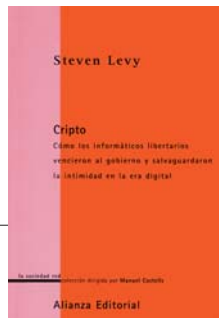


## CRIPTO Cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad en la era digital

**Autor:** Steven Levy  
**Editorial:** Alianza Editorial  
**Año 2002 – 366 páginas**  
**ISBN:** 84-206-9108-9  
[www.alianzaeditorial.es](http://www.alianzaeditorial.es)



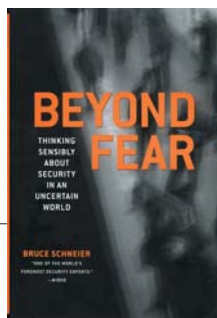
Los tomos depositados en las estanterías de cualquier librería suelen estar divididos por materias y clasificados por géneros. Las obras que pertenecen a la disciplina de la seguridad TIC no son distintas, y entre ellas se pueden encontrar manuales de corte técnico y ensayos de divulgación científica. Al segundo de estos géneros pertenece el volumen escrito por **Steven Levy**, que pretende comunicar, con desigual fortuna, los resultados de una investigación de seis años que le llevó a entrevistar a personajes tan señeros como Witfield Diffie, Martín Hellman y el famoso trío de investigadores Rivest, Shamir y Adleman, entre otros.

Con un estilo cercano y sólidamente narrado, el consagrado periodista amplía los conocimientos de los usuarios en las áreas de las historias de vida y los rumores pseudo-históricos relacionados con la criptográfica moderna, recogiendo en sus páginas conspiraciones políticas sobre los oscuros orígenes del DES, misteriosas operaciones encubiertas de ectoplásmicas agencias gubernamentales y anécdotas como la afición de Diffie por los mapas militares, el camuflaje y la guerra bacteriológica, que le llevó a considerar seriamente la posibilidad de emprender la carrera militar.

En conclusión, este libro es parecido en grado sumo al volumen "Los Códigos Secretos", publicado por Simon Singh hace cuatro años, quizás con un tono más ameno y didáctico y con la diferencia de resaltar, casualmente, las etapas más enigmáticas y peor documentadas.

## BEYOND FEAR Thinking sensibly about security in a uncertain world

**Autor:** Bruce Schneier  
**Editorial:** Copernicus Books  
**Año 2003 – 295 páginas**  
**ISBN:** 0-387-02620-7  
[www.copernicusbooks.com](http://www.copernicusbooks.com)

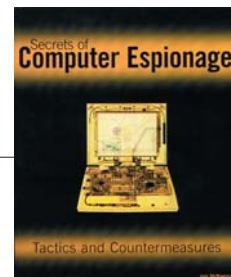


Al cabo del día son muchas las decisiones que tomamos sin percatarnos de ello. La vida está llena de riesgos y como en todo proceso natural debemos determinar, por ejemplo, el momento en el que cruzamos una calle, el lado de la acera por la que andamos, la zona donde aparcamos el coche, etc. Parecen cosas triviales, pero aplicadas al presupuesto de un departamento corporativo de seguridad de la información no lo son tanto. De todo esto trata el libro escrito por el eminente criptógrafo **Bruce Schneier**, que recoge en esta ocasión anécdotas sacadas de la Historia, los deportes y las películas y las aplica a entornos tecnológicos con el objetivo de ayudar a los profesionales que tienen que gestionar riesgos.

El volumen lo conforman diecisiete capítulos, divididos en tres partes, con la siguiente distribución: **Parte I: Seguridad sensible** [Temas: 1) La seguridad complica el intercambio, 2) Los intercambios seguros son subjetivos, 3) Los intercambios seguros dependen de la energía y de la agenda]; **Parte II: Cómo funciona la seguridad** [Temas: 4) Cómo fallan los sistemas, 5) Conociendo a los atacantes, 6) Los atacantes nunca cambian de tono, sí de instrumento, 7) La tecnología crea desequilibrios en la seguridad, 8) La seguridad consiste en conocer los puntos críticos, 9) La fragmentación produce inseguridad, 10) La seguridad gira alrededor de la gente, 11) Trabajar la detección cuando la prevención falla, 12) La detección es inútil sin respuesta, 13) Identificación, autenticación y autorización, 14) Todas las contramedidas tienen valor, pero no todas las contramedidas son perfectas, 15) Luchando contra el terrorismo]; **Parte III: El juego de la seguridad** [Temas: 16) Negociando la seguridad, 17) Desmitificando la seguridad].

