



UNIVERSIDAD NACIONAL DEL ENTRE RÍOS
FACULTAD DE INGENIERÍA
CENTRO DE MEDICINA
BIBLIOTECA

4410 = =

Índice

ACERCA DEL AUTOR

PRÓLOGO11

INTRODUCCIÓN13

CAPÍTULO 1

EL PROBLEMA DE LOS VIRUS INFORMÁTICOS17

1.1 Los virus informáticos y su contribución a la muerte de personas17

1.2 Del vandalismo al sabotaje18

1.3 Desarrollo de los virus18

1.4 Pérdidas económicas19

1.5 Generación de pérdidas21

1.2 Daños que producen a los sistemas22

1.3 La solución del problema23

1.4 Conclusiones24

CAPÍTULO 2

FUNCIONAMIENTO DE LOS VIRUS INFORMÁTICOS29

2.1 Daños que produce un virus informático30

2.2 El peligro de los virus informáticos30

2.3 La solución31

2.4 Evolución del problema32

2.5 Funcionamiento33

2.6 Daño34

2.7 Ejecución de un virus34

2.7.1 Ejecución de un virus en un archivo ejecutable infectado35

2.7.2 Ejecución de un virus en el sector de arranque36

2.7.3 Dispersión de un virus de sector de arranque37

2.8 Clasificación de los virus informáticos39

2.9 Definición técnica de un virus informático39

2.10 Potencial de daño de un virus informático39

2.11 Modelo de virus informático40

2.11.1 Módulo de reproducción40

2.11.2 Módulo de ataque40

2.11.3 Módulo de defensa41

2.12 Infección de un sistema de computadoras42

2.13 Conclusiones43

CAPÍTULO 3

MACROVIRUS47

3.1 El problema47

Virus informáticos

Introducción

3.2 Definición de macrovirus.....	49
3.3 Funcionamiento de un macrovirus.....	50
3.3.1 Funcionamiento de un macrovirus de Word.....	51
3.3.2 Word Basic, el lenguaje de los macrovirus.....	53
3.4 Dispersión de un macrovirus.....	54
3.5 Análisis de macrovirus.....	54
3.5.1 Macrovirus para MS Word.....	54
3.5.2 Macrovirus de MS Excel.....	61
3.5.3 Macrovirus para aplicaciones no-Microsoft.....	63
3.6 Características de los macrovirus conocidos.....	64
3.7 Técnicas avanzadas de macrovirus.....	64
3.7.1 Polimorfismo.....	65
3.7.2 Stealth (ocultamiento).....	65
3.7.3 Encriptación.....	65
3.8 Medidas de prevención para macrovirus.....	65
3.9 Las soluciones de Microsoft.....	66
3.9.1 MS Word 6.x y 95.....	66
3.9.2 Para MS Word 95a (versión 7.0a) y MS Word 97.....	67
3.9.3 Microsoft Excel Virus Search Add-ins.....	68
3.10 Macrovirus detectados hasta septiembre de 1997.....	68

CAPÍTULO 4

LOS VIRUS EN INTERNET.....	83
4.1 Infección de una computadora a través de Internet.....	85
4.2 Normas y procedimientos para prevenir una infección vía Internet.....	86
4.3 Otros programas dañinos en Internet.....	88
4.3.1 Caballos de Troya.....	88
4.3.2 Virus Hoax.....	88

CAPÍTULO 5

LOS ANTIVIRUS.....	99
5.1 Función de un antivirus.....	99
5.2 Identificación.....	100
5.3 Detección.....	101
5.4 Modelo de un sistema antivirus.....	102
5.4.1 Módulo de control.....	103
5.4.2 Módulo de respuesta.....	104
5.4.3 Características de un buen antivirus.....	104
5.5 Normas para la utilización de programas antivirus.....	105
5.5.1 Revisión de un sistema.....	105
5.5.2 Remoción de un virus.....	106
5.6 Elección de un antivirus.....	108
5.7 Programas antivirus disponibles en nuestro país.....	108

CAPÍTULO 6

ESTRATEGIAS ANTIVIRUS.....	125
6.1 Estrategia de seguridad antivirus para un usuario individual.....	127
6.1.1 Normas y procedimientos antivirus para usuarios individuales.....	128
6.1.2 Conclusiones.....	130
6.2 Conceptos de seguridad informática.....	130
6.2.1 Necesidad de seguridad informática.....	131
6.2.2 Integridad de la información.....	132
6.2.3 Operatividad de la información.....	132
6.2.4 Confidencialidad de la información.....	132
6.2.5 Objetivo de la seguridad informática.....	132
6.2.6 Definición de sistema para la seguridad informática.....	133
6.2.7 Componentes de un sistema informático.....	134
6.2.8 Los virus como riesgo de un sistema informático.....	135
6.2.9 La seguridad disminuye la operatividad.....	136
6.2.10 Áreas de la seguridad informática.....	137
6.2.11 Plan de contingencia.....	138
6.2.12 Determinación de responsables y poder político.....	139
6.2.13 Documentación de la estrategia de seguridad.....	139
6.3 Desarrollo de una estrategia de seguridad.....	140
6.3.1 Análisis de riesgos.....	140
6.3.2 Herramientas de una estrategia antivirus.....	141
6.3.3 Normas y procedimientos.....	142
6.3.4 Llevar adelante la estrategia de seguridad.....	142
6.4 Plan de contingencia.....	142
6.4.1 Normas y procedimientos de contingencia para una infección por virus informático.....	143
6.4.2 Llevar adelante el plan de contingencias.....	143
6.4.3 Documentación de plan de contingencia.....	143
6.5 Desarrollo paso a paso de la estrategia de seguridad antivirus para una pequeña o mediana empresa.....	143
6.5.1 Descripción de la empresa.....	143
6.5.2 Determinación de los responsables.....	144
6.5.3 ¿Qué es lo que hay que proteger?.....	144
6.5.4 ¿De qué hay que protegerse? El análisis de los riesgos.....	144
6.5.5 Normas y procedimientos de seguridad recomendados.....	146
6.4.6 Plan de contingencia.....	147

CAPÍTULO 7

CASOS DE VIRUS EN EMPRESAS.....	151
7.1 Virus con complemento humano.....	151
7.2 Virus de daño específico.....	153
7.3 Virus de sabotaje corporativo.....	154
7.4 Virus de infección virtual.....	156
7.5 Falsa alarma de un antivirus.....	157
7.6 Sistema de infección casi imposible.....	159

APÉNDICE A

MITOS SOBRE LOS VIRUS	163
Existen virus informáticos benignos y malignos	163
Los virus informáticos se contagian vía módem	163
Existen virus que se alojan en la CMOS de las computadoras.....	163
Los antivirus son infalibles.....	164
Virus que se activan al leer un mensaje de correo electrónico	164

APÉNDICE B

ASPECTOS JURÍDICOS DE LOS VIRUS INFORMÁTICOS	167
--	-----

APÉNDICE C

TENDENCIAS DE LOS VIRUS INFORMÁTICOS.....	177
---	-----

APÉNDICE D

LOS VIRUS ARGENTINOS	223
----------------------------	-----

APÉNDICE E

BREVE HISTORIA DE LOS VIRUS INFORMÁTICOS.....	237
---	-----

APÉNDICE F

CALENDARIO DE VIRUS	245
---------------------------	-----