TECNOLOGÍAS DE CIBERSEGURIDAD

Autor: Rafa López
Editorial: Publicación independiente
Año: 2024 – 183 páginas
ISBN: 979-8-324-05940-8
www.amazon.es

Reconocido profesional y conferenciante en el sector más técnico, **Rafa López** se estrena como autor con esta obra pensada para entender y comprender el ecosistema de ciberseguridad. "Las tecnologías que son necesarias para proteger el entorno digital, pero, también, los procedimientos necesarios a seguir a la hora de diseñar un entorno seguro para nuestra organización", destaca.

Dirigida a un público que necesita iniciarse en este mundo, ya sea de sectores tecnológicos o de cualquier otro ámbito, y que quiera aprender desde cero, la obra es un buen punto de partida tanto para profesionales experimentados, como para iniciados, por el excelente repaso que ofrece de conceptos básicos, que siempre viene bien refrescar, como de nuevas tecnologías aplicadas a la ciberprotección.

Así, el lector podrá desde aprender conceptos y acrónimos, tanto clásicos como los más recientes, aplicados a este ámbito, hasta 'vivir' en primera persona cómo estas tecnologías permiten hacer frente en el día a día, en el sector público y privado, al cibercrimen, convirtiéndose también en una obra excelente para impulsar la concienciación en cualquier organización.

LA IA Y EL CONTROL ALGORÍTMICO DE LOS DERECHOS FUNDAMENTALES

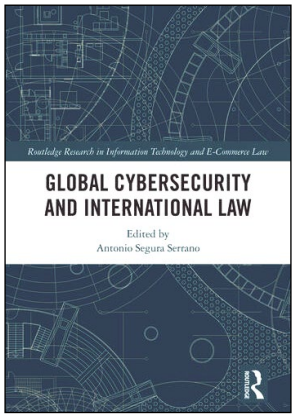
Autor: David Martín Herrera
Año: 2024 – 216 páginas
ISBN: 978-8-411-62477-0
www.lajuridica.es

Entender la forma con la que actualmente los algoritmos condicionan nuestras vidas es una materia extremadamente novedosa que parece quedar relegada al entendimiento de unos pocos expertos. Sin embargo, al despertar una mínima curiosidad por lo que es y de dónde proviene, el algoritmo nos sorprende que ésta no es una terminología moderna pero que, en las últimas dos décadas, se está convirtiendo en un *corpus* con capacidad de desplazar a la masa humana en buena parte de sus tareas.

Por ello, el autor plantea en esta obra, eminentemente profesional, muchos interrogantes dirigidos al público que aún no se cuestiona los retos legales que supone la aplicación de las nuevas tecnologías al ámbito corporativo y, también, al día a día de la gente pero que, sin duda, pueden condicionar la forma futura de vivir y relacionarnos supeditada a la "supremacía de unos pocos no elegidos por el pueblo", destaca su autor.

No deja de lado el análisis de cuestiones que afectan al ejercicio legítimo de los derechos fundamentales, tanto en su vertiente positiva como negativa, y propone algunos cauces que deberían aplicarse para que el libre ejercicio de éstos siga estando garantizado.

GLOBAL CYBERSECURITY AND INTERNATIONAL LAW



Autor: Antonio Segura Serrano (coordinador)
Editorial: Routledge
Año: 2024 – 230 páginas
ISBN: 978-1-003-34412-4
www.routledge.com

En un momento donde la geopolítica está de la mano con todo tipo de iniciativas cibernéticas maliciosas, es de especial relevancia el contenido de este volumen, a cargo de autores internacionales de reconocido prestigio, que cuenta con un excelente punto de vista la capacidad del derecho internacional existente para abordar la amenaza y el uso de la fuerza en el ciberespacio, redefiniendo la ciberguerra y la ciberpaz en la era del Internet de las Cosas.

El lector encontrará en él análisis en profundidad de temas candentes, como el incremento del ciberespionaje económico y su impacto, las herramientas legales para la cooperación internacional para combatir el cibercrimen, el uso de instrumentos de política exterior en la ciberdiplomacia, además de ofrecer varios apartados para analizar las ciberoperaciones maliciosas respaldadas por los Estados, así como qué grado de protección de los derechos humanos hay frente a las actividades de seguridad de algunos estados. No deja de lado varias reflexiones notables sobre las reformas necesarias por parte de las instituciones internacionales, como las Naciones Unidas, la Unión Europea, el Consejo de Europa y la OTAN, para proporcionar nuevas respuestas a las cuestiones críticas de la ciberseguridad global y el derecho internacional.

