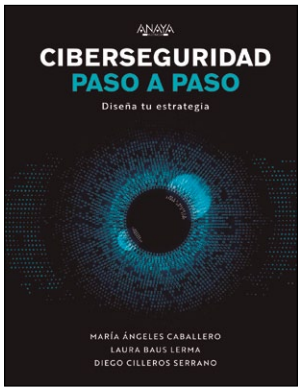
CIBERSEGURIDAD PASO A PASO: DISEÑA TU ESTRATEGIA



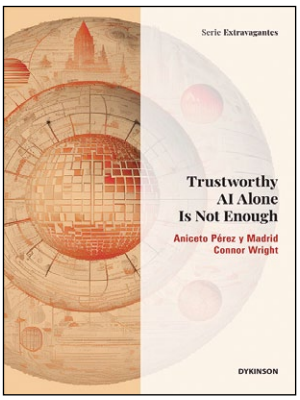
Autores: María Ángeles Caballero, Laura Baus y Diego Cilleros
Editorial: Anaya Multimedia
Año: 2023 – 600 páginas
ISBN: 978-8441548442
https://anayamultimedia.es

Algunos estudios alertan de que en torno al 60% de las pymes que sufren un ciberataque cierra a los seis meses. Y es que, el cibercrimen tiene un coste de trillones de euros superando al PIB de muchos países. Así lo destacan los tres destacados profesionales en ciberseguridad, autores de este libro que se ha escrito a modo de guía. Se trata de un libro "en el que elaboramos el nuevo y sencillo marco de ciberseguridad CABACI, que permite evaluar el nivel de madurez de cualquier empresa", destacan.

Así, con profundidad, pero de manera didáctica, el lector podrá aprender a valorar la importancia de entender el negocio y la tecnología, así como identificar a sus *stakeholders* y profesionales que estén comprometidos con el programa de ciberseguridad de una compañía para tener capacidad para detectar, responder y recuperarse de un incidente, y comunicarlo adecuadamente.

Por ello, se convierte en una valiosa aportación bibliográfica para un público no experto en este ámbito que puede aprender "paso a paso cómo construir una estrategia de ciberseguridad adaptada a sus necesidades", destacan.

TRUSTWORTHY AI ALONE IS NOT ENOUGH



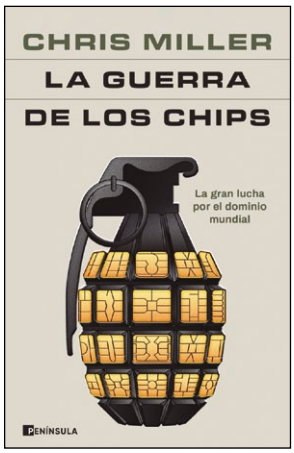
Autores: Aniceto Pérez y Madrid y Connor Wright
Editorial: Dykinson.
Año: 2023 – 153 páginas
ISBN: 978-84-1170-600-1
www.dykinson.com

El objetivo de este libro es hacer accesible tanto al público general, como a los responsables políticos, las complejidades involucradas en el concepto de la inteligencia artificial (IA) confiable, abordándose desde puntos de vista filosóficos, técnicos, sociales y prácticos.

Para ello, sus autores comienzan con una explicación de lo que es una IA confiable y sus componentes, según el informe 'HLEG for AI'. A partir de ahí, se centran en detalle en cómo se aterriza la IA confiable en todo tipo de entornos, desde grandes modelos de lenguaje, hasta los robots antropomórficos y, también, en los drones autónomos, que plantean desafíos específicos debido a su estrecha interacción con los humanos.

Los autores también ofrecen una breve presentación del esquema de validación ética para las propuestas presentadas bajo el programa Horizonte Europa, como una posible forma de abordar la operacionalización de la regulación ética más allá de reglas rígidas y análisis éticos parciales. En su parte final, este ensayo aboga por un enfoque de la ética de la virtud en la IA, que sus autores consideran "un enfoque humano e integral para una IA confiable que puede adaptarse al ritmo del cambio tecnológico".

LA GUERRA DE LOS CHIPS



Autores: Chris Miller, Àlex Guàrdia Berdiell (traductor)
Editorial: Ediciones Península
Año: 2023 – 544 páginas
ISBN: 978-8411001984
www.planetadelibros.com

Llega, por fin, la traducción de una de las obras más vendidas en EE.UU. de 2023, considerado el 'mejor libro del año' por The Economist. "Si hay un conflicto que está definiendo ahora mismo la geopolítica mundial es la guerra de los chips", recuerda su autor. "La economía mundial, el equilibrio de poderes, la supremacía militar y el desarrollo industrial dependen de su producción constante. Hasta hace poco, EE.UU. era el principal productor de semiconductores, lo que le permitía mantener su liderazgo como primera superpotencia mundial", añade sobre esta obra donde alerta de que "su posición dominante se ve cada vez más amenazada por competidores de Taiwán, Corea, Europa y, sobre todo, China, que inyecta anualmente miles de millones en un programa de fabricación de procesadores con el fin de alcanzar a su competidor estadounidense".

