

CONTENIDO

	AGRADECIMIENTOS	xix
	PROLOGO	xxi
	INTRODUCCION	xxiii
	POR QUE ESTE LIBRO ES PARA USTED	1
PARTE UNO	¿QUE SON LOS VIRUS INFORMATICOS Y DE DONDE PROCEDEN?	3
UNO	SEPARANDO LA REALIDAD DE LA FICCIÓN	5
	¿QUE ES UN VIRUS INFORMATICO?	6
	TIPOS DE SOFTWARE ROGUE	9
	Bug-Ware	11
	El caballo de Troya	12
	Camaleones	12
	Bombas de software	13
	Bombas lógicas	13
	Bombas de tiempo (<i>de relojería</i>)	13
	Reproductores	14
	Gusanos	14
	Virus	14
	¿QUE GRAVEDAD SUPONE LA AMENAZA VIRICA?	15
	PROTECCION DE SUS COMPUTADORAS	16
DOS	LA INFECCION DE LOS PCs IBM Y COMPATIBLES	17
	CONTAGIO DEL GERMEN	18
	Reproducción dentro de una única computadora	18
	Reproducción entre múltiples computadoras	20

	Consecución del objetivo: total saturación del sistema	20
	PUENTE DE LAS MEDIDAS ANTIVIRUS	20
TRES	TIPOS DE VIRUS INFORMATICOS	23
	CONTAMINADORES DE SECTOR DE ARRANQUE (BSIs)	23
	CONTAMINADORES DE PROCESADOR DE ORDENES (CPIs)	25
	CONTAMINADORES DE PROPOSITO GENERAL (GPIs)	27
	CONTAMINADORES MULTIPROPOSITO (MPIs)	27
	CONTAMINADORES DE ARCHIVO ESPECIFICO (FSIs)	28
	CONTAMINADORES RESIDENTES EN MEMORIA (MRIs)	29
	METODOS POPULARES DE INFECCION USADOS POR LOS VIRUS INFORMATICOS	30
	Añadidura	31
	Inserción	32
	Reorientación	33
	Sustitución	34
	El armazón vírico	35
CUATRO	MAS ALLA DEL MS-DOS	37
	OS/2	37
	Entorno del modo protegido	38
	Peligros del sistema de doble arranque	38
	Virus de la orden de arranque	39
	Virus del CONFIG.SYS	40
	Virus de archivos ejecutables	40
	PROGRAMACION ORIENTADA A OBJETO (POO)	41
PARTE DOS	<i>IMPEDIR LA PROPAGACION DE LOS VIRUS INFORMATICOS</i>	43
CINCO	MEDIDAS A TOMAR, MEDIDAS A EVITAR	45
	EVALUACION DEL SOFTWARE ANTIVIRUS	46
	Sistemas de prevención	46
	Sistemas de detección	48
	Detectores antibomba	48

	Detectores antivirus	48
	EL PROBLEMA DEL SOFTWARE ANTIVIRUS	50
	Vacunas	51
	Antídotos	53
	Utilidades de comparación de archivos	55
	Exploradores de virus	56
	Visualizadores de mapas de disco	57
	Programas antivirus residentes en memoria	58
SEIS	REALIZACION DE UNA EFICAZ POLITIVA DE ANTIVIRUS	61
	AISLAMIENTO DE LAS COMPUTADORAS: POR QUE FRACASA	62
	GESTION DEL SOFTWARE DE DOMINIO PUBLICO Y DEL <i>SHAREWARE</i>	63
	GESTION DE SOFTWARE DE CASA	64
	GESTION DE LA PIRATERIA DE SOFTWARE	64
	SU MEJOR DEFENSA: USUARIOS INSTRUIDOS	65
	LINEAS DE GUIA PARA USAR EL SOFTWARE DE DETECCION VIRICA	66
	UNA COLECCION DE TECNICAS ANTIVIRUS	68
	Arranque desde un disco flexible	69
	Eemple software de detección de virus	70
	Use comprobaciones de archivos antes de su ejecución	71
	Cambie los atributos de los archivos	72
	Use señuelos de procesador de órdenes	73
	Use señuelos de archivos de aplicaciones	74
	Reinicialice el sistema	75
	Reinstale los archivos de aplicaciones	76
	Reformatee los discos duros	76
	Utilice con precaución los gestores de disco de bajo nivel	77
	Observe la carga del programa y los tiempos de acceso al disco	78
	Registre el espacio disponible del disco	78
	Registre los sectores malos	78
	Utilice el <i>shareware</i> con cuidado	80
	No use software pirateado	83
	Cuidado con los regalos de los vendedores	83
	¡Haga copias de seguridad!	84
	MANTENER FUERTE EL BALUARTE	84

