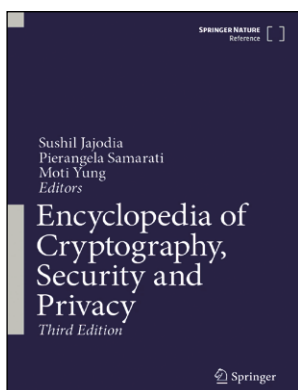


## ENCYCLOPEDIA OF CRYPTOGRAPHY, SECURITY AND PRIVACY



**Autores:** Sushil Jajodia, Pierangela Samarati y Moti Yung  
**Editorial:** Springer  
**Año:** 2025 – 2.817 páginas  
**ISBN:** 978-3-030-71520-5  
<https://link.springer.com>

Así pues, la obra ofrece una excelente recopilación de las nociones más importantes de hasta un total de 1.067 temas de criptografía, seguridad y privacidad, para hacerlas accesibles a investigadores con interés en tener claro todo tipo de conceptos. Y es que, el gran valor de este volumen es facilitar el acceso a las nociones más destacadas de estas áreas de forma tan concreta en pocos artículos.

Esta edición, que toma el relevo de su predecesora, de 2011, cuenta como principales novedades con la actualización de muchos conceptos que han evolucionado por los continuos avances tecnológicos que vivimos, un mayor peso a lo que lo que atañe a la privacidad y, también, una visión integral y cobertura al detalle de lo que supone en estos campos la llegada de nuevas tecnologías.

Se han escrito una gran cantidad de artículos y libros de calidad sobre criptografía, seguridad y privacidad, pero en su mayoría se dirigen a un lector académico con tiempo para empezar desde el principio y leer todo el texto. Por eso, el valor de esta tercera edición de la enciclopedia en dichas temáticas, cuyos autores han contado, también, con destacados referentes en la materia. Entre ellos, **Javier López Muñoz**, director del **NICS Lab** y catedrático de la **Universidad de Málaga**, que aporta, como editor de sección por segunda vez, su interesante opinión y conocimiento sobre estos ámbitos.



## LA TINTA INVISIBLE: DOMINA LA FIRMA DIGITAL

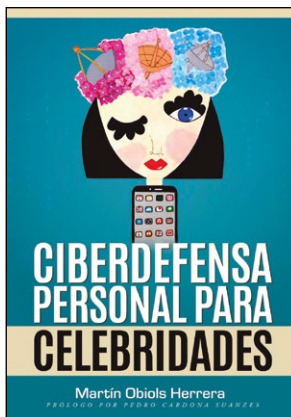
**Autora:** Rocío Casanova  
**Editorial:** SealSign  
**Año:** 2025 – 70 páginas  
**ISBN:** 978-8-409-72166-5  
[www.sealsign.es](http://www.sealsign.es)

de uso reales (en RR.HH., ventas, legal, salud, finanzas...), permitiendo tener claro cómo elegir la solución de firma adecuada para tu negocio, cuáles son los tipos de firma –simple, avanzada y cualificada–, así como las actuales exigencias normativas de la ley española y europea sobre firma digital y sus retos, a través de iniciativas como el ID Wallet que revolucionará nuestra identidad digital.

En definitiva, esta obra, de descarga gratuita a través de la web de la compañía, es una lectura imprescindible para profesionales, estudiantes y cualquier persona interesada en comprender la evolución de nuestra identidad en el mundo digital.

¿Te gustaría firmar documentos sin imprimir, sin escanear, sin perder tiempo... y con plena validez legal? Esta es la premisa a la que da respuesta la directora de **SealSign** (marca de **Factum**), **Rocío Casanova**, en esta obra, eminentemente práctica, que se ofrece más allá de ser una guía técnica, como herramienta de gran utilidad para empresas y profesionales de la era digital y de la IA. A través de sus páginas, se puede conocer desde los fundamentos legales sobre la firma digital, hasta los casos

## CIBERDEFENSA PERSONAL PARA CELEBRIDADES



**Autores:** Martín Obiols (Autor), Victoria Ruiz (Ilustradora), Pedro Cardona (Prólogo)  
**Editorial:** Publicación independiente  
**Año:** 2025 – 419 páginas  
**ISBN:** 979-8-311-61197-8  
<https://amazon.es>

estos perfiles altamente expuestos.

Con un enfoque prudente, riguroso y accesible, a lo largo de cinco apartados, 24 capítulos, cinco guías de referencia rápida y más de 250 notas, los lectores menos técnicos encontrarán explicaciones claras y sencillas para proteger su identidad y sus datos. Para los que busquen un nivel superior, también se ofrece información con tácticas avanzadas de seguridad operacional para enfrentarse a las amenazas más dirigidas. “Es un libro más exhaustivo que extenso, en el que he invertido dos años de trabajo pero que han dado, sin duda, una obra que puede servir tanto para mejorar la ciberprotección personal como para impulsar la cultura de ciberseguridad en las empresas a través de su lectura”, ha explicado su autor a Revista SIC.