Así, Miller muestra cómo los microprocesadores han revolucionado el mundo y cambiado la Historia, y cómo la lucha por esta tecnología podría conducir no solo a su escasez mundial, sino también al nacimiento de una nueva Guerra Fría.

LA OLA QUE VIENE

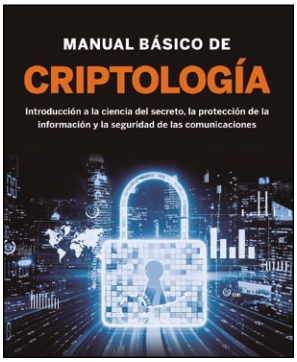
Autores: Mustafa Suleyman y Michael Bhaskar; Claudia Fernández (traductora)
Editorial: Debate
Año: 2023 – 392 páginas
ISBN: 978-8419399649
www.penguinlibros.com

"Estamos a punto de cruzar un umbral crítico en la historia de nuestra especie. Todo lo que conocemos va a cambiar. Pronto viviremos rodeados de una inteligencia artificial responsable de ejecutar tareas complejas. Habitaremos un mundo de impresoras de ADN y ordenadores cuánticos, patógenos artificiales y armas autónomas, robots asistentes y energía abundante. Todo esto supone una transformación radical en la capacidad humana. No estamos preparados", destaca el autor, **Mustafa Suleyman**, cofundador de la conocida compañía DeepMind y un referente mundial en IA.

Fruto de su experiencia, asegura que la próxima década estará marcada por esta gran ola de nuevas y poderosas innovaciones de rápida proliferación. Impulsadas por incentivos estratégicos y comerciales, estas herramientas ayudarán a afrontar retos globales y crearán una enorme riqueza, pero también provocarán revueltas a una escala antes inimaginable, según el autor.

De hecho, considera que esta revolución "amenaza seriamente las bases del orden mundial". "Nos enfrentamos a un dilema existencial: por un lado, a los daños sin precedentes derivados de una exposición incontrolada a estas nuevas tecnologías; por otro, a la amenaza de una vigilancia tiránica y abusiva".

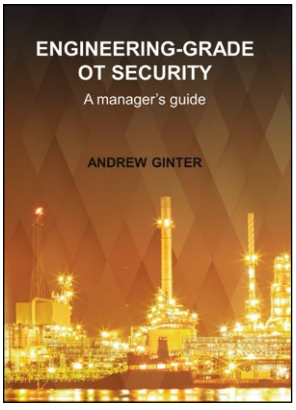
MANUAL BÁSICO DE CRIPTOLOGÍA: INTRODUCCIÓN A LA CIENCIA DEL SECRETO



Autor: Luis Hernández Encimas
Editorial: Pinolia
Año: 2023 – 304 páginas
ISBN: 978-8419399649
https://almuzaralibros.com

"La seguridad de la información es cada vez más importante en nuestras vidas hiperconectadas, pero no siempre somos conscientes de ello ni sabemos cómo funcionan mecanismos que pueden resultar muy cómodos de usar, pero abrumadoramente complejos de comprender", destaca el autor, reconocido profesional en el ámbito académico, que pretende con esta obra abrir la puerta a los que quieran adentrarse en el fascinante mundo del cifrado de información. **Luis Hernández**, criptólogo y matemático, permite al lector sumergirse en un recorrido por la historia de la criptografía: desde la escítala usada por griegos y romanos, la tabla de Polibio, los discos de Alberti o los diversos métodos de cifrado usados por reyes, reinas, templarios o francmasones para mantener sus mensajes lejos de ojos indiscretos, hasta la máquina Enigma utilizada durante la Segunda Guerra Mundial por los alemanes para enviar mensajes encriptados y descifrada por los Aliados con la ayuda de Alan Turing. Además, profundiza en los métodos de seguridad actuales, como las finanzas en línea, los pagos con tarjeta de crédito o las criptomonedas y la tecnología *blockchain*.

