

INDICE

Introducción	XV
Parte 1:	
Aspectos generales de la seguridad informática	
Capítulo 1	3
Acerca de virus, gusanos y demás familia	
Historia de una guerra anunciada	
Pequeñas presentaciones para una gran familia	5
¡Tiempo muerto! ¿Hablamos de viejas glorias?	11
Presentando al tronco principal	
Pero, ¿Qué es un virus?	13
Sobre Hackers, Phreakers, Sneakers, Wrakers y Riders	18
Capítulo 2	
Disección de un ordenador	21
El ordenador	
Interiores de un PC	23
La información	
¿Qué hacemos con nuestro programa?	27
¿Qué es un sistema operativo?	29
Las rutinas de la BIOS y del DOS	
¿Nos dejamos el Boot?	30
Capítulo 3	
Todo lo que usted quiso saber sobre la estructura lógica de sus ficheros	33
Y no se atrevió a preguntar	
Un 0 y un 1 hacen binario y con binarios tenemos hexadecimales	34
Bits y Bytes no solo son palabras (sino que hacen palabras)	36
Su majestad del chip	37
Volvemos a la CPU	39
Encienda al el ordenador y vea que sucede	40
¿Tienen un disquete a mano?	41
Capítulo 4	
El ordenador bajo ataque: como funciona un virus	45
¿Esta seguro de que no tiene V.I.R.U.S.? lea a Homero	46
Como actúa un virus	47
El virus siempre llama dos veces	48
Métodos de contaminación y ocultamiento	
Contaminación del Boot	50
Contaminación de un fichero. COM	
Contaminación de un fichero. EXE	51
Ocultamiento	52
Fase de control	55
El temido momento de la producción	56
Y ahora ¿Qué?	
Vectores de interrupción	58
Capítulo 5	
Miscelánea vírica	63
Consejos para aprender a meter la pata	

¿Sabe cuando debe tener miedo?	64
Pero ¿Existen los virus?	66
Análisis de una catástrofe	67
Consejos que tal vez funciones	68
Pregunte, pregunte	
¿Quién hace los virus?	69
¿Se propagan los virus por ficheros de datos?	
¿Puede contagiarse un disco si lleva la etiqueta de protección?	70
¿Se contagian los ordenadores “porque sí”?	
¿Sufre un virus mutaciones?	
¿Puede infectarse un antivirus?	
¿Qué son los errores “falso positivo (Tipo I)” y “falso negativo (Tipo II)”	71
¿Qué hacer si creo haber detectado un virus nuevo?	
¿Es posible proteger un sistema solo con software?	
¿Qué puede hacerse con una protección de hardware?	72
¿Para proteger un fichero basta con el atributo de “Solo lectura”?	
¿Puede una clave de acceso proteger ficheros	
¿Puede proteger un disquete la pegatina de protección contra escritura?	
¿Puede un virus del Boot infectar un disco que no sea de arranque?	
¿Pueden un virus ocultarse en la CMOS?	73
¿Es mala la desinfección de los virus?	
¿Cuánto tipos de virus hay?	
¿Puede un virus dañar el Hardware de un ordenador?	
El virus “Tostadora”. ¿Existe?	74
Capítulo 6	
Programas antivirus	75
Sistemas de prevención	76
Sistemas de detección	77
Vacunando al ordenador	
Comparando ficheros	78
Los virus duelen	79
Hágalo usted mismo	80
Como saber si su sistema ha sido infectado	81
Que hacer ante una infección	
Como revisar software antivirus	82
Capítulo 7	
El (CASI) largo brazo de la ley	87
La seguridad informática para legisladores	
Casos y cosas	89
Hablando de accesos	
¿Cuánta seguridad?	90
Política de protocolos	91
Ética y leyes	92
Capítulo 8	
¿Hablando de futuro?	95
V.I.R.U.S. en las redes	
V.I.R.U.S. militares	96
¿Sueña los ordenadores con ovejas eléctricas?	97
Parte 2:	101

Guía de virus informáticos	
Capítulo 9	
Virus de UNIX	
Capítulo 10	
Virus de amiga	105
Capítulo 11	
Virus de Atari	133
Capítulo 12	
Virus de Macintosh	149
Resumen	165
Capítulo 13	
Virus del MS-DOS	167
Capítulo 14	
Virus del MVS	307
Capítulo 15	
Como nombrar virus	309
Nombre de familia	310
Nombre de grupo	
Nombre de la variante mayor	311
Nombre de la variante menor	
Virus del Boot	312
Infectadores de ficheros	314
Otros tipos de programas malignos	
Droppers	327
Gérmenes	
Apéndices	
A-Lista de interrupción del MS-DOS	331
Interrupciones de la BIOS	
Interrupciones del DOS	
Llamadas de la INT 21h del DOS	332
B- Los doce del patíbulo	335
Troyanos	336
C- Calendario de activación	341
D- Como usar el disquete del libro	349
E- Addenda del autor	351
Índice alfabético	355