Perfecta obra para los que quieran mejorar su ciberseguridad, sin tener grandes nociones de la materia. El autor, un referente en una conocida entidad financiera, ofrece un ‘manual de uso’ con todo tipo de consejos prácticos para perfiles destacados del ecosistema digital –desde cantantes, hasta *influencers*, políticos, y personas con puestos de responsabilidad– que precisan de una protección mayor, pero que, lógicamente, sirve para cualquier persona que quiera mejorar en este ámbito. En esta guía, el lector encontrará todo lo necesario para diseñar y aplicar una estrategia de ciberdefensa personal enfocada a



## GUERRAS COGNITIVAS

**Autor:** Daniel Iriarte  
**Editorial:** Arpa Editores  
**Año:** Mayo 2025 – 280 páginas  
**ISBN:** 978-8-410-31385-9  
<https://arpaeditores.com>

a la trastienda tecnológica, a los ejércitos virtuales, los *bots* y las aplicaciones de la IA, capaz de manipular informaciones, difundir mentiras, hundir reputaciones, propiciar odios y xenofobias, y hasta crear conflictos en la vida real que acaban en sangre, en masacres, en guerras”. Así de directo se muestra el periodista **Daniel Iriarte**, experto en geopolítica y amenazas híbridas, que plasma en este ensayo, meticuloso, muy ilustrativo y fruto de su gran experiencia como reportero más de medio centenar de países sobre cómo todo tipo de países están usando el ciberespacio para la guerra cognitiva como estrategia principal de influencia. “El campo de batalla es la mente de la población, que desconoce cómo los datos que un simple teléfono móvil recaba a cada segundo sirven para moldear los cerebros de millones de personas sin que siquiera lo perciban”, destaca.

¿De qué forma puede alterar una campaña en redes un resultado electoral? ¿Cuántas empresas llevan a cabo estas prácticas por motivos económicos? ¿Cómo políticos y grupos terroristas copian esas técnicas para sus propios fines? Detrás de ese fenómeno global se esconden las denominadas guerras cognitivas, que son, en definitiva, verdaderas estrategias de manipulación mental por medios digitales convertidas en un canal subterráneo de poder que ya mueve el mundo.

“Ya sea en la guerra de Ucrania o en el conflicto de Gaza, en las elecciones de Estados Unidos, de Rumanía o en los movimientos geopolíticos de China, el poder de influencia se ha desplazado

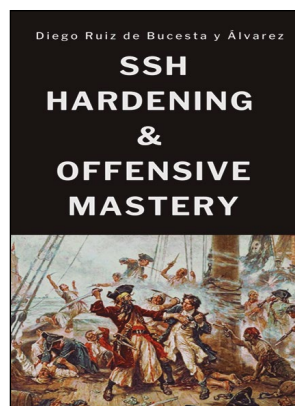


## HACKING HOME DEVICES II: POCS & HACKS JUST FOR FUN

**Autor:** Gerard Fuguet  
**Editorial:** OxWord  
**Año:** 2025 – 370 páginas  
**ISBN:** 978-8-409-69035-0  
<https://oxword.com>

Segunda parte de la obra que, sin duda, es ya una referencia en ciberprotección en dispositivos IoT domésticos y que muestra, tanto para profesionales, técnicos y no técnicos, las claves para saber lo que “se mueve en las cavernas cibernéticas”, destaca su autor. A lo largo de cinco extensos capítulos, **Fuguet** muestra desde cómo configurar puertos y servicios de todo tipo de dispositivos, hasta técnicas para reducir el denominado *sniffing* –para evitar que los cibercriminales ‘nos escuchan’ en nuestra Red–, hasta cómo auditar las redes del hogar o la oficina, además de disponer de alertas, paneles de control y una vi-

sión clara de que nuestro ‘ciberespacio personal’ tiene el mínimo riesgo frente a cualquier incidente cibernético, además de dedicar también un espacio a malas prácticas que hay que evitar. Sin duda, ahora que el teletrabajo es más habitual que nunca, este es un libro extenso y meticuloso para poner en práctica en el día a día de nuestro hogar conectado, haciendo que la ciberseguridad comience, de forma eficaz, con la vivienda de cualquiera que trabaje en este ámbito... o que quiera acercarse a él. “Recuerda que, tú eres propietario@ de tu república independiente y estableces las reglas que consideres”, destaca el autor.



## SSH HARDENING & OFFENSIVE MASTERY

**Autor:** Diego Ruiz de Bucesta y Álvarez  
**Editorial:** Ed. independiente  
**Año:** 2025 – 122 páginas  
**ISBN:** 978-8-412-95772-3  
<https://dsdsec.com>

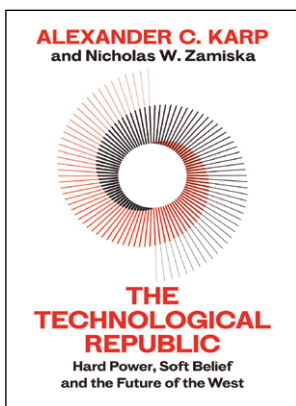
El autor permite conocer cómo fortalecer la seguridad del protocolo SSH (Secure Shell), fundamental para la administración remota de servidores. “Se trata de un recurso indispensable que cubre aspectos defensivos y ofensivos, incluyendo técnicas de túneles y secuestros”, ha explicado sobre él **Rames Sarwat**, destacado experto en este ámbito.

