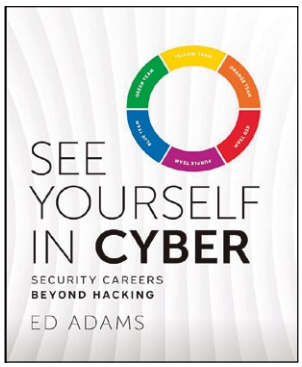
SEE YOURSELF IN CYBER: SECURITY CAREERS BEYOND HACKING

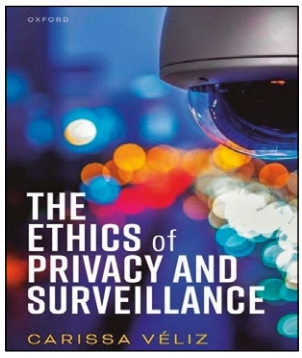


Autor: Ed Adams
Editorial: Wiley
Año: 2024 – 256 páginas
ISBN: 978-1-394-22560-6
www.wiley.com

Fundador y director ejecutivo de la compañía Security Innovation, **Ed Adams** ofrece una interesante aportación a través de un ensayo en el que analiza los diferentes roles que hay en las empresas y que no están necesariamente en el departamento de ciberseguridad pero que contribuyen de forma notable a ella. A lo largo de sus capítulos, pone en valor la aportación de profesionales como desarrolladores, expertos en DevOps, la alta dirección, los directores generales y cómo todos, con concienciación y formación, pueden impulsar la madurez de la compañía en ciberprotección.

Así, utilizando la conocida analogía de la rueda cromática, el autor explica los roles y responsabilidades modernos de los profesionales que operan dentro de cada 'porción', con abundantes ejemplos y estudios de casos de éxito que evidencian la importancia de aplicar el enfoque que plantea Adams en su obra. Además, cuenta con la aportación, a través de entrevistas, de destacados referentes para, en definitiva, proponer una estrategia viable y una metodología específica para que todos los que están en cualquier empresa aporten su 'granito' en ciberprotección.

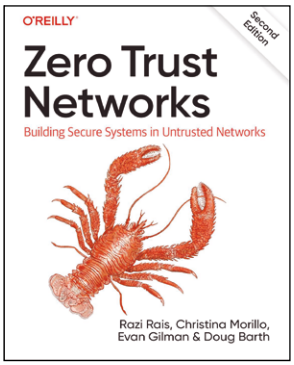
THE ETHICS OF PRIVACY AND SURVEILLANCE



Autora: Carissa Véliz
Editorial: OUP Oxford
Año: 2024 – 256 páginas
ISBN: 978-0-198-87017-3
www.oup.es/es

Tras su interesante 'Privacidad es poder: Datos, vigilancia y libertad en la era digital', **Carissa Véliz** vuelve en este reciente volumen a poner el foco en la importancia de la ética y la privacidad en una época donde la vigilancia digital se ha exacerbado por el uso intensivo de las nuevas tecnologías. Por ello, la especialista de Oxford, propone esta obra, con la que pretende contribuir a una mejor comprensión de la privacidad desde un punto de vista filosófico: qué es, qué está en juego en su pérdida y cómo se relaciona con otros derechos y valores. Así, las cinco partes que componen este libro responden a preguntas básicas sobre privacidad: ¿De dónde viene la privacidad? ¿Qué es la privacidad? ¿Por qué es importante? ¿Qué debemos hacer con ella? ¿Dónde estamos? Por la escasez de obras sobre ética en el ámbito digital, ésta resulta de gran interés ya que, sin duda, es una de las pioneras en profundizar en ella ante los riesgos que supone la IA y la demanda de datos de todo tipo que precisa para su entrenamiento, vinculado a todo tipo de modelos de negocio. Por ello, "es hora de que la filosofía mire más de cerca la privacidad", comenta Véliz.

