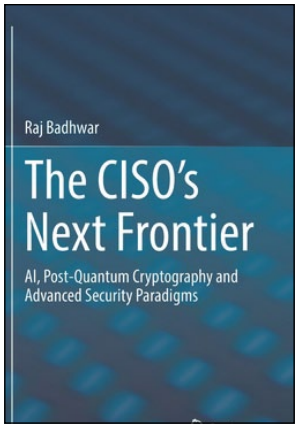
THE CISO'S NEXT FRONTIER: AI, POST-QUANTUM CRYPTOGRAPHY AND ADVANCED SECURITY PARADIGMS

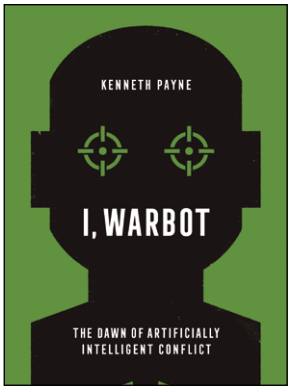


Autor: Raj Badhwar
Editorial: Springer
Año: 2021 - 387 páginas
ISBN: 9783030753535
www.springer.com

Con más de 25 años en el sector, **Raj Badhwar**, que ha ocupado destacados puestos en ciberseguridad y TI en compañías como AIG, BAE Systems Inc., Bank of America, Time Warner Cable y AOL Time Warner (donde actualmente, es CISO) ofrece en este libro abundante información, teórica y práctica, para tener una amplia comprensión de los riesgos a los que se enfrentan las empresas con las tecnologías, incluyendo la computación cuántica, la inteligencia artificial y el aprendizaje automático para la ciberseguridad, sin dejar de lado un amplio espacio a lo que supone para la seguridad de la información el trabajo en remoto, la nube y la importancia de medir el riesgo cibernético organizacional.

Pensada para CISOs, CTOs, CIOs y CFOs, este notable volumen incluye un análisis detallado de muchas tecnologías y enfoques importantes para disminuir, mitigar o remediar esas amenazas, tanto actuales como futuras. Además, al final de cada capítulo, el autor proporciona una evaluación sumamente útil con una visión, perspectiva y casuísticas propias de la figura y desempeño del CISO.

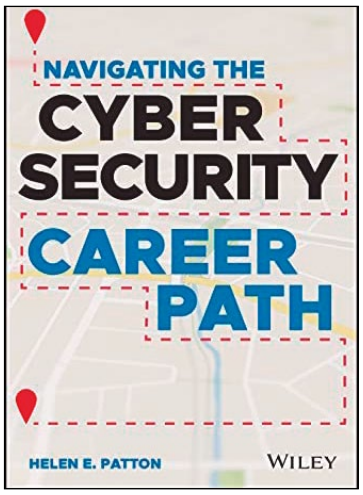
I, WARBOT: THE DAWN OF ARTIFICIALLY INTELLIGENT CONFLICT



Autor: Kenneth Payne
Editorial: Oxford University Press
Año: 2021 - 336 páginas
ISBN: 978-0197611692
Global.oup.com

El conocido autor de libros relacionados con la psicología y la guerra, **Kenneth Payne** se adentra en esta ocasión en el análisis del impacto de los sistemas autónomos con inteligencia artificial, en los actuales y futuros conflictos, y qué revolución suponen para el campo de batalla. "Los sistemas de armas inteligentes están hoy aquí y muchos otros están de camino" destaca, resaltando que el cambio que suponen las nuevas guerras con "drones sin piloto, tanques robóticos y sumergibles no tripulados" y cuarteles generales lejos de donde se produce el combate. "Los *warbots* serán más rápidos, más ágiles y más mortíferos que las armas tripuladas de hoy. Surgirán nuevas tácticas y conceptos, con suplantación de identidad y enjambre para engañar y abrumar a los enemigos. Las estrategias también están cambiando", plantea a la vez que propone reglas para regular el empleo de este tipo de armas, mostrando cómo se podría conseguir en un futuro no tan lejano. Un mundo donde Payne destaca que la ética lo decidirá todo. En última instancia, tras exponer sus novedosas tres reglas robóticas –que sustituyen inquietantemente a las clásicas propugnadas por Asimov– deja patente una sobrecogedora aseveración: "Por primera vez mentes no humanas pueden tomar las decisiones en una guerra".

