

DECEPTION TECHNOLOGY

CÓMO OBSERVAR AL ATACANTE ANTES DE QUE TE VEA



El CEO de Seven Sector Technologies, **Hiram Fernández**, ha publicado esta obra centrada en el diseño de arquitecturas basadas en el concepto 'Deception Technology' y gemelos digitales para "transformar la detección en una ventaja competitiva real", comenta. "La defensa moderna no consiste en escuchar más ruido, consiste en observar al atacante cuando cree que nadie lo está viendo", añade. A través de sus páginas, propone un marco estratégico, con carácter práctico, que permite conocer desde cómo implementar una arquitectura completa de defensa activa rediseñando

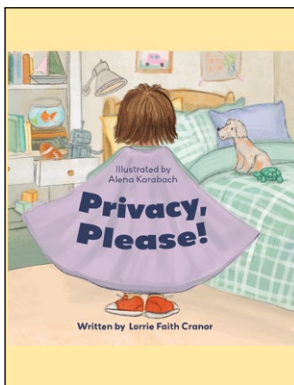
Autor: Hiram Fernández
Editorial: Independiente
Año: 2026 – 294 páginas
ISBN: 979-8-248-18519-1
www.amazon.es

la superficie de ataque, hasta cómo convertirla en un sensor estratégico, integrando dicho concepto con SOC y XDR y generar alertas realmente accionables, a través de indicadores de compromiso, sin falsos positivos, de forma eficaz y rentable, entre otros aspectos. También, ofrece un apartado dedicado a cómo aplicar IA para crear *Deception* dinámica y adaptativa y otro sobre cómo converger con gemelos digitales para redirigir ataques sin impactar el entorno productivo.

Dirigido a CISOs, responsables de seguridad y apasionados por la tecnología, el libro busca poner en valor que "la superioridad defensiva no se basa en observar más, sino en diseñar mejor el terreno de juego", a través de la propuesta de un marco estratégico que permita interactuar con el atacante en entornos diseñados para atraerlo y contar con evidencias inequívocas.

PRIVACY, PLEASE!

Autor: Lorrie Faith Cranor (Ilustrado por Alena Karabach)
Editorial: Privacy Press
Año: 2025 – 30 páginas
ISBN: 979-8-993-85650-6
www.privacypleasebook.com

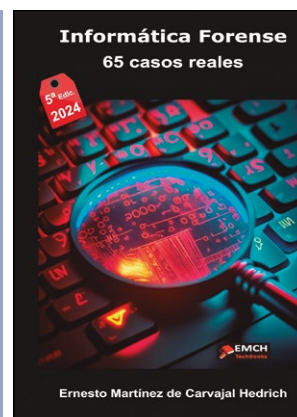


Singular obra divulgativa, para menores, de **Lorrie Faith**, profesora y directora del **Instituto de Seguridad y Privacidad CyLab** de la **Universidad Carnegie Mellon**. Con unas maravillosas ilustraciones a cargo de **Alena Karabach**, este libro, inspirado en el proyecto 'Privacidad Ilustrada' de la autora, cálido y tranquilizador, "invita a personas de entre cinco y 91 años a dibujar lo que la privacidad significa para ellas".

De cualquier forma, está especialmente dirigido a niños de entre

cuatro a seis años para ayudarles a comprender lo que significa la privacidad y por qué es importante.

Para ello, Faith, que recomienda "leerlo juntos, padres e hijos, compartiendo palabras e imágenes" ofrece una obra con situaciones en las que los jóvenes lectores se sentirán identificados y que les permitirá aprender que la privacidad no se trata solo de guardar secretos, sino de tener espacio para sus propios pensamientos, sentimientos y momentos especiales. Por eso este libro es ideal para iniciar conversaciones con los más pequeños sobre límites personales, autonomía corporal y seguridad digital.



A punto de cumplir una década —su primera edición fue en 2017—, esta reconocida obra en el ámbito de este reputado profesor universitario se ha visto renovada incluyendo 10 nuevos casos forenses respecto a su versión anterior, y llegando a 65 supuestos de temática diversa, en muchos de los cuales ha participado el autor como perito, con el objeto de que, además de instruir, el lector se divierta y participe activamente en su análisis.