## SECRETS OF COMPUTER ESPIONAGE Tactics and Countermeasures

**Autor:** Joel McNamara  
**Editorial:** John Wiley & Sons  
**Año 2003 – 362 páginas**  
**ISBN:** 0-7645-3710-5  
[www.wiley.com](http://www.wiley.com)

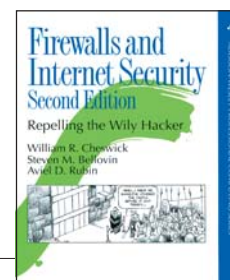


El título del volumen redactado por **Joel McNamara** recoge con precisión el tema de su obra, que no es otro que el espionaje informático. Este aspecto de la seguridad TIC, aunque de por sí bastante baqueteado, no siempre ha sido analizado en profundidad. Precisamente por ello, su tratamiento editorial tiene que ser riguroso debido, entre otras cosas, a la alta "inflamabilidad" de la materia en cuestión.

Según el Diccionario de la RAE "espíar" significa "observar con disimulo lo que pasa". Aplicado al espacio intangible configurado por las redes de comunicaciones lo que quedaría sería "observar con disimulo la información que circula". El autor coincide con esta definición y así lo plasma en sus primeras páginas al transcribir una cita de Ronald Reagan, en la que asegura que "la información es el oxígeno de la sociedad actual". Es así, pero conviene matizar. No se trata de la relevancia de los datos, que también tiene su aquél, sino del control y la disponibilidad de los mismos. Por desgracia, el autor hace una trabajosa mezcla de estos conceptos y en un intento fallido de confeccionar un repositorio técnico de información sobre los bajos fondos informáticos –analizando tácticas, herramientas y contramedidas– se retrotrae a un cruce de sendas ya andadas, en las cuales se imponen las historias de *jaquers* trasnochados en *thrillers* de los años sesenta, por supuesto, beodos de información secreta.

## FIREWALLS AND INTERNET SECURITY Repelling the Wily Hacker - Second Edition

**Autores:** William R. Checkwick,  
Steven M. Bellovin, Aviel D. Rubin  
**Editorial:** Addison- Wesley  
**Año 2003 – 433 páginas**  
**ISBN:** 0-201-63466-X  
[www.awprofessional.com/](http://www.awprofessional.com/)  
[www.pearsoned.es](http://www.pearsoned.es)



El presente volumen, escrito al alimón por **Checkwick, Bellovin** y **Rubin**, continua en la línea de otras obras ya glosadas en esta sección, enfocadas a compilar datos y procedimientos, en su mayoría de carácter técnico, en esta ocasión centrado genéricamente en los dispositivos diseñados para la protección perimetral, y más concretamente en los sistemas cortafuegos. Con un estilo claro y conciso, los autores han actualizado la primera edición –aparecida en 1994– con numerosas anécdotas, historias y comentarios de profesionales que han tenido que tomar decisiones en situaciones delicadas, rebajando a su vez, la aridez tecnológica con numerosos ejemplos prácticos y gráficos.

El libro está dividido en seis partes y diecinueve capítulos estructurados del siguiente modo: **Parte I: Para comenzar** [Temas: 1) Introducción, 2) Revisión de los protocolos de seguridad: niveles bajos, 3) Protocolos de nivel alto, 4) La web: ¿amenaza?]; **Parte II: Las amenazas** [Temas: 5) Tipologías de ataques, 6) Técnicas y herramientas *hacker*]; **Parte III: Protección y servicios** [Temas: 7) Autenticación, 8) Utilizando algunas herramientas y servicios]; **Parte IV: Cortafuegos y VPNs** [Temas: 9) Clases de cortafuegos, 10) Servicios de filtrado, 11) Ingeniería de cortafuegos, 12) Túneles cifrados y redes privadas virtuales]; **Parte V: Protegiendo una organización** [Temas: 13) Capas de red, 14) Protegiendo un *host* en un entorno hostil, 15) Detección de intrusos]; **Parte VI: Lecciones aprendidas** [Temas: 16) Una tarde con Berferd, 17) La decisión de Clark, 18) Comunicaciones seguras frente a redes inseguras, 19) Conclusiones].