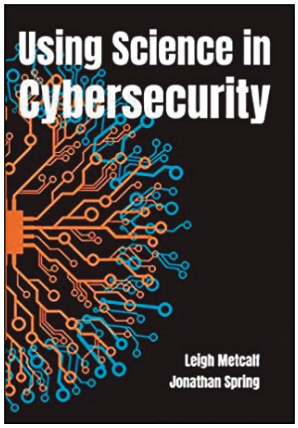
## USING SCIENCE IN CYBERSECURITY

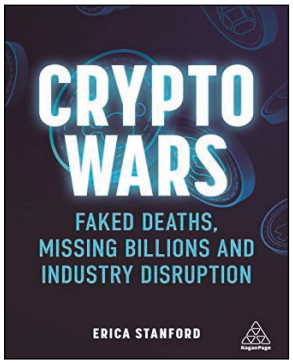



**Autores: Leigh Metcalf / Jonathan Spring**
**Editorial: World Scientific Publishing Company**
**Año: 2021 – 304 páginas**
**ISBN: 978-9811235856**
**www.worldscientific.com**

La implementación del método científico en ciberseguridad cuenta con todo tipo de apoyos para sacar el máximo provecho de la tecnología. Si bien la mayoría de las publicaciones sobre ello enfatizan que los principios científicos son necesarios, lo cierto es que pocos autores se han centrado en proponer obras de referencia que los descubran y permitan aplicarlos a la ciberprotección. Es un vacío que intenta cubrir este libro que brinda a los lectores herramientas prácticas que se pueden aplicar a la seguridad cibernética.

En él, sus autores examinan el camino necesario para desarrollar las bases de la ciberseguridad teniendo en cuenta los datos inciertos. Además, aportan numerosos ejemplos que muestran cómo implementar la ciberseguridad para resolver nuestros problemas cotidianos. De esta forma, se convierte en una obra de referencia tanto para estudiantes avanzados de pregrado y posgrado, como para investigadores y profesionales en los campos de la ciberseguridad y la seguridad de la información.

## CRYPTO WARS: FAKED DEATHS, MISSING BILLIONS AND INDUSTRY DISRUPTION

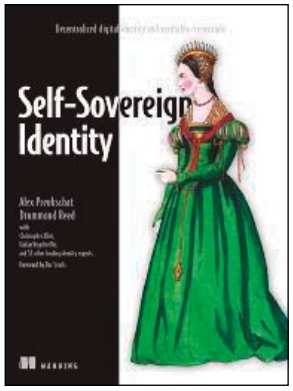



**Autor: Erica Stanford**
**Editorial: Kogan Page**
**Año: 2021 – 264 páginas**
**ISBN: 978-1398600683**
**www.koganpage.com**

"Las criptomonedas son una gran noticia. Es posible que usted mismo sea usuario o que tenga amigos que elogien su intención de hacerse rico rápidamente. Así pues, ármese con el conocimiento para llegar a la cima en las guerras criptográficas", destacó **Erica Stanford** en la presentación de este libro, que ofrece una interesante semblanza del mundo que se esconde tras las criptomonedas. "Si miles de personas pueden perder millones de dólares en OneCoin, ideado por la ahora infame Missing Cryptoqueen, que se hizo famosa por la serie de podcasts de la BBC y llamada 'una de las estafas más grandes de la historia' por The Times, ¿qué te hace pensar que tu dinero está seguro?", añade la autora.

En su libro, Stanford revela cómo afectaron a millones de personas, algunas de ellas conocidas celebridades, las estafas más impactantes de los últimos años en el mundo de las criptomonedas. Además, muestra de forma ilustrativa "los esquemas de manipulación de todo el mercado, los procesos no regulados y la nueva colección de tecnologías que, aunque a menudo se malinterpretan, se han explotado para crear el salvaje oeste de las criptomonedas". Sin duda, una obra imprescindible para comprender mejor esta tecnología que tiene el potencial de revolucionar la banca y el mundo como lo conocemos.

## SELF-SOVEREIGN IDENTITY: DECENTRALIZED DIGITAL IDENTITY AND VERIFIABLE CREDENTIALS

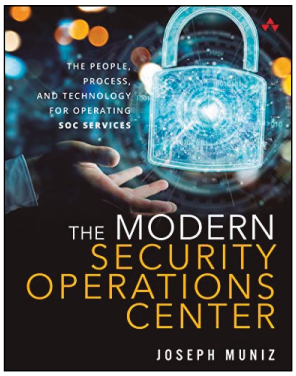



**Autores: Alex Preukschat / Drummond Reed**
**Editorial: Manning Publications**
**Año: 2021 – 504 páginas**
**ISBN: 978-1617296598**
**www.manning.com**

La identidad soberana (SSI) es un modelo de identidad digital en Internet gracias a la que se puede demostrar quiénes somos a los sitios web, servicios y aplicaciones con los que se precisa establecer relaciones de confianza, para acceder o proteger información privada. Impulsada por nuevas tecnologías y estándares en criptografía, redes distribuidas, computación en la nube y teléfonos inteligentes, la SSI es un cambio de paradigma que muchos especialistas consideran como un paso similar al que se dio cuando los primeros móviles se convirtieron en teléfonos inteligentes.

