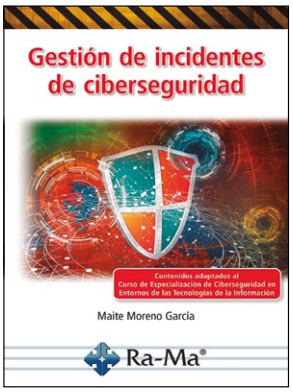
## GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD




**Autora: Maite Moreno García**
**Editorial: Editorial Ra-Ma**
**Año: 2022 – 202 páginas**
**ISBN: 978-8418971730**
**www.ra-ma.es**

Con un lenguaje claro y didáctico, **Maite Moreno** –experta de **S2 Grupo** y ponente en **Securmática**– ofrece una guía muy práctica para adquirir rápido los conocimientos necesarios para establecer y definir las líneas de actuación ante incidentes de ciberseguridad. Para ello, a lo largo de sus 10 capítulos, va desgranando los diferentes aspectos esenciales para gestionar crisis cibernéticas, partiendo de la taxonomía de los incidentes y analizando el papel que juegan los equipos de respuesta, qué capacidades deben tener, así como las herramientas, procesos y estándares más habituales.

También, ofrece información detallada de la utilidad de las plataformas de inteligencia de amenazas y cómo se monitorizan los incidentes. Por supuesto, no faltan abundantes ejemplos prácticos y un capítulo dedicado a las métricas e indicadores, así como la importancia de las 'lecciones aprendidas'.

Se trata pues de un libro de gran utilidad, tanto para los profesionales que trabajan en estos ámbitos, como para los que quieren acercarse a ellos. De hecho, los contenidos han sido adaptados para lo requerido en el módulo profesional de 'Incidentes de ciberseguridad', que se engloba dentro del 'Curso de Especialización de Ciberseguridad en Entornos de las Tecnologías de la Información' (del Título LOE).

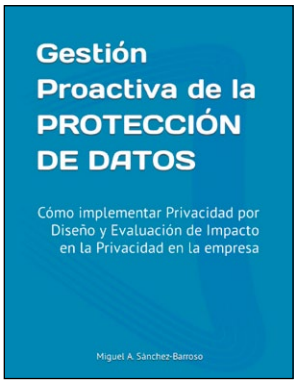
## MALWARE MODERNO: TÉCNICAS AVANZADAS Y SU INFLUENCIA EN LA INDUSTRIA

**Autor: Sergio de los Santos**
**Editorial: 0xword**
**Año: 2022 – 366 páginas**
**ISBN: 978-8409366231**
**0xword.com**

Con una redacción técnica, pero al alcance del público profesional, **Sergio de los Santos**, veterano de lides malagueñas del sector y experto en Telefónica, ofrece una excelente perspectiva –salvo el garrafal error de utilizar 'troyano' en lugar del apropiado 'Caballo de Troya'– sobre cómo ha evolucionado el software malicioso desde el año 2000 hasta hoy y qué pasos ha dado la industria de la ciberseguridad para hacerle frente, a través de normativas, tecnologías o regulaciones nacionales.

Así, la obra ofrece una rigurosa recopilación de las características de las muestras de *malware* más relevantes detectadas en las últimas dos décadas, acompañándolas de abundantes explicaciones, ejemplos y cómo se han analizado. Por ello, este libro, fruto de muchos meses de trabajo de uno de los grandes especialistas españoles en la materia, se convertirá posiblemente en obra de referencia para los que quieran comenzar y entender el mundo del *malware*, cómo funciona, cómo se analiza, y, también, para cualquier profesional de ciberseguridad que ya trabaje en este campo. No obstante, es, hasta la fecha, el libro más voluminoso de la editorial que no ha querido escatimar en páginas ante lo que considera una valiosa fuente de información.

## GESTIÓN PROACTIVA DE LA PROTECCIÓN DE DATOS




**Autor: Miguel A. Sánchez Barroso**
**Editorial: Publicación independiente**
**Año: 2022 – 236 páginas**
**ISBN: 978-1549513619**
**www.iberlibro.com**

Tras el éxito de su primera edición, en 2017, **Sánchez Barroso** ofrece una revisión actualizada y ampliada para ayudar a "implementar la Privacidad por Diseño y la Evaluación de Impacto en la Privacidad en la empresa", según se destaca en su portada. En ella, el lector encontrará un listado exhaustivo de los mejores métodos y herramientas que permiten llevar a cabo un programa de Gestión de la Privacidad basado en los requisitos de responsabilidad proactiva del Reglamento Europeo de Protección de Datos.

El autor, un reconocido profesional con más de una década de experiencia en privacidad y seguridad de la información con foco en escenarios financieros, aporta de forma precisa y muy 'al grano', a modo de manual, información completa y fácil de aplicar sobre cómo cumplir el enfoque de riesgos que ahora se exige en la normativa europea.