La obra comienza con abundante información sobre estrategias defensivas detalladas, entre las que muestra cómo acometer configuraciones seguras, autenticación de dos factores, Fail2Ban e integración con Suricata. A continuación, permite al lector profundizar en técnicas ofensivas a través de escenarios prácticos, eva-

luando vulnerabilidades y estrategias de mitigación, desde ataques básicos hasta avanzados, como el secuestro y el *malware* mediante túneles.

No falta en sus páginas el examen exhaustivo de posibles amenazas actuales como el conocido ataque Terrapin (CVE-2023-48795), además de profundizar, de forma técnica y muy especializada, en la exploración de túneles SSH, secuestro de agentes y herramientas en Tcpl/Expect y Perl. Por ello, este libro, dedicado al profesional que trabaja en estos entornos, es mucho más que una *checklist* permitiendo alcanzar un conocimiento profundo de la seguridad, tanto para los que ya trabajan en ello como para los que buscan dar los primeros pasos. Para facilitar su lectura se ofrece en descarga gratuita.

## THE TECHNOLOGICAL REPUBLIC



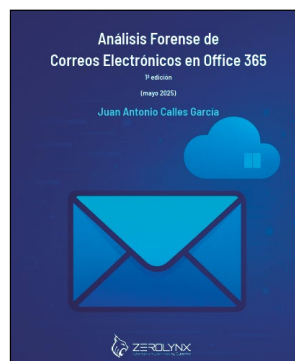
**Autores:** Alexander C. Karp y Nicholas W. Zamiska  
**Editorial:** Bodley Head  
**Año:** 2025 – 320 páginas  
**ISBN:** 978-84-09-65948-7  
<https://www.penguin.co.uk>

más brillantes colaboraron en su día con el gobierno para impulsar tecnologías que transformaron el mundo. Sus esfuerzos aseguraron el dominio de Occidente en el orden geopolítico. Pero esa relación se ha erosionado, con peligrosas repercusiones”, recuerdan a la vez que realizan una “crítica mordaz a nuestro abandono colectivo de la ambición”.

Por ello, en sus páginas, además de repasar y repensar los riesgos actuales de las nuevas tecnologías en las relaciones geopolíticas actuales, también argumentan que, “para que Occidente conserve su ventaja global y preserve las libertades que damos por sentadas, la industria del software debe renovar su compromiso de abordar nuestros desafíos más urgentes, incluida la nueva carrera armamentística de la inteligencia artificial”.

Gran éxito editorial en EE.UU. y una excelente obra para leer en los meses de verano por lo que plantea de crítica contundente a la cultura de complacencia de Occidente y un llamamiento apasionado a despertar “nuestra nueva realidad”, a través del análisis de dos referentes, como el cofundador y director ejecutivo de la conocida Palantir –sin duda uno de los grandes referentes en *big data* e IA aplicados a la Defensa–, **Alexander C. Karp**, y de **Nicholas W. Zamiska**. “Nuestras mentes de ingeniería

## ANÁLISIS FORENSE DE CORREOS ELECTRÓNICOS EN OFFICE 365



**Autor:** Juan Antonio Calles / Miguel Ángel Guergué (Prólogo)  
**Editorial:** Publicación independiente  
**Año:** 2025 – 234 páginas  
**ISBN:** 978-84-09-72674-5  
[www.zerolynx.com](http://www.zerolynx.com)

Presentado de forma oficial en el congreso **Osintomático Conference**, en mayo, y rindiendo homenaje a la obra X1Red+Segura, de **Ángel Pablo Avilés** –conocido como ‘Angelucho’–, que ha cumplido 12 años desde su publicación, el CEO de **Zerolynx**, **Juan Antonio Calles** ha escrito esta obra “con una intención clara y muy en la línea de mi gran amigo: educar y aportar valor a un sistema de justicia en el que los peritos tecnológicos estamos asumiendo un papel cada vez más relevante”.

Pensada para peritos, auditores, profesionales de la ciberseguridad y,

también, los que trabajan en el ámbito jurídico (desde jueces a fiscales y letrados a lo largo de sus 10 capítulos, se ofrecen una información exhaustiva desde cuáles son los fundamentos del análisis forense digital, cómo aplicarlos a Microsoft 365, el marco legal y pericial que hay que conocer para auditorías en este entorno, así como herramientas para el análisis de correos-e, diferentes tipos de investigación y cómo acometerla con éxito analizando las evidencias exportadas y manteniendo la cadena de custodia, entre otros aspectos de interés (incluso como abordar una prueba contrapericial). En definitiva, una obra de obligada lectura para los que trabajen en este ámbito. Además, se ofrece en descarga gratuita, en formato digital, desde la web de la compañía.