Sin embargo, "el cambio de SSI es más profundo que un simple cambio de tecnología: es un cambio en la infraestructura subyacente y la dinámica de poder de la propia Internet", destacan los autores de esta obra que, a su vez, recuerdan que "en un mundo de regulaciones de privacidad cambiantes, robo de identidad y anonimato en línea, la identidad es un concepto precioso y complejo". Para entender y profundizar más en este concepto, el libro ofrece un ilustrativo resumen de la situación de la SSI, así como sus principales aspectos y qué supone en todo tipo de ámbitos como la transferencia de propiedad, la banca electrónica o los servicios comerciales en línea.

## THE MODERN SECURITY OPERATIONS CENTER



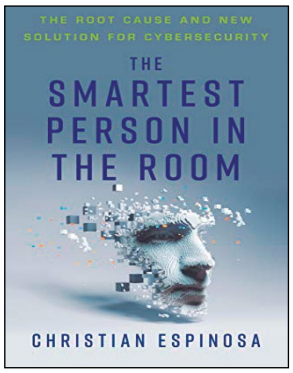

**Autor: Joseph Muniz**
**Editorial: Addison-Wesley Professional**
**Año: 2021 – 752 páginas**
**ISBN: 978- 0135619858**
**www.pearson.com**

Para los que buscan información de calidad sobre cómo construir, mantener y operar un Centro de Operaciones de Seguridad (SOC) moderno que sea capaz de brindar servicios de protección de la manera más eficiente y rentable posible esta obra es, sin duda, una buena fuente de consulta. Tanto por su calidad técnica como por la profundidad y extensión con la que aborda el reto de poner en marcha estas infraestructuras con equipos muy especializados.

Su autor, el arquitecto de seguridad, **Joseph Muniz**, permite conocer sus capacidades actuales, con amplias recomendaciones para alinear el SOC con el negocio y planificar su evolución para hacer frente a las nuevas amenazas.

En su obra, aborda los retos en personas, procesos y tecnología explorando cada servicio clave manejado por los SOCs más maduros y dando interesantes orientaciones para gestionar riesgos, vulnerabilidades y cumplimiento. Para ello, incluye abundantes ejemplos prácticos que también muestran cómo los equipos 'rojos' y 'azules' más avanzados trabajan en todo tipo de situaciones usando herramientas como Kali Linux y Ansible. En definitiva, Muniz ofrece una 'vista previa' del futuro de los SOC, incluyendo en él tecnologías en boca como la de Secure Access Service Edge (SASE) y apostando por una automatización cada vez más sofisticada.

# THE SMARTEST PERSON IN THE ROOM: THE ROOT CAUSE AND NEW SOLUTION FOR CYBERSECURITY

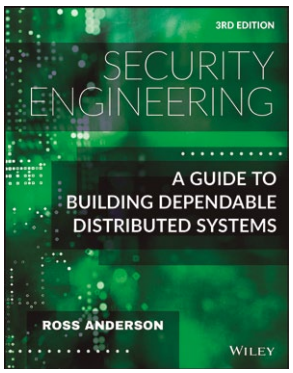



**Autor: Christian Espinosa**
**Editorial: Lioncrest Publishing**
**Año: 2021 – 280 páginas**
**ISBN: 978-1544516219**
**https://lioncrest.com**

Desarrollar las habilidades de las personas puede ser un desafío, sobre todo en un entorno tan complejo y cambiante como el de la ciberseguridad. Espinosa muestra cómo sacar partido y aprovechar los mejores talentos de la empresa para mejorar en ciberprotección. La obra, elaborada con un enfoque holístico, analiza la importancia de las llamadas 'habilidades blandas', muy demandadas en ciberprotección, y de cómo sacar partido a los grandes referentes de cualquier empresa a través de la comunicación, el liderazgo y la motivación.

"Muchas empresas y organizaciones se equivocan al pensar que contratar a las mentes más brillantes les ayudará a superar cualquier desafío", explica el autor, quien opina que, para tener éxito, hay que contar con "algo más que un coeficiente intelectual alto". Su propuesta pasa por una metodología, plasmada en siete pasos ilustrados con historias que "permiten desarrollar equipos de ciberseguridad cohesionados, capaces de sacar partido de su especialización y convertirse en referentes en su ámbito empresarial". Con ellos se propone un itinerario pensado para ayudar a fortalecer las habilidades de los empleados y mejorar la comunicación entre ellos, algo que Espinosa considera determinante.