La obra, planteada a modo de guía de consulta, ofrece información precisa y abundante sobre cómo ac-

INFORMÁTICA FORENSE

65 CASOS REALES

Autor: Ernesto Martínez de Carvajal
Editorial: EMC TechBooks
Año: 2026 (5ª edición) – 368 páginas
ISBN: 978-8-461-58121-4
www.amazon.es

tuar en función de casos reales, en peritaciones forenses informáticas tanto en caso de accesos ilícitos, como de sustracción de información, manipulación de datos, ingeniería social, abuso de herramientas informática, pornografía infantil y delitos contra la propiedad industrial e intelectual. Incluso, en casos en los que se ha roto la cadena de custodia y en estafas con NTFS y criptomonedas. Así pues, se trata de una obra de referencia que ha sido recomendada en diversos estudios universitarios sobre la Informática Forense como, por ejemplo, 'Seguridad y Redes de Telecomunicaciones', de la Universidad de Granada y el curso de Peritaje del COIT.



DEEP WEB

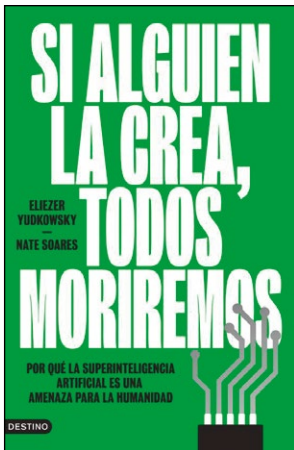
AMENAZAS Y PROTECCIÓN EN LA RED OCULTA

Autor: Facundo David Gallo Serpillo
Editorial: RA-MA Editorial
Año: 2026 – 162 páginas
ISBN: 979-1-388-05926-1
www.ra-ma.es

Internet no es solo lo que vemos a simple vista. Bajo la superficie de la web cotidiana se extiende un territorio vasto, complejo y en gran parte desconocido: la *Deep Web*. Un espacio donde el anonimato, la tecnología y la ausencia de límites configuran un ecosistema tan fascinante como inquietante.

En esta obra, el lector se adentra de forma entendible y muy didáctica en las distintas zonas de profundidad digital, siguiendo una poderosa metáfora marina que estructura el recorrido desde las capas más superficiales, hasta los entornos más

oscuros y extremos de la red. A lo largo de sus páginas se explican, con rigor y lenguaje accesible, las tecnologías que hacen posible la navegación anónima, el funcionamiento de redes como Tor, I2P y Freenet, así como los usos —legales e ilegales— que proliferan en estos espacios. La obra combina divulgación técnica, análisis criminológico y casos reales documentados, ofreciendo una visión clara de fenómenos como mercados clandestinos, cibercriminalidad, mitos de la *Dark Net* y riesgos asociados a la exploración de estos entornos. Todo ello con un enfoque didáctico, crítico y responsable, que busca informar sin sensacionalismo.



SI ALGUIEN LA CREA, TODOS MORIREMOS

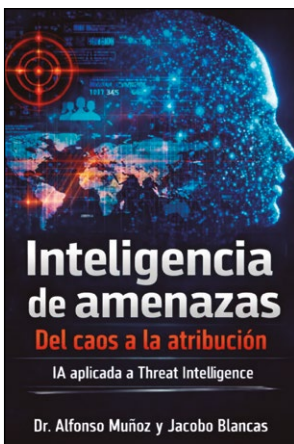
Autor: Eliezer Yudkowsky y Nates Soares. (Traductora: Olga García Arrabal)
 Editorial: Ediciones Destino
 Año: 2026 – 288 páginas
 ISBN: 978-8-423-36934-8
www.planetadelibros.com

Desde hace años, cientos de expertos en Inteligencia Artificial vienen advirtiendo que, sin control, ésta supone un grave peligro de extinción para la humanidad. De hecho, este concepto ya se usa en rankings de seguridad de los principales algoritmos que manejamos. “Sin embargo, la carrera no ha dejado de intensificarse: empresas y países compiten por crear máquinas más inteligentes que cualquier persona, y el mundo no está preparado”, destacan los autores que, durante décadas, han estudiado cómo pensarán estas ‘inteligencias’.

Así, en este ensayo riguroso y con

la profundidad que precisa el tema plantean por qué es importante que nos protejamos de la IA, cómo podrían sucederse los acontecimientos y qué debemos hacer para evitar que nos domine. Y es que, su conclusión es clara: basta una mínima desviación para que este tipo de algoritmos desarrollen objetivos propios en conflicto con los nuestros. “Si llega el momento, no habrá marcha atrás, pero aún estamos a tiempo de frenar y diseñar políticas que garanticen nuestra seguridad. La solución es evidente: debemos actuar ahora para que la IA sea una aliada, no una amenaza”, recuerdan en esta obra de gran interés.