APRENDIENDO CIBERSEGURIDAD PASO A PASO

Autora: Alejandro Corletti Estrada
Editorial: Publicación independiente
Año: 2024 – 313 páginas
https://darFe.es

Interesantísima aproximación a la ciberprotección a cargo de un profesional de gran prestigio que ofrece en esta amplia obra amplia, en formato PDF y de descarga gratuita bajo licencia *Copyleft,* una recopilación de los contenidos de 50 ponencias divulgativas *on line*, impartidas en los últimos dos años –en la actualidad, ya superan el centenar–. Con ella, y de forma práctica, permite al lector ir 'paso a paso' para capacitarse en ciberseguridad "sobre una base sólida", destaca su autor.

Se trata, pues, de un complemento perfecto a las cuatro obras anteriores de **Alejandro Corletti** –'Seguridad por Niveles', 'Seguridad en Redes', 'Ciberseguridad, una estrategia informática/Militar' y 'Manual de Resiliencia'–.

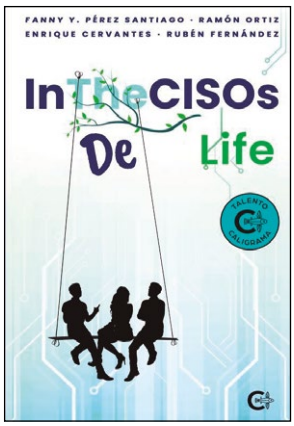
"Sus libros han sido durante años una referencia indispensable en el campo de la ciberprotección, especialmente dentro de la comunidad de habla hispana. Han servido de base para la formación de numerosos especialistas y son fuente de inspiración y consulta. Su temática abarca desde conceptos básicos hasta técnicas avanzadas, ofreciendo una visión completa y actualizada de los desafíos y soluciones en este área en constante evolución", destaca el autor del prólogo de la obra, **José Ignacio Bravo**, subrayando que esta edición es "un recurso imprescindible".

CIVILIZACIÓN ARTIFICIAL

Autor: José María Lasalle
Editorial: Arpa
Año: 2024 – 192 páginas
ISBN: 978-8-419-55845-9
https://arpaeditores.com

Se habla mucho de las extraordinarias oportunidades y riesgos de la IA. Sin embargo, apenas se piensa en lo que supone filosóficamente para la humanidad impulsar el desarrollo de 'algo' que está siendo programado para ser 'alguien' consciente al que se dota de capacidades cognitivas inimaginables, pero sin la conciencia ni los condicionantes morales que acompañan la existencia del creador a quien replica: el ser humano. "La IA es 'algo', todavía. Aunque no sabemos por cuánto tiempo. Va camino de convertirse en la apoteosis de una ciencia que, heredera de Hobbes, ha creído que el conocimiento es poder", destaca el siempre prolijo y didáctico **José María Lassalle**, ex secretario de Estado de Cultura y de Agenda Digital, que analiza con gran lucidez el reto del nihilismo tecnológico sobre el que sigue asentada nuestra sociedad. "Una corriente liderada por Estados Unidos y China para alcanzar la hegemonía mundial, mientras Europa busca una alternativa más humanista: una IA amigable, gobernada por una sabiduría aristotélica que reserve a los seres humanos un rol decisorio y decisivo dentro de la civilización artificial hacia la que nos dirigimos", recuerda en este ensayo de más que obligada lectura.

INTHECISOS LIFE



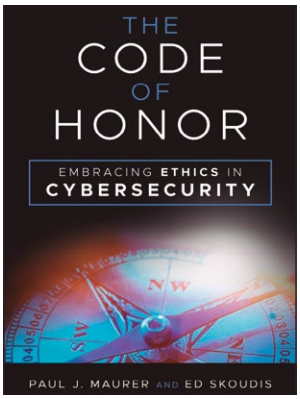
Autores: Fanny Y. Pérez, Ramón Ortiz, Enrique Cervantes y Rubén Fernández
Editorial: Caligrama
Año: 2024 – 152 páginas
ISBN: 978-8-410-26632-2
www.caligramaeditorial.com

Co-escrito por un equipo de conocidos veteranos en las lides de la ciberprotección, el libro –de intencionado título con doble sentido– ofrece una mirada original y auténtica al quehacer diario de este rol cada vez más valorado por las empresas, "alejándose de las convenciones habituales para introducirse en las vivencias personales y profesionales de aquellos que enfrentan diariamente los desafíos de proteger la información en la era digital", destacan sus autores, que recuerdan que esta obra huye de lo planteado en otros libros gracias a que está basada en "historias reales, a veces caóticas y otras divertidas".