# SECURITY ENGINEERING: A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS



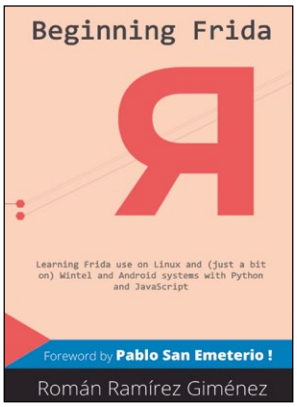

**Autor: Ross Anderson**
**Editorial: John Wiley & Sons Inc**
**Año: 2021–1.182 páginas**
**ISBN: 978-1119642787**
**www.wiley.com**

En la tercera edición de su conocida obra, **Ross Anderson**, profesor de la Universidad de Cambridge, profundiza en aspectos técnicos y organizativos para enseñar a los lectores cómo diseñar, desplegar y probar sistemas para evitar errores y resistir a ataques consiguiendo implementar sistemas distribuidos confiables.

En su primera edición (2001) este libro fue considerado uno de las más innovadores del año, estableciendo la disciplina de la ingeniería de seguridad. En su segunda versión (2008), el autor enriqueció la obra original mostrando cómo los mercados clandestinos han permitido a los cibercriminales especializarse.

Algo contra lo que, según Anderson, se puede luchar centrándose en la usabilidad. En esta edición, el autor explica que, a pesar de que el entorno ha cambiado por la nube, los dispositivos móviles y el IoT, los patrones de la delincuencia son los mismos. Frente a ellos, propone apostar por la criptografía y el control de accesos. En definitiva, el libro es un compendio exhaustivo, con más de 1.000 páginas, para repasar y profundizar en conceptos de la ingeniería de seguridad e implementar lo que Anderson considera el "gran desafío: conseguir una ciberseguridad sostenible" para proteger bienes duraderos críticos.

# BEGINNING FRIDA:
## Learning Frida use on Linux and (just a bit on) Wintel and Android systems with Python and JavaScript




**Autor: Román Ramírez**
**Año: 2021 – 335 páginas**
**ISBN: 979-8503684773**
**www.amazon.es/gp/product/B09536W8NH**

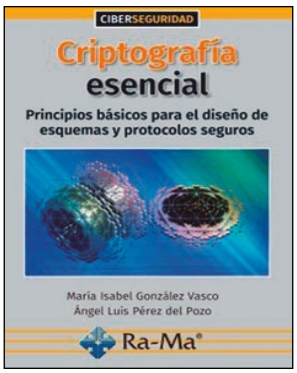
El siempre inquieto y prolífico experto **Román Ramírez** acaba de alumbrar Beginning Frida, un primer volumen centrado en el *framework* y la herramienta Frida, sin duda una de las más interesantes que pueden encontrarse en términos de *hooking* e instrumentación. No ya solo porque tiene multitud de funcionalidades y opciones potentes, sino además porque es muy fácil de usar, de emplear y de extender. Y, con cada nueva versión, es posible alcanzar nuevas metas en la instrumentación de aplicaciones, sin importar la plataforma. Es de reseñar que Frida soporta prácticamente todas las plataformas para las que puede compilarse su ejecutable), empleando una sintaxis muy sencilla, tanto en JavaScript como Python.

El objetivo de esta serie de libros –está previsto que le sigan tres más– es el de guiar a través de un camino de aprendizaje efectivo desde cero a ser competente en Frida, siguiendo las premisas de la metodología "aprender-haciendo" y, muy importante, con sentido del humor y disfrutando de los desafíos.

Dado que, para aprender a volar, primero necesitamos aprender a caminar, este primer volumen –de salida, en inglés, y próximamente en su versión en castellano– está centrado en aportar todas las herramientas y elementos necesarios para Frida: con ejemplos en Linux, Windows y Android.

Como bien corrobora en el prefacio el también competente **Pablo San Emeterio**, se insta a comprar este libro para 'caminar juntos' en el fascinante mundo del *hooking*, la instrumentación y, por supuesto, el *hacking* con Frida.

# CRIPTOGRAFÍA ESENCIAL. PRINCIPIOS BÁSICOS PARA EL DISEÑO DE ESQUEMAS Y PROTOCOLOS SEGUROS




**Autores: Mª Isabel González Vasco / Angel Luis Pérez del Pozo**
**Editorial: RA-MA**
**Año: 2021–234 páginas**
**ISBN: 978-8418551239**
**www.ra-ma.es**

Interesante novedad editorial para conocer, de manera sencilla, amena y didáctica las nociones básicas de la criptografía moderna. Partiendo de las nociones elementales de las matemáticas y la teoría de la complejidad, sus autores introducen al lector en el fascinante mundo de la criptografía presentándole los paradigmas de la clave pública y secreta, con numerosos ejemplos de construcciones clásicas y protocolos avanzados, así como técnicas de ataque y validación formal. Para facilitar el aprendizaje, cada capítulo incluye un test de autoevaluación, así como una breve lista de referencias actualizadas.

En definitiva, se trata de un libro que permitirá a los neófitos en la materia, familiarizarse con la terminología y nociones fundamentales que se utilizan en criptografía moderna, conocer los paradigmas de la simétrica y asimétrica y comprender aspectos elementales de seguridad demostrable, de modo que el lector pueda entender demostraciones matemáticas sencillas de protección y entender las implicaciones prácticas de los teoremas.