SIETE	DIAGNOSIS Y CURAS	85
	DIAGNOSTICO DE COMPUTADORAS IN- FECTADAS	86
	Indicios de aviso de los virus informáticos . . .	86
	QUE HACER CUANDO SUS SISTEMAS SON INFECTADOS	87
	El método quirúrgico	88
OCHO	GESTION GENERAL DEL DISCO DURO .	91
	OBTENCION DE UNA IDEA GENERAL . .	92
	IDEA GENERAL DE LOS SHELL DEL DOS	92
	EL ARCHIVO CONFIG.SYS	93
	EL ARCHIVO AUTOEXEC.BAT	94
	ELIMINACION DE ARCHIVOS DUPLICA- DOS	94
	USO EFICAZ DE LOS CAMINOS (PATH) DE DOS	95
	OPERACIONES DE VERIFICACION	97
	CUIDADO DEL DISCO DURO	97
NUEVE	A VISTA DE PAJARO	99
	¿POR QUE LOS PROGRAMADORES RO- GUE HACEN LO QUE HACEN?	99
	REALIDAD Y EXTENSION DEL PELIGRO VIRICO	100
	EN RESUMEN	101
<i>PARTE TRES</i>	<i>GUIAS DEL USUARIO</i>	<i>103</i>
DIEZ	FATSO: OPCION DE SEGURIDAD PARA LA TABLA DE ASIGNACION DE ARCHI- VOS	105
ONCE	PROTECT, WPD, WPDD: CINTA SOFTWA- RE DE PROTECCION CONTRA ESCRI- TURA	121
DOCE	LOCKUP: BLOQUEO Y CLAVE AUTOMA- TIZADOS DEL DISCO DURO	143
TRECE	PARK: APARCADOR DE LAS CABEZAS DEL DISCO DURO	163
CATORCE	FLU_SHOT+: PROTECCION RESIDENTE EN MEMORIA CONTRA VIRUS	171
	IDEA GENERAL	171
	INSTALACION DE FLU_SHOT+	172
	EL ARCHIVO FLUSHOT.DAT	173
	Protección de los archivos contra el acceso de escritura	174
	Protección de los archivos contra el acceso de lectura	175

Exclusión de archivos	175
Archivos de total (Checksumming) control . . .	175
Registro de un programa TSR	177
Acceso restringido	177
Protección del archivo FLUSHOT.DAT	177
Recomendaciones para la protección	178
Permitir que se ejecuten programas peligrosos .	178
PROTECCION DE LA PISTA DE ARRANQUE	179
EJECUCION DEL FLU_SHOT+	179
Verificación de la suma de control de la tabla en memoria	180
Interceptación de escrituras directas en disco por medio de INT13 e INT40	180
¿Qué ocurre con INT26?	180
Poner fuera de servicio el mensaje de cabecera .	180
Anulación del disparo en la apertura con acceso de escritura	180
Autorización para que trabajen los TSRs	181
Desactivación de FLU_SHOT+	181
Inhabilitación de la desactivación de FLU_SHOT+	181
Desactivación de la presentación basculante de FLU_SHOT+	182
Definición de sus propias claves especiales . . .	182
Forzar a FLU_SHOT+ a que use solamente el BIOS	182
Adormecer FLU_SHOT+ cuando se ejecute primero	183
Interpretación de un disparo de FLU_SHOT+ QUE BUENO ES FLU_SHOT+, ¿DE VERDAD?	183