Así, el lector podrá encontrar en sus páginas desde anécdotas sobre ciberataques hasta reflexiones sobre el estrés y la presión del trabajo, disfrutando de una perspectiva única y reveladora sobre la vida de estos profesionales.

A ello, se suma su estilo lleno de humor y sarcasmo con el que los autores muestran que ser un CISO va más allá de las siglas y los desafíos técnicos, sino que se basa en "construir una comunidad fuerte y unida en un mundo cada vez más interconectado y amenazante", comentan.

THE CODE OF HONOR: EMBRACING ETHICS IN CYBERSECURITY



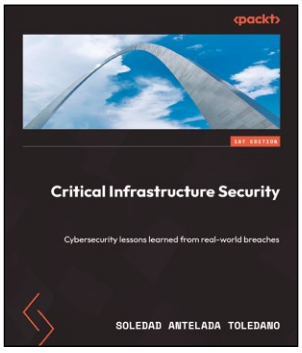
Autores: Paul J. Maurer, Ed Skoudis
Editorial: Wiley
Año: 2024 – 205 páginas
ISBN: 978-1-394-27586-1
https://onlinelibrary.wiley.com

Si bien algunas profesiones –incluidas la medicina, el derecho y la ingeniería– han adoptado un compendio de códigos de ética y conducta de amplio alcance, el campo de la ciberseguridad sigue careciendo de un estándar general. "Este vacío constituye una amenaza importante para la seguridad de los consumidores y las empresas, frena el comercio y retrasa la innovación", destacan los autores que ofrecen una discusión integral sobre los desafíos éticos que enfrentan los trabajadores, gerentes y ejecutivos de seguridad de la información.

Tanto **Ed Skoudis**, presidente del Sans Technology Institute College, como **Paul J. Maurer**, presidente del Montreat College, explican cómo muchas organizaciones y profesionales están desarrollando códigos deontológicos cada vez más adoptados. Así, en este libro, que también incluye consejos, recomendaciones y varios estudios de casos del mundo real, se muestran numerosas historias éticamente complejas a las que muchos profesionales del sector se enfrentan comúnmente.

En definitiva, el lector podrá conocer un "sistema completo de ética en ciberseguridad", así como los marcos más relevantes en este ámbito para la toma de decisiones éticas, basados en los adoptados en innumerables profesiones, credos y civilizaciones.

CRITICAL INFRASTRUCTURE SECURITY: CYBERSECURITY LESSONS LEARNED FROM REAL-WORLD BREACHES



Autora: Soledad Antelada
Editorial: Packt Publishing
Año: 2024 – 270 páginas
ISBN: 978-1837635030
www.packtpub.com

Una de las profesionales españolas con mayor proyección internacional –actualmente es Security Technical Program Manager Office of the CISO en Google, y fundadora de la iniciativa Girls Can Hack–, muestra en esta obra una visión general de los principios fundamentales de la ciberseguridad en infraestructuras críticas para ayudar a los profesionales a "cerrar la brecha de conocimiento asociada con la convergencia TI/OT, a través de ejemplos prácticos", comenta.

El lector encontrará desde apasionantes relatos sobre los ataques más comunes a la infraestructura crítica y sus sistemas, redes y activos, hasta una comprensión precisa y exhaustiva de aspectos como el ciclo de vida de una vulnerabilidad y cómo evaluarla y administrarla. No falta abundante información de los principales riesgos, como ataques DDoS y APTs, mostrando cómo se activa, opera y tiene éxito cada tipo de amenaza, prestando atención también a lo que supone el avance de la IA y la computación cuántica, a la infraestructura heredada.

En definitiva, **Soledad Antelada** busca que el lector pueda "identificar, al finalizar el libro, los principios clave de ciberseguridad que pueden ayudar a mitigar los ataques en evolución a la infraestructura crítica".