



CHIPS Y PODER

Autores: Emilio García García / Marimar Jiménez Páez
Editorial: Catarata
Año: 2025 – 240 páginas
ISBN: 978-8-410-67260-4
www.catarata.org

los chips más eficaces tomará la delantera en inteligencia artificial y en las futuras olas tecnológicas. Y es que los chips se han convertido en la piedra angular de la era digital. Su fabricación, un proceso complejo y costoso, impulsó la globalización y la interdependencia económica. Sin embargo, la creciente tensión entre potencias ha convertido la cadena de suministro en un campo de batalla estratégico. Por eso, el interés de este ensayo es que profundiza en cómo esta lucha está transformando el orden internacional, impulsando el neoproteccionismo y redefiniendo alianzas. ¿Cómo hemos llegado hasta aquí? ¿Por qué nuestro futuro depende de estos diminutos pero poderosos componentes?

Prologado por **Jordi Sevilla**, **Emilio García**, exdirector de Gabinete de la Secretaría de Estado de Telecomunicaciones e Infraestructuras Digitales, y la periodista de El País y Cinco Días, **Marimar Jiménez**, plantean, de forma amena y con gran precisión, la “feroz batalla tecnológica” que vive el mundo, “donde el dominio de los chips definirá la hegemonía global”. Una tensión en la que China y EE.UU. compiten por liderar la carrera, conscientes de que quien logre fabricar

GUÍA PRÁCTICA DEL REGLAMENTO DE INTELIGENCIA ARTIFICIAL



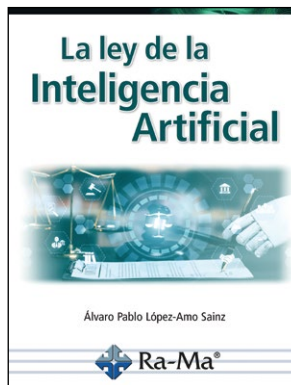
Autor: Carlos Fernández Hernández
Editorial: Aranzadi La Ley
Año: 2025 – 300 páginas
ISBN: 978-8-410-36027-3
tienda.aranzadilaley.es

sino también, va a requerir de un diálogo permanente entre ellos y con expertos en otros ámbitos, como la ciencia de datos, la informática, la estadística, la sociología y la ética”, destaca su autor.

Así, este volumen de **Carlos Fernández** se erige en manual de ayuda a los profesionales que deben aplicar de una u otra manera esta normativa, y a los estudiantes que se inician o continúan en su estudio, a conocer los principales contenidos de esta norma, a partir de un análisis sistemático, a fin de facilitar su cumplimiento, al menos en los momentos iniciales de su entrada en vigor y aplicación.

Abordando el mismo tema que la obra anterior, pero más centrada en el ámbito profesional del Derecho, este volumen se centra en los aspectos más complejos a la hora de cumplir esta norma extensa y compleja, de alto componente tecnológico, cuyo articulado diseña un intrincado conjunto de obligaciones a cargo tanto de las empresas, como de las administraciones públicas que utilicen esta tecnología. “Cumplir el RIA va a exigir, a los profesionales del Derecho y a los de la tecnología, no solo de un estudio detallado de la norma,

LA LEY DE LA INTELIGENCIA ARTIFICIAL



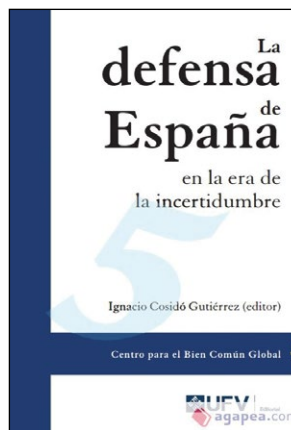
Autor: Alvaro Pablo López-Arno Sainz
Editorial: Editorial Ra-Ma
Año: 2025 – 362 páginas
ISBN: 978-8-410-36027-3
www.ra-ma.es

La obra de **Álvaro Pablo López-Arno Sainz** comienza con una introducción a la IA y su creciente impacto en diferentes sectores, seguido por una explicación detallada de los conceptos básicos legales y la aplicación práctica de la ley en el ámbito de la propiedad intelectual, la privacidad, los recursos humanos o los derechos de los trabajadores, entre otros. Utilizando ejemplos prácticos y casos reales, el libro ilustra cómo se aplican las leyes actuales de IA y desarrolla los desafíos legales emergentes.

Y lo más importante, aborda de qué forma podemos proteger nuestros derechos de un uso indebido o un mal funcionamiento de estas tecnologías y cómo podemos ejercer nuestros derechos para reparar el daño que se haya causado.