En definitiva, Sánchez Barroso permite acceder a abundante información sobre procesos esenciales que deben tenerse en cuenta, como el inventariado de tratamientos de datos o cómo realizar una evaluación de impacto en la privacidad. Sin duda una obra de referencia dada la escasa bibliografía, en castellano, existente sobre este tema.

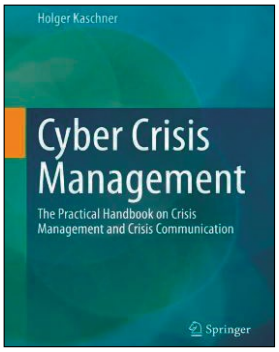
## CONFESIONES DE UN BOT RUSO

**Autor: Bot Ruso**
**Editorial: Debate**
**Año: 2022 – 224 páginas**
**ISBN: 978-8418619151**
**www.penguinlibros.com**

Bajo el pseudónimo de 'Bot ruso', el autor desvela que es un profesional que "ha pasado años manipulando conversaciones en Internet en una empresa de *astroturfing*", término referido a campañas de influencia. Precisamente, el valor de esta obra es la ilustrativa realidad que plantea, vivida en primera línea y en primera persona, mostrada de forma espeluznante a través del 'modus operandi' oscuro que utilizan empresas, partidos políticos y clubes deportivos, entre otros, para influenciar en la opinión pública. "He pasado bastantes años insultándote en redes sociales porque alguien me pagaba. Ahora que ya no estoy en nómina, quiero contarte cómo lo hacía", destaca su autor que confiesa que ha escrito el libro "desde el arrepentimiento ante el daño realizado".

Por eso, y en estos tensos tiempos que corren, se convierte en una obra de especial interés en el ámbito de la desinformación que, también, incluye numerosas indicaciones para anticiparse a este tipo de campañas, cada vez más sofisticadas y que "amenazan con dejar en manos de las grandes corporaciones el control de la información y la opinión pública". Con una prosa irónica y muy entretenida es una buena forma de conocer la 'trastienda' y consecuencias de lo que ha sido la popularización de la web 2.0 provocando que las redes sociales se hayan erigido como el mayor termómetro social.

## CYBER CRISIS MANAGEMENT: THE PRACTICAL HANDBOOK ON CRISIS MANAGEMENT AND CRISIS COMMUNICATION



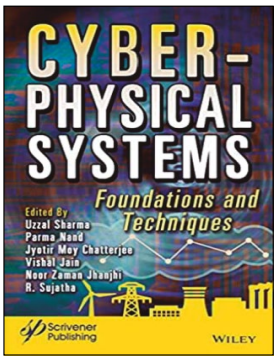

**Autor: Holger Kaschner**
**Editorial: Springer**
**Año: 2022 – 236 páginas**
**ISBN: 978-3658354886**
**link.springer.com**

Los ataques cibernéticos y los fallos de seguridad en TI amenazan a todas las organizaciones. Los incidentes se acumulan y, a menudo, forman el preludio de crisis complejas que amenazan a miles de empresas cada día. Por ello, el autor ha querido plasmar su experiencia –está especializado en crisis cibernética y la ISO 27032– en este volumen a modo de guía de consejos y buenas prácticas para ayudar a gestionarlas, así como a prepararse y prevenirlas.

En inglés –inicialmente fue publicado en alemán– y estructurado de forma muy intuitiva, está pensado para facilitar la labor de los profesionales que trabajan con equipos de respuesta a incidentes, en cualquiera de sus ámbitos, tanto el técnico como el más ejecutivo o el de comunicación. Por eso, incluye numerosas ilustraciones y listas de verificación e, incluso, un capítulo dedicado a los "siete pecados capitales de la gestión de crisis cibernética".

La obra resultará así de utilidad para una variedad de perfiles profesionales, que abarcan desde los miembros de los equipos de gestión de crisis, hasta los CIO y gerentes de TI, los delegados de protección de datos, los CSO y CISO y, por supuesto, los directores generales que quieran contar con una visión más precisa y exhaustiva de qué hacer en este tipo de situaciones.