ZERO TRUST NETWORKS: BUILDING SECURE SYSTEMS IN UNTRUSTED

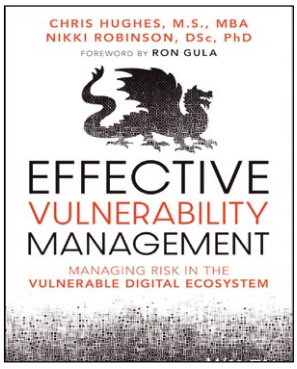


Autores: Razi Rais, Christina Morillo, Evan Gilman y Doug Barth
Editorial: Oreilly & Associates
Año: 2024 – 332 páginas
ISBN: 978-1-492-09659-7
www.oreilly.com

Excelente obra para profundizar en este enfoque a través de cuatro profesionales de reconocido prestigio en este ámbito. A lo largo de sus páginas, el lector, de carácter eminentemente profesional, podrá conocer diferentes recomendaciones y aproximaciones a la Confianza Cero, dando especial protagonismo a aspectos como la autenticación, la autorización y el cifrado en todo momento, además de disponer de acceso compartimentado y agilidad operativa. Aspectos que permitirán poner en marcha una arquitectura de una red de Confianza Cero, a partir de las tecnologías actuales. Además, incluye varios casos prácticos que permiten conocer aproximaciones de compañías que ya apuestan por Zero Trust, a través de conceptos como motores de confianza, de política y agentes de contexto. "Este modelo incorpora la seguridad dentro del funcionamiento del sistema, en lugar de superponerla", resaltan sus autores, que analizan las diferentes arquitecturas, estándares y marcos en está área.

EFFECTIVE VULNERABILITY MANAGEMENT

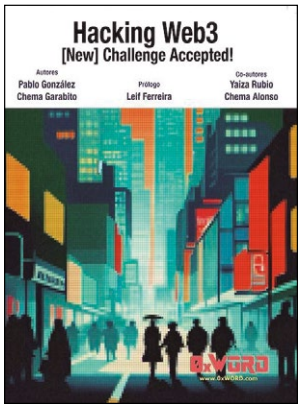
Managing Risk in the Vulnerable Digital Ecosystem



Autores: Chris Hughes, Nikki Robinson
Editorial: Wiley
Año: 2024 – 288 páginas
ISBN: 978-1-394-22120-2
www.amazon.com

Las organizaciones dedican una enorme cantidad de tiempo y recursos a abordar las vulnerabilidades de su tecnología, software y organizaciones. Pero, ¿están bien invertidos ese tiempo y esos recursos? Bajo esta premisa, los coautores Hughes y Robinson ofrecen una obra, eminentemente práctica, que permite tener un excelente conocimiento sobre cómo aplicar una gestión eficaz de vulnerabilidades a través de prácticas, procesos y herramientas que buscan permitir a las organizaciones actuales mitigar el riesgo de manera eficiente y oportuna en la era de la nube, DevSecOps y Zero Trust. Además, describe de forma exhaustiva las tareas de evaluación, planificación, monitorización y asignación de recursos para evitar este tipo de fallos de seguridad, "permitiendo a los lectores eliminar pasos innecesarios, simplificando el proceso de protección de los datos y las operaciones de la organización". Asimismo, el libro "cubre dominios emergentes clave, como la seguridad de la cadena de suministro de software y los factores humanos en la ciberseguridad". Desde luego, una interesante aportación de un tema que, cada año, continúa siendo foco de muchos de los grandes ciberincidentes.

HACKING WEB3: [NEW] CHALLENGE ACCEPTED!



Autores: Pablo González, Chema Garabito. Prólogo: Leif Ferreira
Coautores: Yaiza Rubio y Chema Alonso
Editorial: 0xWord
Año: 2024 – 254 páginas
ISBN: 978-8-409-53983-3
https://0xword.com

Interesante aproximación para aplicar la ciberseguridad al denominado 'mundo de la Web3', la nueva Internet, descentralizada y basada en *blockchain*, que por muchos ya es considerada el nuevo paradigma técnico-económico. Y, como sus posibilidades son casi infinitas, ya hay notables proyectos con ella en todo tipo de ámbitos. Precisamente, para aportar la capa de protección cibernética, los autores y coatores de esta obra que es pionera en el panorama técnico bibliográfico en castellano, buscan a lo largo de sus siete capítulos ofrecer una valiosa información sobre cómo auditar, desarrollar de forma segura y conocer las vulnerabilidades a las que se enfrentan los proyectos de Web3. En definitiva, permiten entender, de forma didáctica, sus diferentes elementos, para aplicar la lógica a proyectos en ella, por ejemplo, implementando *smartcontracts* y evitando muchas de las vulnerabilidades frecuentes en este ámbito. Además, ofrece abundante información de herramientas para mejorar el desarrollo y la calidad del código, así como para proteger e identificar tus proyectos. Incluso se propone aprender con un CTF en Web3.