Dos meses después de entrar en vigor las prohibiciones de la Inteligencia Artificial, y a pocos meses más de que también se incremente el control contra las aplicaciones más críticas, es de interés leer, con un lenguaje claro, didáctico y sin tecnicismos, los aspectos fundamentales de la Ley de la Inteligencia Artificial, dando a conocer la normativa ya vigente sobre la materia y la que en un futuro próximo entrará en vigor.

LA DEFENSA DE ESPAÑA EN LA ERA DE LA INCERTIDUMBRE



Autores: Ignacio Cosidó (editor) y otros
Editorial: Universidad Francisco de Vitoria
Año: 2025 – 182 páginas
ISBN: 978-8-410-08371-4
www.editorialufv.es

mañana multidominio, con la necesidad de sincronizarse con el resto de las capacidades del estado para influir, entendiendo la influencia como un concepto que abarca desde el apoyo y la disuasión hasta la reacción mediante la fuerza militar. Así, entre la más de una decena de expertos que escriben cada capítulo, también se dedica un destacado apartado al ciberespacio, escrito por **Enrique Cubeiro**, actual director de **Ghenova Ciberseguridad**, además de haber sido jefe del Estado Mayor del entonces Mando Conjunto de Ciberdefensa.

También, se dedican capítulos a las operaciones militares en el ámbito cognitivo y multidominio, a la necesidad de la reserva y movilización, así como al presupuesto necesario para atender los retos de este momento con un interesante apartado como conclusión, centrado en las necesidades españolas, a cargo de **Ignacio Cosidó** y **Wenceslao Sánchez**.

La política de defensa, así se reconoce en nuestra estrategia de seguridad, es una política de Estado que, como tal, necesita estabilidad, estudio, reflexión, voluntad política y decisiones ágiles que permitan su adaptación a los cambios estratégicos y al impacto tecnológico agresivo y veloz del siglo XXI. En este libro sobre la defensa de Europa en un cambio de época, se habla de medidas que den confianza a nuestra sociedad europea hoy y aseguren su pervivencia como elemento nuclear de la civilización occidental mañana. Y, a la vez, se tratan temas como la idea de que las operaciones militares son ya y lo serán

ARQUITECTURA DE SEGURIDAD Y PATRONES DE DISEÑO SEGURO



Con la profundidad propia de **Elías Grande**, reconocido ponente y escritor en el ámbito, este nuevo libro, en el que ha invertido más de dos años, aborda los diferentes tipos de arquitecturas software más extendidas a día de hoy a nivel industria como son: las arquitecturas orientadas a servicios, las orientadas a eventos, las de microservicios y las de Internet de las Cosas. Y para cada una de ellas, el autor analiza en detalle sus características, así como sus patrones de diseño arquitecturales más relevantes, teniendo en cuenta los diferentes aspectos y componentes de seguridad a considerar al implementar

Autor: Elías Grande
Editorial: Oxword
Año: 2025 – 228 páginas
ISBN: 978-8-409-65948-7
Oxword.com

cada uno de ellos. Este enfoque proporciona a las disciplinas de seguridad ofensiva y defensiva, de auditoría, y de diseño y desarrollo, el conocimiento y herramientas necesarias para aplicar por diseño la seguridad en las aplicaciones. “Los activos más importantes para cualquier organización son sus usuarios y sus datos. Los usuarios son los que consumen los servicios ofrecidos por las aplicaciones de la organización, y son a través de estas aplicaciones por las que fluyen sus datos e información”, destaca el autor que, por esa misma razón, apremia a “mejorar la comprensión y entendimiento, desde un punto de vista de seguridad, de las diferentes formas que pueden tomar estas aplicaciones en función de los modelos de negocio, casos de uso e infraestructura tecnológica disponible de cada organización”.

NEW PARADIGM OF SOCIAL HUMANOIDS



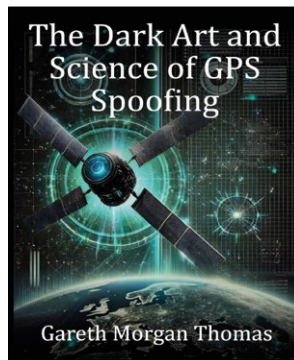
“La robótica no trata de máquinas, sino de crear compañeros que mejoren las capacidades humanas”, dice **Raffaello D’Andrea**. Así comienza esta obra, en versión digital e impresa, de carácter académico, en la que se ofrece una visión general, pero en profundidad con gran rigor y, también, de forma muy ilustrativa, del desarrollo de las tecnologías humanoides y su integración en la sociedad. Su objetivo es explorar cómo los robots humanoides, con inteligencia artificial, pueden mejorar la calidad de vida de los humanos en su día a día en tareas como las labores domésticas, en entornos médicos o, también, como herramientas educativas interactivas. Eso sí, también se dedica un amplio apartado a la preservación de los valores humanos junto

Autores: Balazs Barta, Krisztina Bardos, Marton Barta y otros
Editorial: Centro de investigación aplicada, desarrollo y capacitación de Pannon Business Network (PBN)
Año: 2025 – 172 páginas
ASIN: B0DT4PQY1L
www.amazon.com
https://m4dwwj-mf.myshopify.com

con el avance de la IA y la robótica y de cómo deben convivir ambos aprovechando lo mejor de ambos mundos.