QUINCE	VIRUSCAN: EXPLORADOR DE VIRUS DE LINEA DE ORDEN	189
	PROGRAMA EJECUTABLE (SCAN.EXE)	189
	Notas sobre la versión 57	190
	PERSPECTIVA	190
	EJECUTANDO VIRUSCAN	191
	Códigos de salida	193
	SUPRESION DEL VIRUS	193
	Contaminaciones de sector de arranque	193
	Contaminaciones de archivo ejecutable	193
	Contaminadores de tabla de partición	193
	NOTAS SOBRE LAS VERSIONES	194

DIECISEIS	CLEAN-UP: UTILIDAD PARA LA ERRADICACION DE VIRUS	199
	PROGRAMA EJECUTABLE (CLEAN.EXE)	199
	PERSPECTIVA	200
	EJECUCION DE CLEAN-UP	200
DIECISIETE	EL SISTEMA DE DETECCION VIRICA	
	CHECKUP DE RICH LEVIN	205
	FUNCIONAMIENTO DE CHECKUP	205
	EJECUCION DE CHECKUP	206
	Opciones de línea de orden de CHECKUP	208
	Archivos .XUP de CHECKUP	212
	Extensiones alternativas del archivo de salida de CHECKUP	213
	NIVELES DE ERROR DE CHECKUP	214
	El archivo CHECKUP.LOG	215
	Creación de discos flexibles CHECKUP limpios	216
	Archivo XUP.BAT/AUTOEXEC.BAT de CHECKUP	218
	Mensajes en tiempo de ejecución	220
	Códigos de error y mensajes de error	222
	CONFLICTOS CON OTROS PROGRAMAS	
	ANTIVIRUS	226
<i>PARTE CUATRO</i>	<i>APENDICES</i>	229
APENDICE A	EL SOFTWARE <i>ROGUE</i> Y LA LEY	231
	ALGUNOS CASOS HIPOTETICOS	232
	PERSPECTIVA DE LAS LEYES PENAL Y CIVIL	233
	Agravios	234
	Intrusión en bienes muebles y apropiación ilícita	234
	Fraude, engaño y tergiversación	235
	Invasión de la intimidad	236
	Negligencia	237
	Responsabilidad de productos: teorías de agravio y garantía	239
	LEY PENAL	241
	Delitos de la ley común	242
	Delitos estatutarios contra el estado	243
	Delitos estatutarios federales	247
	Propuestas legislativas	248
APENDICE B	<i>COMPUSERVE MAGAZINE</i> : LINEA DE TIEMPO DE LA HISTORIA DEL VIRUS	251
	UN «VIRUS» CONTAMINA LAS COMPUTADORAS COMMODORE	252

EL VIRUS SE TRASLADA A LAS COMPUTADORAS	252
EL MENSAJE DE SALUDOS NAVIDEÑOS BLOQUEA EL SISTEMA DE CORREO ELECTRONICO DE IBM	253
UN VIRUS INFORMATICO AMENAZA EL SISTEMA GENERAL DE LA UNIVERSIDAD HEBREA	254
LOS INFORMATICOS DE TAMPA LUCHAN CONTRA EL VIRUS	255
LOS PROGRAMAS VIRICOS PODRIAN TENER APLICACIONES UTILES, DICE UN COLUMNISTA	255
UN ABONADO Y UN SYSOP BLOQUEAN UN POSIBLE «VIRUS» EN EL APPLE HYPERCARD FORUM	256
DOD INTENTA PROTEGER SUS COMPUTADORAS DE UN VIRUS ELECTRONICO	258
UN EXPERTO DE DOS ESCENARIOS PARA EL PROBLEMA DEL «VIRUS» INFORMATICO	259
EL VIRUS INFORMATICO ES CONSIDERADO UN FRAUDE	259
EL VIRUS DEL HYPERCARD ES CONSIDERADO «INOFENSIVO»	260
UN EDITOR DEFIENDE SU PROGRAMA «VIRICO» COMO «BUENO» PARA LA COMUNIDAD	261
DOS EMPRESAS OFRECEN «INOCULARNOS» CONTRA LOS «VIRUS» INFORMATICOS	262
UN «VIRUS» SE PROPAGA A UN PROGRAMA COMERCIAL; SE ESTUDIA UNA DEMANDA LEGAL	263
LA AMENAZA DEL «VIRUS» SACADA FUERA DE PROPORCION, DICEN NORTON Y SYSOPS	265
SALE UNA HOJA INFORMATIVA SOBRE EL VIRUS INFORMATICO	266
SIR-TECH DESVELA UN ANTIVIRUS	266
UN NUEVO VIRUS INFECTA LOS MACINTOSH EN LA NASA Y APPLE	267
EL «VIRUS» VIERNES 13 FRACASA	267
EL PERIODICO R. I. DESALOJA UN VIRUS	268