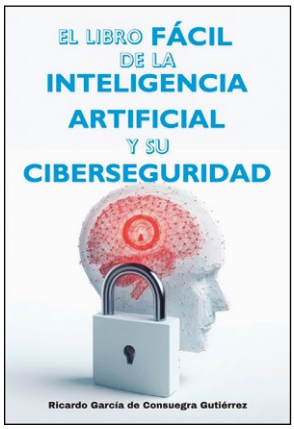
SECURITY IN THE CYBER AGE

An Introduction to Policy and Technology

Autor: Derek S. Reveron
Editorial: Cambridge University Press
Año: 2023 – 412 páginas
ISBN: 978-1-009-30858-8
www.cambridge.org

El ciberespacio es esencial para socializar, aprender, comprar y, en definitiva, realizar numerosas actividades en la vida moderna. Sin embargo, también tiene un lado oscuro: actores subnacionales, transnacionales e internacionales están desafiando la capacidad de los gobiernos soberanos de proporcionar un entorno seguro para sus ciudadanos. Según explica el autor de este libro, "los grupos criminales mantienen como rehenes a empresas y gobiernos locales mediante *ransomware*, los servicios de inteligencia extranjeros roban propiedad intelectual y realizan operaciones de influencia, los gobiernos intentan reescribir los protocolos de Internet para facilitar la censura y los ejércitos se preparan para utilizar operaciones en el ciberespacio en guerras". Por ello, con esta obra, busca ofrecer unas claves para entender cómo funciona el ciberespacio, así como el *modus operandi* de los actores estatales y no estatales aprovechándose de vulnerabilidades. Una obra, de carácter científico, que permite profundizar en formas tecnológicas, políticas y éticas de proteger el ciberespacio con un enfoque interdisciplinario.

EL LIBRO FÁCIL DE LA INTELIGENCIA ARTIFICIAL Y SU CIBERSEGURIDAD



Autor: Ricardo García de Consuegra Gutiérrez
Editorial: Publicación independiente
Año: 2024 – 150 páginas
ISBN: 979-8-875-70102-3
www.amazon.es

Curiosa aproximación a la Inteligencia Artificial desde un punto de vista de la ciberprotección, para los que busquen una obra sencilla de entender, aunque muy práctica. A lo largo de sus seis capítulos García de Consuegra, profesional con una amplia trayectoria en ciberseguridad, repasa desde qué cambios conlleva la IA, qué supone para la seguridad cibernética y cómo está impactando en el trabajo de los están en este sector.

Con un estilo ameno, abundantes ejemplos e historias curiosas, permite ir profundizando en los conceptos que hay que tener sobre esta tecnología y cómo se está aplicando, para bien y mal, a la ciberseguridad. Además, cuenta con un apartado final lleno de reseñas bibliográficas y enlaces con muchas aplicaciones y herramientas recientes, también, para protegerse de los ataques que ya la usan en el día a día.

LA TRANSFORMACIÓN DE LA GUERRA EN EL SIGLO XXI

Estudios estratégicos para su comprensión

Coordinadores: Alberto Bueno y Guillem Colom-Piella
Editorial: UNED
Año: 2024 – 212 páginas
ISBN: 978-84-362-7878-1
https://portal.uned.es

Este libro coral aborda algunas de las cuestiones más relevantes para comprender un fenómeno político, la guerra, que marca de forma radical las agendas nacionales e internacionales en la actualidad. Desde la asunción de que la naturaleza del conflicto armado permanece constante, se observa que muchos de sus elementos definitorios están experimentando en el siglo XXI un profundo proceso de transformación tecnológica, social, organizativa o informativa.

Por ello, según destacan sus autores, "el impacto multidimensional de la guerra exige la adecuada comprensión de sus dimensiones estratégica y militar. Así, los Estudios Estratégicos son el campo de conocimiento preocupado por el análisis en profundidad de conceptos y procesos vinculados con el empleo de la fuerza armada". Esa es la razón de esta obra, en la que participan grandes especialistas en este ámbito, como **Alberto Guerrero, Beatriz Cózar, Christian Villanueva, Rocío Vales, Jesus Román, Samuel Morales** y **Javier Miguel Gil,** quien, precisamente, es el autor del capítulo dedicado a la ciberguerra y sus implicaciones estratégicas.