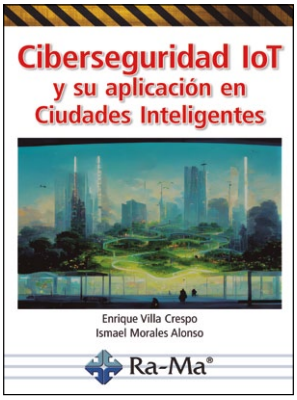
CIBERSEGURIDAD IOT Y SU APLICACIÓN EN CIUDADES INTELIGENTES



Autores: Enrique Villa e Ismael Morales
Editorial: RA-MA Editorial
Año: 2022 – 290 páginas
ISBN: 978-84-19444-73-8
www.ra-ma.es

El Internet de las Cosas (IoT) está directamente relacionado con todos los ámbitos y, sin duda, uno en el que mayores repercusiones tendrá son las ciudades 'inteligentes' y su gestión, las denominadas *smart cities*. Sin embargo, la apuesta por la gestión digital de las grandes urbes, con los beneficios que aporta, también supone un reto en el ámbito de la ciberseguridad y la privacidad digital.

Para ofrecer visibilidad a lo que se está acometiendo, así como las necesidades en ciberprotección que plantea este paso, los dos autores, reconocidos expertos en la materia, ofrecen a lo largo de los cinco capítulos de esta obra una completa introducción a las tecnologías IoT, su evolución en todo tipo de sectores, como el industrial y el de salud, además de información detallada sobre qué necesidades surgirán de las ciudades inteligentes en el ámbito de la ciberseguridad IoT.

Además, en su cuarto capítulo proponen un *framework* de ciberseguridad *para smart cities*, con una guía de implementación, dedicando la última parte del libro a la posible evolución del IoT en las ciudades inteligentes y qué se precisa para llevarla a cabo de forma segura.

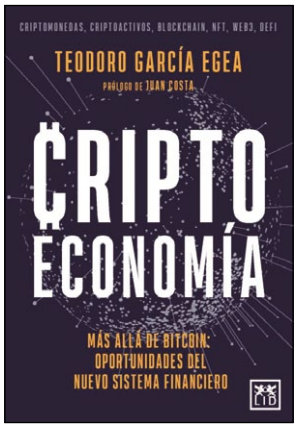
DE LA CAVERNA AL METAVERSO: UN RELATO DISRUPTIVO DE LA TECNOLOGÍA

Autor: Felipe Colorado
Editorial: 0xword
Año: 2023 – 266 páginas
ISBN: 978-84-09-45152-4
https://0xword.com/

Singular aportación, por cuanto hay poco publicado, con rigor y profundidad sobre el tan nombrado y polémico metaverso, en el que **Felipe Colorado** presenta cómo se ha evolucionado "desde el sílex al silicio", hasta llegar al cibermundo que vivimos. "Desde que el hombre tomó una piedra en su mano, supo que podría transformar el mundo. Tecnología para la guerra, la represión y el delito. También, para la difusión universal del conocimiento, la mejora de la calidad de vida y la lucha contra enfermedades y pandemias", destaca Colorado.

A través de una fusión de arqueología, narrativa y ficción, también con humor, el autor transporta al lector a un viaje por nuestra historia, con amplia presencia de la seguridad de la información y de muchos de sus hitos, partiendo de 1834 y mostrando la actividad de los hacktivistas, además de recordar qué riesgos plantean "los bajos fondos de una Web 2.0, pronta a dar el relevo a su sucesora y al naciente Metaverso". Por supuesto, no faltan reflexiones sobre la ética de muchos de los aspectos digitales que nos rodean. Para facilitar la profundización del lector en este ámbito, la obra viene acompañada de un PDF descargable con más de 150 referencias 'webgráficas' y 23 imágenes exclusivas.

CRIPTOECONOMÍA. MÁS ALLÁ DEL BITCOIN: OPORTUNIDADES PARA EL SISTEMA FINANCIERO

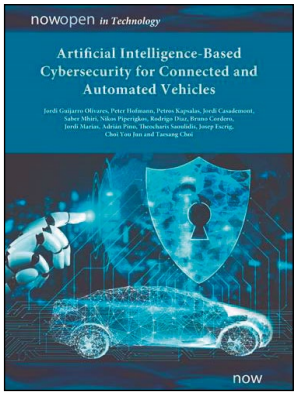


Autor: Teodoro García Egea
Editorial: LID Editorial
Año: 2023 – 208 páginas
ISBN: 9788417277499
www.lideditorial.com

"*Tokenización* de activos, préstamos seguros entre particulares, contratos inteligentes que se ejecutan automáticamente, financiación de proyectos sostenibles... Aunque en la mente de muchas personas la criptoeconomía equivale tan solo a invertir en bitcoins, el intercambio de valor a través de la red ya ha puesto en marcha un nuevo sistema económico que está cambiando el mundo", destaca el autor de este libro, conocido por su etapa política como secretario general del Partido Popular de 2018 a 2022, **Teodoro García Egea**.