LOS MACINTOSH DE EPA SE RECUPERAN DE VIRUS	269
EL CONGRESO ESTUDIA LOS PROBLEMAS VIRICOS	270
UN TEJANO, SOMETIDO A JUICIO POR SUPUESTA CONTAMINACION DE UN SISTEMA CON UN «VIRUS»	270
EL FBI ES LLAMADO A INVESTIGAR EL CASO DE UN VIRUS	271
EL BBS DE NUEVO MEJICO PRESENTA DEMANDA SOBRE UN VIRUS	272
LOS LUCHADORES CONTRA UN VIRUS LUCHAN ENTRE SI	273
EL JUICIO POR EL VIRUS EMPIEZA EN FORT WORTH	274
UN VIRUS ATACA UNA RED JAPONESA	274
UN TRIBUNAL CONDENA A UN PROGRAMADOR POR SEMBRAR UN VIRUS	274
PROFESORES UNIVERSITARIOS ATACAN A VIRUS INFORMATICOS	276
UN SEGUNDO VIRUS ES ENCONTRADO EN ALDUS CORP.	276
UN HOMBRE ES CONDENADO EN EL PRIMER CASO JUDICIAL CRIMINAL DE LA NACION RELACIONADO CON VIRUS	277
EL VIRUS DEL CEREBRO ATACA HONG KONG	278
SESENTA EMPRESAS INFORMATICAS ESTABLECEN LOS OBJETIVOS DEL VIRUS	278
MILES DE COMPUTADORAS DE LA UNIVERSIDAD Y DE INVESTIGACION ATACADAS EN UN ASALTO DE PRIMERA MAGNITUD	279
UNOS INFORMES DESIGNAN A UN ESTUDIANTE DE CORNELL, DE 23 AÑOS, COMO EL AUTOR DEL VIRUS	281
LOS AMIGOS DE ROBERT MORRIS DICEN QUE NO HUBO MALICIA ALGUNA CON EL SUPUESTO VIRUS	283
UN GRUPO NUEVO DEL LABORATORIO LAN OFRECE SUGERENCIAS PARA LA PREVENCIÓN DEL VIRUS	285
EL FBI ELEVA LA INVESTIGACION SOBRE EL VIRUS A UNA «INVESTIGACION CRIMINAL COMPLETA»	286

EL GOBIERNO PUEDE MANDAR COMPARECER A CORNELL	287
EL «VIRUS DEL CEREBRO» APARECE EN HOUSTON	287
UN EXPERTO EN UNIX CONSIDERA EL «PANICO» DEL VIRUS INNECESARIO Y CULPA A LA MALA PLANIFICACION	288
EL FBI ESTUDIA UNA AMPLIA GAMA DE POSIBLES VIOLACIONES EN EL CASO DEL VIRUS	289
MICHIGAN HACE BALANCE DE LA LEY ANTIVIRICA	290
UN VIRUS ATACA LOS MACINTOSH DE CALIFORNIA	290
UN EXPERTO EN SEGURIDAD INFORMATICA OFRECE CONSEJOS	291
LA AMENAZA DEL VIRUS ES CONSIDERADA EXAGERADA	291
EL FBI CONSIGUE LOS REGISTROS DE MORRIS EN LA INVESTIGACION DEL CASO NACIONAL DEL VIRUS	292
SPA FORMA UN GRUPO PARA ACALLAR LOS RUMORES SOBRE VIRUS INFORMATICOS	293
UN VIRUS ATACA LA UNIVERSIDAD DE OKLAHOMA	293
EL VIRUS «VIERNES 13» ATACA	294
EL VIRUS «VIERNES 13» PUEDE SER UNA NUEVA VERSION DE UN VIRUS DE ISRAEL	294
LA BIBLIOTECA DEL CONGRESO ES VICTIMA DEL VIRUS	295
¿PROCEDE DE FRANCIA EL VIRUS NAVI-DEÑO?	295
EXISTE DIVISION DE COMO PROCESAR AL HOMBRE ACUSADO DEL VIRUS DEL ARPANET	296
UN GRUPO FEDERAL LUCHA CONTRA LOS VIRUS	297
LOS VIRUS INFORMATICOS, UN TEMA CANDENTE EN EL CONGRESO	297
EL CONGRESO CONSIDERA OTRO PROYECTO DE LEY DE PROTECCION INFORMATICA	298
EL CREADOR DE UN VIRUS ENCONTRADO MUERTO A LOS 39 AÑOS	298