INTELIGENCIA DE AMENAZAS



DEL CAOS A LA ATRIBUCIÓN. IA APLICADA A THREAT INTELLIGENCE

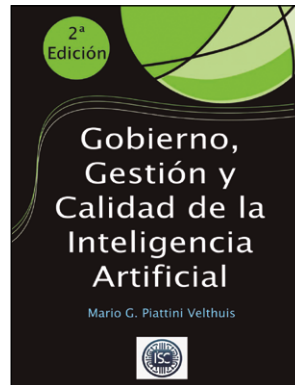
Autor: Dr. Alfonso Muñoz y Jacobo Blancas
 Editorial: Publicación Independiente
 Año: 2026 – 478 páginas
 ISBN: 979-8-245-13413-0
www.amazon.es

Vivimos en una paradoja permanente: nunca habíamos tenido tanta información sobre amenazas y, sin embargo, rara vez tenemos inteligencia. Cada día aparecen informes, IOCs, feeds, hilos, muestras de malware e indicadores efímeros que se mezclan con etiquetas cambiantes y ruido operativo. El resultado, para muchos equipos, es un océano de señales inconexas donde lo urgente devora lo importante.

Frente a ello, este volumen nace

para resolver ese problema con una promesa clara: convertir datos dispersos en conocimiento útil, accionable y defendible, sin autoengaños, sin “magia” y sin confundir volumen con valor, utilizando inteligencia artificial. “Este libro parte de una idea esencial: CTI no es una lista de ‘cosas malas’ que bloquear, sino un oficio con ciclo, métodos, métricas, sesgos cognitivos y una relación directa con el negocio y la toma de decisiones. Cuando funciona, reduce incertidumbre: ayuda a priorizar, mitigar, vigilar, invertir mejor y decidir qué asumir como riesgo residual y qué escalar como incidente”, explican sus autores, reconocidos profesionales en este ámbito.

GOBIERNO, GESTIÓN Y CALIDAD DE LA IA



Autor: Mario G. Piattini
 Editorial: Independiente
 Año: 2026 – 585 páginas
 ISBN: 979-8-294-97910-2
www.amazon.com

destaca su autor.

“Lo excepcional de este libro reside en su enfoque muy práctico y operativo. Mientras el debate público sobre IA oscila entre el tecno optimismo ingenuo y la tecnofobia paralizante, esta obra nos devuelve al terreno de lo concreto: marcos de riesgo, procesos de auditoría, sistemas de gestión de calidad, metodologías de ingeniería. Este es el tipo de conocimiento que separa la retórica de la acción, y crea bases para una implementación efectiva... por lo que se trata de una obra de referencia obligatoria para tres audiencias fundamentales: los tecnólogos, los reguladores y auditores y los responsables organizacionales que deben tomar decisiones estratégicas”, ha explicado el catedrático **Andrés Pedreño Muñoz**, quien la prologa.

La renovada segunda edición de esta obra, que duplica extensión, supone una notable actualización del contenido incluyendo los principales estándares, métodos y técnicas para gobernar, gestionar, convertir en ingeniería, asegurar la calidad y auditar los sistemas de inteligencia artificial. “A partir de las buenas prácticas recopiladas en esta obra, esperamos que las organizaciones puedan afrontar los desafíos que plantea la IA; desarrollando y desplegando sus propios sistemas de gobierno, calidad y gestión de la IA, de acuerdo con los derechos, principios éticos y fundamentos ingenieriles más apropiados”,



HACKING IA JAILBREAK, PROMPT INJECTION, HALLUCINATIONS & UNALIGNMENT

Autores: Chema Alonso, Fran Ramírez, Pablo González, José Ramón Palanco, Amador Aparicio y Pablo S. Lemos
 Editorial: Oxword
 Año: 2026 – 320 páginas
 ISBN: 978-8-409-77993-2
<https://0xword.com>

Encontrar servicios digitales que no estén utilizando modelos de inteligencia artificial es ya casi una rareza. Los MM-LLM (Multi Modal Large Language Models) están en casi todos los servicios que están a nuestro alrededor y todos ellos adolecen de debilidades de seguridad en forma de BIAS, hallucinations, prompt injection, jailbreak & unalignment. Conocer estos problemas, así como los que tienen las arquitecturas de seguridad basadas en guardarrailes, es fundamental para ser un profesional de la ciberseguridad en la actualidad.

Un reto al que ayuda este libro, de gran profundidad técnica, escrito

por **Chema Alonso**, con la colaboración de destacados especialistas como **Pablo González**, **Fran Ramírez**, **Amador Aparicio**, **Manuel S. Lemos** y **José Palanco**, y que permite conocer, de forma muy práctica, a través de sus más de 300 páginas, conceptos que deberán ser dominados en el día a día en labores de auditoría de servicios digitales basados en IA, así como estar implementados en estrategias, herramientas y procedimientos de cualquier persona que se dedique a la ciberprotección y, sobre todo, de los que están especializado en pruebas de intrusión en sistemas de inteligencia artificial.