite resolver el problema de no evaluar en su justa medida el riesgo. Así, esta obra pretende convertirse en una "guía práctica que sirva como camino hacia una mejor evaluación de riesgos", brindando al lector "una potente colección de estrategias y herramientas", resaltan sus autores.

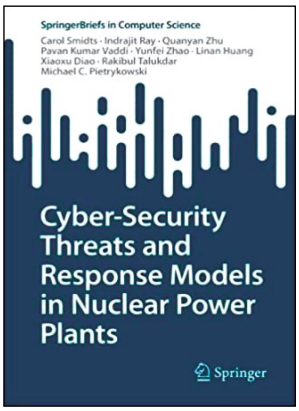
ARTIFICIAL INTELLIGENCE (AI) GOVERNANCE AND CYBER-SECURITY: A BEGINNER'S HANDBOOK ON SECURING AND GOVERNING AI SYSTEMS



Autora: Taimur Ijlal
Editorial: Publicación independiente
Año: 2022 - 104 páginas
ISBN: 979-8806138355
www.amazon.com

La inteligencia artificial (IA) está desatando cambios masivos en nuestras vidas, tanto a nivel individual como social, y se espera que este mercado global alcance alrededor de los 123.000 millones de euros, en 2025. El problema para la ciberseguridad es que, "a medida que más y más decisiones se trasladan a los sistemas de IA, se introducen más riesgos únicos", destaca su autora, que muestra en este libro cuáles son los más habituales, además de facilitar, a través de abundantes datos y bibliografía, la puesta en marcha de un marco de gobernanza para identificar y mitigar los riesgos de la IA, identificando también los más acuciantes en ciberprotección. Incluso, dando a conocer cómo crear bases de datos de referencia en seguridad cibernética para los sistemas de IA. Con todo, este libro permite, sin conocimientos previos, entender "cómo gobernar y proteger la IA" y mantener un alto grado de ciberseguridad. Su autora, además, destaca que los lectores que adquieran este libro en versión digital, también recibirán actualizaciones, al menos una vez al año, "con las últimas tendencias y riesgos en el mundo de la IA".

CYBER-SECURITY THREATS AND RESPONSE MODELS IN NUCLEAR POWER PLANTS

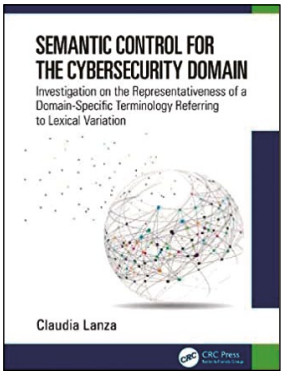


Autores: Carol Smidts, Indrajit Ray, Quanyan Zhu, Pavan Kumar Vaddi, Yunfei Zhao, Linan Huang, Xiaoxu Diao, Rakibul Talukdar, Michael C. Pietrykowski
Editorial: Springer
Año: 2022 - 501 páginas
ISBN: 978-3031127106
link.springer.com

Tanto por la gran experiencia de sus autores en entornos industriales, como por los peligros que supone no ciberproteger las plantas nucleares, este libro es, sin duda, una obra más que recomendable para los que quieran mejorar su conocimiento de la ciberseguridad en entornos industriales. Con este objetivo, en sus páginas se ofrece una interesante comprensión sobre cómo se realizan las evaluaciones probabilísticas de riesgos (PRA) en este tipo de infraestructuras, qué técnicas de detección de eventos anormales se aplican a sistemas de control industrial (ICS) y cómo usar la teoría de juegos para desarrollar "modelos de respuesta a ataques cibernéticos".

Ofrece, además, un exhaustivo marco de evaluación "para comprender los impactos de los ataques cibernéticos en el mundo físico". Con todo, el libro se presenta como "una herramienta muy útil tanto para los investigadores que trabajan en las áreas de ciberseguridad en sistemas de control industrial, sistemas de energía y sistemas físicos cibernéticos, como a los menos expertos que quieren tener un 'nivel avanzado' en su protección", destacan sus autores.

SEMANTIC CONTROL FOR THE CYBERSECURITY DOMAIN: INVESTIGATION ON THE REPRESENTATIVENESS OF A DOMAIN-SPECIFIC TERMINOLOGY REFERRING TO LEXICAL



Autora: Claudia Lanza
Editorial: CRC Press
Año: 2022 - 180 páginas
ISBN: 978-1032250809
www.routledge.com

Este volumen presenta un tesauro bilingüe (italiano e inglés), y su conversión en un sistema de ontología orientado al campo de la ciberseguridad, que permite contar con una "una valiosa referencia para los estudiosos de las investigaciones basadas en corpus, la terminología, las TIC, la documentación y biblioteconomía, la investigación en procesamiento de textos, el área de interés de la semántica distribucional, así como para los profesionales involucrados en las organizaciones de ciberseguridad".

En definitiva, esta obra de Lanza permite a los lectores "compilar y estudiar importantes corpus de documentación", para contar con un alto grado de conocimiento de la terminología más usada en el ámbito de la protección cibernética a través de una "descripción de varias técnicas pertenecientes al campo de la lingüística y la ingeniería del conocimiento". Una obra que, por su especialización, pero también por su utilidad, no debería pasar desapercibida.