UN HOSPITAL ES ATACADO POR UN VIRUS INFORMATICO	299
MAS HOSPITALES, ATACADOS POR EL VIRUS	299
EL GOBIERNO HACE PLANES PARA CENTROS ANTIVIRICOS	301
EL «GUSANO» DE MORRIS NO ERA OBRA NI DE UN GENIO NI DE UN DELINCUENTE, DICE LA COMISION	301
SE NECESITAN ESTUDIOS DE ETICA EN INFORMATICA	302
ILLINOIS ESTUDIA LA LEY VIRICA	303
LOS ERRORES, NO LOS INTRUSOS, PRINCIPAL AMENAZA	303
EXPERTOS TESTIFICAN SOBRE EL DELITO INFORMATICO	304
MASSACHUSSETTS ESTUDIA UNA NUEVA LEY DE INTRUSION	305
EL MERCADO DE LA VACUNA INFORMATICA PROSPERA CON EL MIEDO DEL USUARIO	306
MORRIS ES SUSPENDIDO EN CORNELL	306
CRITICADAS LAS LEYES INFORMATICAS PENDIENTES	307
UN NUEVO VIRUS ATACA LAS COMPUTADORAS TAILANDESAS	307
EL CONGRESO ESTUDIA LOS VIRUS INFORMATICOS	308
GLOSARIO DE TERMINOS RELACIONADOS CON EL VIRUS	309
MORRIS, ACUSADO EN EL INCIDENTE DEL GUSANO	310
UN INVESTIGADOR PONE AL DESCUBIERTO EL VIRUS 12 DE OCTUBRE	311
MORRIS SE DECLARA INOCENTE	312
NIST FORMA UNA RED DE SEGURIDAD INFORMATICA	312
UN AUSTRALIANO ES ACUSADO DE INTRUSION	313
¿ESTA DE VUELTA EL VIRUS DE INTERNET?	314
LA FUERZA AEREA AVISA A SUS BASES DE UN POSIBLE «VIRUS DEL DIA DE COLON»	314
LOS VIRUS INFORMATICOS INFECTAN EL CONGRESO	315

	UN VIRUS ATACA AUSTRALIA	316
	LA AMENAZA VIRICA, ABSURDAMENTE EXAGERADA, DICEN LOS EXPERTOS .	317
	UN SOFTWARE ENFERMO CONTAMINA 100 HOSPITALES EN TODA LA NACION	318
	EL EJERCITO VA A COMENZAR LA IN- VESTIGACION DEL VIRUS	318
	SE INFORMA DEL LLAMADO VIRUS «DA- TACRIME» EN LA RED DANESA POST- GIRO	319
	IBM ESTA EDITANDO SOFTWARE ANTI- VIRICO	319
	LOS INFORMATICOS HOLANDESES TE- MEN AL VIRUS «DATACRIME»	320
APENDICE C	VIRUS CONOCIDOS DEL PC IBM	321
	INTRODUCCION Y FORMATO DE EN- TRADA	322
	LISTADO RESUMEN	324
	REFERENCIAS CRUZADAS	364
APENDICE D	VIRUS DE LOS MACINTOSH	369
	VIRUS CONOCIDOS DE LOS MACINTOSH QUE HACER SI CREE QUE TIENE UN VI- RUS	369 373
	COMO PROTEGER SU MACINTOSH	373
APENDICE E	LISTADO DE VENEDORES	375
APENDICE F	UNA GUIA DE TERMINOS POPULARES RELACIONADOS CON VIRUS	379
	INDICE	383