NAVIGATING THE CYBERSECURITY CAREER PATH

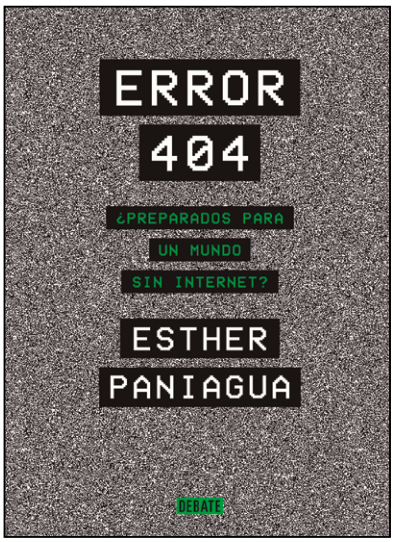


Autora: Helen E. Patton
Editorial: Wiley
Año: 2021 - 336 páginas
ISBN: 978-1-119-83343-7
www.wiley.com

"Encontrar la posición correcta en ciberseguridad es un desafío. Tener éxito en la profesión requiere mucho trabajo. Y convertirse en un ejecutivo de ciberseguridad responsable de un equipo es aún más difícil". Así lo destaca la autora de este libro, **Helen E. Patton**, que asesora como CISO a grandes empresas y brinda una 'discusión práctica y perspicaz' para los aspirantes a trabajar en ciberprotección, y para los que ya forman parte de ella y quieren mejorar su trayectoria profesional.

Así, la autora analiza los aspectos más notables del actual mercado laboral en ciberprotección y sus perfiles más demandados, aportando abundantes recomendaciones, fruto de la experiencia de la autora, para "pasar de un puesto de nivel de entrada en la industria a uno de responsabilidad". Además, destaca su apéndice con abundantes recursos (desde *podcast* hasta *blogs* y libros) para ampliar la información.

ERROR 404: ¿PREPARADOS PARA UN MUNDO SIN INTERNET?



Autora: Esther Paniagua
Editorial: Debate
Año: 2021 - 352 páginas
ISBN: 978-8418056062
www.penguinlibros.com

"Es cuestión de tiempo que la Red caiga. ¿Estamos preparados? Error 404 no es una distopía. Es un impactante ensayo que trata de anticiparse a ella antes de que sea demasiado tarde. Es cuestión de tiempo que la red caiga. Internet se vendrá abajo y viviremos oleadas de pánico. ¿Suena apocalíptico? No lo es". Con este planteamiento, la periodista sobre tecnología, **Esther Paniagua,** aborda cómo podría producirse un gran apagón de la red de redes, qué caos podría desatarse y lo dependientes que somos de ella. Además, analiza quiénes están detrás de Internet y cómo actúan en ella cibercriminales y entes que buscan beneficio propio con la manipulación y la desinformación. En definitiva, ofrece una interesante visión del funcionamiento oculto de "una tiranía digital que George Orwell o Aldous Huxley tan siquiera imaginaron".

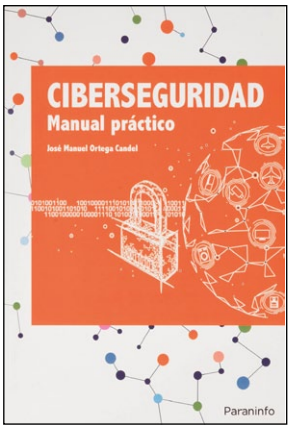
EL LIBRO DEL HACKER EDICION 2022

Autores: María Ángeles Caballero y Diego Cilleros Serrano
Editorial: Anaya Multimedia
Año: 2021 - 744 páginas
ISBN: 978-8441544338
anayamultimedia.es

En la cuarta edición de este libro -la primera salió en 2014-, **María Ángeles Velasco,** CISO del Centro Corporativo del Banco de Santander, y **Diego Cilleros,** Senior Manager en Deloitte, muestran "desde aspectos esenciales de la ciberprotección y el *hacking,* hasta conocimientos avanzados para hacer frente a las principales técnicas de ataque". Por supuesto, también ofrecen abundante información de lo que está pasando con la ciberguerra y el ciberespionaje, así como de los retos y riesgos que plantea la nube, los datos, la identidad, la criptográfia y la cadena de bloques.

Por ello, y por la profundidad técnica que ofrecen, este volumen es un excelente punto de referencia tanto para los profesionales de TI que quieren mejorar su conocimiento de la ciberprotección, como para los ya contrastados que quieran actualizar conceptos y técnicas, también frente a la ingeniería social. En definitiva, una obra que permite entender el 'modus operandi' cibercriminal'… con pensamiento 'hacker'.