Apasionado por la ciberseguridad y las nuevas tecnologías, Egea, en su retorno a estos ámbitos, está centrando su actual trabajo en el entorno de las criptomonedas y fruto de ello es este ensayo presentado en marzo pasado en el que repasa y profundiza en las consecuencias de lo que denomina la criptoeconomía. Un concepto que considera que "va a generar una disrupción similar a la que generó la llegada de internet", transformando por completo muchos de los sectores que conocemos. Se trata sin duda de un libro divulgativo para expertos y no expertos que permite conocer, de forma sencilla y amena, qué son tecnologías como el *blockchain* y qué impacto económico están teniendo en todo tipo de entornos.

ARTIFICIAL INTELLIGENCE BASED CIBERSECURITY FOR CONNECTED AND AUTOMATED VEHICLES



Autores: Jordi Guijarro, Peter Hofmann, Petros Kapsalas, Jordi Casademont, Nikos Piperigkos, Rodrigo Díaz, Bruno Cordero, Jordi Marías, Adrián Pino, Theocharis Saoulidis, Josep Escrig, Choi You Jun, Taesang Choi
Editorial: Now publishers Inc
Año: 2022 – 166 páginas
ISBN: 978-1-63828-061-3
https://nowpublishers.com

Los vehículos conectados ya son una realidad en las carreteras y, en pocos años, también llegarán los coches autónomos. Por ello, los efectos de los ataques cibernéticos sobre ellos pueden ser tremendos, incluyendo los daños físicos a ocupantes y peatones. Para anticiparse a estos riesgos, entre otras iniciativas, la UE está financiación el proyecto Caramel (Ciberseguridad basada en inteligencia artificial para vehículos conectados y automatizados), que ha desarrollado varias soluciones antipiratería para la nueva generación de vehículos.

Cofinanciado por la UE, en el marco del programa Horizonte 2020, este consorcio cuenta con 15 organizaciones de ocho países europeos junto con tres socios coreanos. Su reto es aplicar un enfoque proactivo basado en técnicas de Inteligencia Artificial y Aprendizaje Automático para detectar y prevenir posibles amenazas de ciberseguridad para vehículos autónomos y conectados.

Este enfoque se ha abordado en base a cuatro pilares: Movilidad Autónoma, Movilidad Conectada, Electromovilidad y Vehículo a Control Remoto. Este libro presenta la teoría y los resultados de cada una de estas direcciones técnicas.

SPACE ROGUE: HOW THE HACKERS KNOWN AS L0PHT CHANGED THE WORLD

Autor: Cris Thomas
Editorial: Independiente
Año: 2023 – 362 páginas
ISBN: 979-8987032411
www.barnesandnoble.com

Interesante relato sobre uno de los grupos hackers más conocidos de EE.UU., en los años 90. En mayo de 1998, el Congreso invitó a los siete miembros del denominado 'L0pht' a testificar sobre el estado de la seguridad informática del gobierno. Dos años más tarde, sus integrantes se profesionalizaron fundando la consultoría de seguridad @stake. "En el camino, se enfrentaron a gigantes tecnológicos como Microsoft, Oracle, Novell y otros para exponer las debilidades de los principales productos de esas empresas", recuerda su autor que también destaca que "a pesar de la destreza técnica de L0pht, el grupo no pudo mantener lo que habían construido juntos cuando el dinero y la política interna se volvieron amigos contra amigos".

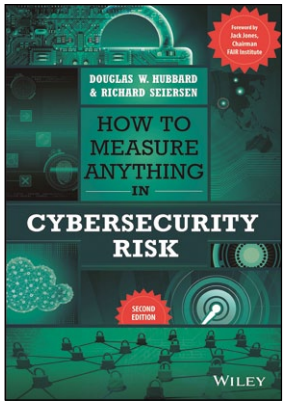
Se trata en definitiva de un excelente relato sobre la historia de la ciberseguridad, la influencia hacker y sus aportaciones a la industria, llevando al lector a través de un apasionante viaje en el que el talento, las habilidades técnicas y, también, el afán de destacar permite disfrutar de lo que fueron los orígenes de los investigadores de ciberseguridad. "El colectivo de hackers L0pht ya no existe, pero su legado sigue vivo", subraya su autor a la que vez recuerda que L0pht estableció el estándar sobre cómo la industria de la seguridad cibernética publica ahora información sobre vulnerabilidades.