ENGINEERING-GRADE OT SECURITY: A MANAGER'S GUIDE

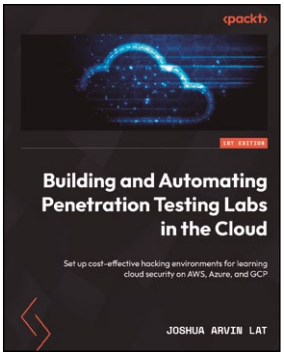


Autor: Andrew Ginter
Editorial: Abterra Technologies
Año: 2023 – 230 páginas
ISBN: 978-0995298491
https://bookscouter.com

Imagine que trabaja en una central eléctrica que utiliza media docena de enormes calderas de vapor de cinco pisos de altura. Si un ciberataque hace que una caldera se sobrepresurice y explote, lo más probable es que le mate a usted y a todos los que estén cerca. ¿Qué mitigación de ese riesgo preferiría, una válvula de sobrepresión mecánica en cada caldera donde, si la presión en la caldera sube demasiado, el vapor fuerza la válvula a abrirse, el vapor escapa y se libera la presión? ¿O una contraseña más larga en el ordenador que controla las calderas?

Estas son las premisas que el autor pretende responder, ya que considera que "abordar los riesgos cibernéticos de las operaciones físicas requiere más que ciberseguridad. La profesión de ingeniería ha gestionado riesgos físicos y amenazas a la seguridad y la seguridad pública durante más de un siglo. La ingeniería de procesos, automatización y redes son herramientas poderosas para abordar los riesgos cibernéticos de OT, herramientas que simplemente no existen en el dominio de TI". Por ello, esta obra explora estas herramientas, el riesgo y analiza lo que significa "debido cuidado" en el cambiante panorama actual de amenazas cibernéticas.

BUILDING AND AUTOMATING PENETRATION TESTING LABS IN THE CLOUD

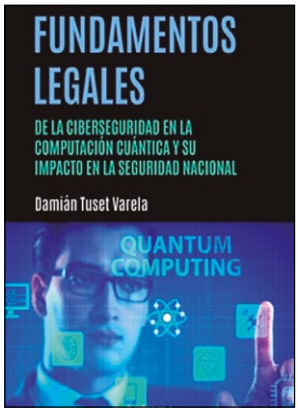


Autor: Joshua Arvin Lat
Editorial: Publicación independiente
Año: 2023 – 562 páginas
ISBN: 978-1837632398
www.amazon.com

En esta obra, eminentemente técnica, el autor ofrece una guía paso a paso, para diseñar y crear laboratorios de pruebas de intrusión que imiten los entornos de nube modernos que se ejecutan en AWS, Azure y Google Cloud Platform. Además, ofrece notable información sobre cómo utilizar soluciones de infraestructura como código (IaC) para gestionar una variedad de entornos de laboratorio en la nube, aprovechar las herramientas de IA generativa, como ChatGPT, para acelerar la preparación de plantillas y configuraciones de IaC y a validar vulnerabilidades explotando configuraciones erróneas y utilizando diversas herramientas y técnicas de pruebas de penetración.

En su parte final, también propone estrategias prácticas para gestionar la complejidad, el coste y los riesgos involucrados. En definitiva, el libro pretende enseñar a lectores con conocimientos técnicos, a "diseñar y construir entornos de laboratorio en la nube vulnerables y rentables donde podrá experimentar y practicar diferentes tipos de ataques y técnicas de pruebas de seguridad lo más parecido a la realidad", explica el autor.

FUNDAMENTOS LEGALES DE CIBERSEGURIDAD EN COMPUTACIÓN CUÁNTICA Y SU IMPACTO EN LA SEGURIDAD NACIONAL



Autor: Damián Tuset Varela
Editorial: Letrame
Año: 2023 – 86 páginas
ISBN: 9788411811958
www.casadellibro.com

En este libro el lector encontrará un concienzudo análisis sobre cómo está evolucionando la tecnología que busca la popularización de la computación cuántica, "una revolución tecnológica que plantea desafíos únicos y complejos en términos de ciberseguridad y seguridad nacional".

En concreto, el autor se enfoca en un punto de vista jurídico, exhaustivo, de los marcos legales y normativos actuales, evaluando su efectividad en la mitigación de los riesgos asociados con este salto tecnológico. La tesis de la obra se centra en el hecho de que la computación cuántica, a pesar de sus enormes ventajas, plantea dilemas legales y normativos en áreas como la protección de datos, la criptografía o la propiedad intelectual, entre otras.

El libro también propone recomendaciones estratégicas para futuros desarrollos legislativos para "prevenir amenazas a la seguridad nacional y promover la ciberseguridad en la era de la computación cuántica". Con ello, pretende ofrecer "una herramienta para los legisladores, profesionales del derecho y tecnólogos, brindándoles una guía para navegar en el cambiante mundo de la ciberseguridad y la informática cuántica", explica **Damián Tuset**.