## CYBER-PHYSICAL SYSTEMS: FOUNDATIONS AND TECHNIQUES



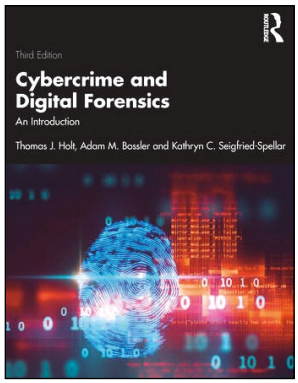

**Autores: Uzzal Sharma, Parma Nand, Jyotir Moy Chatterjee, Vishal Jain, Noor Zaman Jhanjhi, R. Sujatha**
**Editorial: Wiley-Scrivener**
**Año: 2022 – 336 páginas**
**ISBN: 978-1119836193**
**www.amazon.com**

Interesante aproximación a los denominados 'sistemas ciberfísicos' (CPS, por sus siglas en inglés) que representan la interconexión de los virtuales o cibernéticos con los físicos y que cada vez están más presentes en todo tipo de entornos corporativos e industriales. "En los CPS, el proceso físico y el procesamiento de la información están tan estrechamente conectados que es difícil distinguir la contribución individual de cada proceso de la salida" y, cada vez, surgen más tecnologías nuevas como la Inteligencia Artificial (IA), el Internet de las Cosas (IoT), Machine Learning (ML) o Deep Learning (DL) que mejoran sus capacidades, pero, también, lo hacen más vulnerables", destacan sus autores.

Precisamente, para conocer en profundidad este tipo de sistemas el sexteto de autores de este innovador y bien actualizado volumen cubren los diferentes aspectos asociados con los CPS dando información abundante, desde del tipo de algoritmos que se usa como la aplicación de la tecnología en esta clase de sistemas.

Quizá, no es la primera obra dedicada a ellos, pero sí la más actual, con abundante bibliografía y la experiencia de un amplio elenco de profesionales muy experimentados en la materia.

## CYBERCRIME AND DIGITAL FORENSICS: AN INTRODUCTION

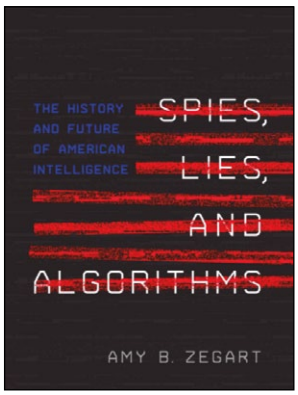



**Autores: Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar**
**Editorial: Routledge**
**Año: 2022 – 794 páginas**
**ISBN: 978-0367360078**
**www.penguinlibros.com**

La tercera edición de 'Cybercrime and Digital Forensics' ofrece una información actualizada y de gran utilidad para los profesionales que trabajan en la lucha o la investigación del cibercrimen. El libro es un recurso fundamental tanto para los especialistas en la materia como para los que quieren acercase a ella, destacando dos nuevos capítulos: uno dedicado a la guerra cibernética y las operaciones de información en línea; y, el otro, a las operaciones en mercados ilícitos para todo tipo de productos, tanto en Open Web como en Dark Web. Además, incluye abundantes estudios de casos que permitirán tener un conocimiento exhaustivo de las últimas tendencias en pericia forense y cibercriminalidad.

Por supuesto, repasa los diferentes ciberdelitos contemplados en legislaciones internacionales y nacionales, cómo los encaran los cuerpos de seguridad de forma transnacional y qué aporta la investigación forense digital. En definitiva, a través de la gran experiencia de sus autores, reconocidos criminalistas, y con abundantes ejemplos, algunos de especial actualidad, se ofrece una perspectiva global sobre el delito cibernético difícil de encontrar en el ámbito académico.

## SPIES, LIES, AND ALGORITHMS: THE HISTORY AND FUTURE OF AMERICAN INTELLIGENCE




**Autora: Amy B. Zegart**
**Editorial: Princeton University Press**
**Año: 2022 – 424 páginas**
**ISBN: 978-0691147130**
**press.princeton.edu**

En **'Espías, mentiras y algoritmos'**, esta reconocida especialista en inteligencia, muestra con precisión –separando la realidad de la ficción–, el pasado, presente y futuro de la comunidad de inteligencia estadounidense, ahora impulsada por la revolución cibernética. Ello supone que "necesitamos reimaginar lo que la Inteligencia puede y debe hacer en la era digital, y eso comienza por darnos cuenta de que los secretos ya no juegan el papel que solían jugar", destacó la autora.

El libro, basado en sus tres décadas de investigación y decenas de entrevistas, ofrece una apasionante historia del espionaje estadounidense desde la Guerra de la Independencia, en tiempos de George Washington, hasta nuestros días, a través de las capacidades que da el ciberespacio, "analizando cómo los 'espías ficticios' influyen en los funcionarios reales".

También, incluye una excelente relación de los conceptos básicos de inteligencia y cómo es la vida de verdad dentro de las agencias de EE.UU., prestando atención a temas controvertidos, como las acciones encubiertas, quién 'vigila al vigilante' o los posibles traidores. Pero, quizá, el aspecto más interesante es su capacidad para mostrar cómo la tecnología está empoderando a nuevos enemigos.