CLAVES DE INTELIGENCIA ARTIFICIAL Y DERECHO

Autor: Pablo García Mexía
Editorial: La Ley
Año: 2022 – 184 páginas
ISBN: 978-8419032850
https://tienda.wolterskluwer.es

La inteligencia artificial (IA) constituye uno de los avances tecnológicos clave para la humanidad como también que representa uno de los retos más críticos desde el punto de vista social, ético y jurídico. "Tal contraste confiere a este libro su más profunda razón de ser. Si las sociedades son al menos significativamente escépticas sobre el impacto de la IA, parece más que justificado que aquellos de sus componentes que puedan suponer más riesgos sociales encuentren un contrapeso ético y, en lo que aquí más interesa, desde el Derecho", destaca, tan preclaro como en él es habituaL, el autor, que "explora las causas y consecuencias de todo y contribuye a enriquecer el debate sobre los aspectos jurídicos de las tecnologías de IA". Una obra pionera en la materia en España que ha sido escrita con un enfoque abierto, por cuanto, aunque se centra en los aspectos jurídicos, no prescinde de los tecnológicos.

Así, en ella el lector podrán encontrar un punto de partida para tener una buena visión de los retos que la IA plantea al Derecho, además de contar con información especializada de cómo se está acometiendo su regulación en Europa y España, tanto para los que tienen que trabajar con ella en su día a día como para los que piensen comenzar a aprovechar sus capacidades.



HOW TO MEASURE ANYTHING IN CYBERSECURITY RISK

Autores: Douglas W. Hubbard y Richard Seiersen
Editorial: Wiley
Año: 2023 – 368 páginas
ISBN: 978-1119892304
www.wiley.com

Segunda edición, revisada y actualizada de esta obra de referencia, a cargo de uno de los pioneros de la ciberseguridad y un reconocido analista, ofreciendo un texto revelador permite sacar partido "del lenguaje cuantitativo del análisis de riesgos a la ciberseguridad", destacan sus autores. Así, en este libro el público profesional encontrará una aproximación rigurosa y en detalle de cómo cuantificar la incertidumbre en este ámbito en entornos corporativos, con numerosas referencias a cómo medir objetivos aparentemente intangibles.

En definitiva, se trata de una "una hoja de ruta imprescindible" con la que los ya consolidados profesionales en este tema mejorarán sus conocimiento y los que se aproximen a este tema podrán dar una gran pasos a través de los abundantes consejos detallados de **Hubbar** y **Seiersen** para mejorar la evaluación de riesgos con un marco directo y simple para una variedad de casos de uso entre los que están desde cómo acometer una auditoría rápida de riesgos, para una primera evaluación cuantitativa, hasta cómo medir el impacto real del daño a la reputación, acompañado de nuevos ejemplos bayesianos para evaluar el riesgo con pocos datos, además de diferentes materiales sobre medición y recomendaciones de e cómo combinar la opinión de expertos.

CYBER SECURITY IN MERGERS & ACQUISITIONS: THE INDUSTRY HANDBOOK

Autor: Rajinder Tumber
Editorial: CRC Pres
Año: 2022 – 252 páginas
ISBN: 978-0367676780
www.routledge.com

Esta novedad bibliográfica se torna, por lo poco tratado de su tema, en una lectura más que recomendable para cualquier profesional de ciberseguridad. Su autor que, reconocido por la Cámara de los Lores, en Reino Unido, aborda con profundidad, aunque con una prosa de fácil lectura, el reto de cómo evaluar la madurez cibernética de una organización durante la fase previa a la negociación de su adquisición. "Una violación de datos imprevista durante una fusión o adquisición podría resultar en la eliminación de cientos de millones de euros", recuerda Tumber poniendo como ejemplo la rebaja de 317 millones de euros que tuvo que realizar Yahoo a Verizon, en 2016, por una brecha que comprometió más de 1.000 millones de cuentas de correo-e.

Se trata, pues, de un libro, pensado sobre todo para los que trabajan en inversiones y fusiones o compras de compañías en este sector, pero también para los que quieran tener una visión clara de qué aspectos aportan más valor en este tipo de operaciones y cómo apostando por las mejores prácticas de seguridad se puede contar con ella como multiplicador del valor de cualquier compañía. Además, proporciona el marco 'CyberDD6' para llevar a cabo este tipo de operaciones.