Además, para profundizar en temas concretos cuenta con la participación de grandes especialistas europeos como **Árpád Rab** que escribe sobre los ‘Humanoides más allá de 2030’, **Ana Hafner** con un revelador análisis sobre las patentes de humanoides y, sobre todo, el capítulo dedicado a la ciberseguridad en este tipo de sistemas a cargo de **Marton Barta** y el siempre interesante **Alberto Partida**, colaborador habitual de SIC –en su columna ‘Cavilaciones seguras’–, y que disecciona de forma magistral los retos y cómo acometerlos en ciberprotección de este tipo de tecnologías que, seguramente, cambiarán nuestra forma de vivir en las próximas décadas.

THE DARK ART AND SCIENCE OF GPS SPOOFING: SATELLITE WARS, HIJACKED SIGNALS, AND THE INVISIBLE THREAT



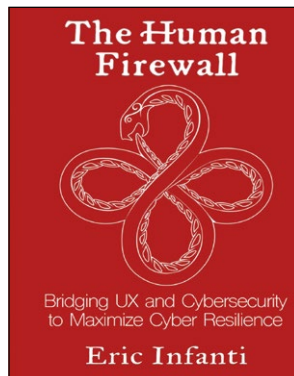
Autor: Gareth Morgan Thomas
Editorial: Publicación independiente
Año: 2025 – 265 páginas
ISBN: 979-8-305-60440-5
www.amazon.es

atacada por estados con recursos.

“En un mundo impulsado por la tecnología GPS, la amenaza invisible de la suplantación de identidad es muy grande. Desde operaciones militares y vehículos autónomos hasta sistemas financieros y navegación diaria, la suplantación de identidad GPS puede trastocarlo todo. Pero, ¿qué es la suplantación de identidad GPS? ¿Cómo funciona? Y, lo más importante, ¿cómo se puede detener?”. Así lo destaca el autor de este volumen cuya temática, por ser tan crítica y poco explorada, resulta fascinante y en el que desvela desde casos reales que se han dado de suplantación de GPS generando guerras por satélite, hasta de señales secuestradas y la amenaza invisible que supone esta tecnología tan crítica

La obra, eminentemente para el profesional de ciberseguridad, ofrece una mirada intensa a los fundamentos del GPS, la mecánica de la suplantación de identidad, numerosos estudios de casos del mundo real, así como las principales contramedidas que se pueden aplicar –protecciones criptográficas, antenas antisuplantación de identidad y sistemas de detección impulsados por IA, entre otras–. Además, dedica un amplio apartado al futuro de la seguridad de la navegación a través de tecnologías emergentes, como el GNSS cuántico y la autenticación basada en *blockchain*. “Ya sea que esté defendiendo sistemas críticos, explorando oportunidades profesionales o simplemente fascinado por las batallas invisibles en la era digital, este libro lo mantendrá informado, inspirado y a la vanguardia”, destaca su autor.

THE HUMAN FIREWALL. BRIDGING UX AND CYBERSECURITY TO MAXIMIZE CYBER RESILIENCE



Autor: Eric Infanti
Editorial: Publicación independiente
Año: 2025 – 114 páginas
ISBN: 979-8-305-82276-2
www.amazon.com

En el acelerado mundo digital de hoy, la ciberseguridad no se trata solo de *firewalls* y cifrado, sino de personas. El error humano representa el 95% de los incidentes, pero la mayoría de las soluciones de seguridad descuidan a las personas a las que pretenden proteger. ‘The Human Firewall’ fusiona los mundos del diseño de la experiencia del usuario (UX) y la ciberprotección para abordar uno de los mayores desafíos de la era digital: crear sistemas que no solo sean seguros sino, tam-

bién fáciles de usar. Escrito por **Eric Infanti** para diseñadores, desarrolladores, profesionales de la seguridad y ejecutivos, este libro va más allá de la jerga técnica para revelar el papel fundamental que desempeña el diseño UX en la creación de sistemas que permitan a los usuarios ser la primera línea de defensa contra las amenazas cibernéticas. Por eso, se convierte en una guía más que recomendable para los que estén creando un nuevo producto, mejorando un sistema existente o capacitando a su equipo, a través de herramientas, conocimientos y estrategias fáciles de usar y de eficacia probada en este ámbito.