CIBERSEGURIDAD. MANUAL PRÁCTICO



Autor: José Manuel Ortega Candel
Editorial: Paraninfo
Año: 2021 - 346 páginas
ISBN: 978-8413661162
www.paraninfo.es

Ingeniero e investigador de ciberseguridad -y habitual ponente en eventos nacionales e internacionales-, **Ortega Cándel** es autor prolijo en libros de ciberprotección e informática (con obras como 'Desarrollo seguro en ingeniería del software, Tecnologías para arquitecturas basadas en microservicios o Hacking ético con herramientas Python, entre otros). En su nuevo libro, que confiesa que se le ocurrió "leyendo la Revista SIC, de la que soy suscriptor hace tiempo", ofrece un enfoque teórico-práctico para permitir al lector alcanzar una excelente visión de alcance holístico –con la profundización justa– del estado de la ciberseguridad en ámbitos como la seguridad en la nube, la privacidad, las aplicaciones web e, incluso, a través de herramientas de *hacking* ético, herramientas para análisis en fuentes abiertas (OSINT) o el funcionamiento de los Centros de Operaciones de Ciberseguridad (SOC). En definitiva, ofrece una información útil y razonablemente exhaustiva que complementa con numerosas referencias bibliográficas para estar "actualizado ante nuevas amenazas".

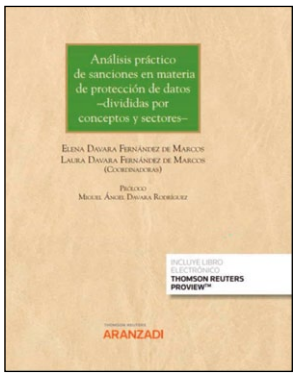
¿TE VA A SUSTITUIR UN ALGORITMO? EL FUTURO DEL TRABAJO EN ESPAÑA

Autora: Lucía Velasco
Editorial: Turner Libros
Año: 2021 - 272 páginas
ISBN: 978-8418895050
www.turnerlibros.com

"No es ciencia ficción. La tecnología ya está cambiando el trabajo, para bien o para mal. 85 millones de empleos van a experimentarlo antes de 2025 en todo el mundo", destaca en la introducción de su libro, la economista **Lucía Velasco.**

Actual Directora de ONTSI (el Observatorio Nacional encargado del estudio de la digitalización y el impacto de la tecnología en la sociedad) y cofirmante -junto con **Luis Muñoz-** de su reciente estudio 'Indicadores sobre confianza digital y ciberseguridad en España y la Unión Europea', en este libro parte de que, en países como España, "la automatización podría afectar a la mitad de los puestos. Contratos, pensiones, habilidades, formación, estudios universitarios...". Y plantea una interesante reflexión de cómo prepararse ante este futuro cercano para tener claro qué ha supuesto la pandemia, qué se debería estudiar para estar preparado ante nuevos perfiles profesionales, cómo será el futuro del trabajo para las mujeres e, incluso, propone una 'caja de herramientas para gobernantes', expuestas de modo sucinto pero de no poco interés para correcciones de rumbo absolutamente perentorias.

ANÁLISIS PRÁCTICO DE SANCIONES EN MATERIA DE PROTECCIÓN DE DATOS DIVIDIDAS POR CONCEPTOS Y SECTORES



Autoras (Coordinadoras): Elena y Laura Davara
Editorial: Monografías Aranzadi
Año: 2021 - 800 páginas
ISBN: 9788413910321
www.marcialpons.es

Este libro ofrece a través de una notable recopilación dirigida por las expertos Elena y Laura Davara –herederas de una solvente dinastía de especialistas en la materia– un análisis práctico de sanciones impuestas tanto por parte de la AEPD, así como de otros organismos análogos de fuera de nuestro país. Dividido por sectores (banca, seguros, redes sociales, etc.) y por conceptos clave (información, videovigilancia, consentimiento, delegado de protección de datos y datos de salud, entre otros) el lector podrá encontrar, de forma rápida y precisa, los casos que le sean de mayor interés, incluyendo en su información un análisis de sus antecedentes, las alegaciones presentadas y la razón de la sanción.

Por ello, se trata de una obra extensa y de consulta profesional que, seguro, facilitará la labor de los Delegados de Protección de Datos (DPO), asesores jurídicos en esta materia y CISOs más directamente concernidos, gracias a su planteamiento práctico, que permite resolver dudas y conocer qué hacer en cada situación.