

Índice

Prólogo	11
Preliminares.....	13
1. ¿Era mi abuela una experta en seguridad?	13
2. Objetivos	15
3. Herramientas básicas para este libro	17
4. Descargo de responsabilidad	18
Capítulo I	
Seguridad física	19
1. BIOS.....	19
Contraseñas en la BIOS	19
Eludir las contraseñas	20
DEP, XD, ND, Enhanced Virus Protection.....	23
Otras opciones	27
Seguridad en UEFI	28
Capítulo II	
Seguridad del sistema operativo	31
1. Instalación y parcheado.....	31
Parchear “offline”	31
¿Y ahora cómo se parchea?	33
Particionado seguro	34
2. Definir perfiles y usuarios	39
Cómo funcionan los perfiles.....	40
Cambiar la ubicación de un perfil.....	40
El proceso de arranque	42
UAC.....	52

3. Contraseñas	66
LM y NTLM	66
Tipos de ataque	69
Syskey	76
Usuarios en Windows	79
Grupos en Windows	80
NTFS se compone de ACL	82
NTFS	84
Permisos en carpetas especiales	94
Cuidado con los destkop.ini	95
Opciones de seguridad	102
Privilegios	104
4. Configuración y mantenimiento	104
Cortafuegos	104

Capítulo III

Seguridad del software	121
1. Prevenir el código dañino	121
Comprobar la integridad de ficheros	121
2. Bloquear el código dañino	136
DEP	136
ASLR	143
3. Bloquear el código en general	155
Directivas de restricción de software	155
AppLocker	162

Capítulo IV

Seguridad del software	177
1. En el principio fue EMET	177
Windows Defender Exploit Guard	181
AMSI : Anti Malware Scan Inteface	198

Capítulo V

Seguridad del navegador	203
1. El modo protegido	203
Niveles de integridad	203

2. Funcionalidades del navegador que afectan al sistema operativo.....	214
Amenazas del navegador	214
Zonas de seguridad	216
Control de adjuntos.....	221
WAPD.....	231

Capítulo VI

Seguridad de los datos245

1. TrueCrypt	245
Qué es EFS y cómo funciona	247
Copias de seguridad por archivo	250
Copias de seguridad en general	250
Agentes de recuperación.....	252
Curiosidades EFS	254
Inconvenientes de EFS	255
2. Cifrado de datos con BitLocker	256
BitLocker con y sin TPM	256
Contraseñas en BitLocker.....	258
Ventajas e inconvenientes de BitLocker.....	259
3. Borrado de datos	261

Capítulo VII

Recuperación de pequeños desastres263

1. Modo a prueba de fallos.....	263
Cómo funciona	264
El modo seguro.....	266
2. Consola de recuperación	267
Comprobaciones rutinarias.....	270

Capítulo VIII

Seguridad en Windows 11273

1. Filosofía y mejoras en Windows 11	273
Microsoft Defender Application Guard	275
Microsoft Pluton.....	276
Config Lock.....	276
Personal Data Encryption.....	276

Smart App Control.....	277
Enhanced phishing protection for Microsoft Defender	278
Hardware-enforced stack protection	278
Windows Defender System Guard Secure	278
Windows Credential Guard	279
Resumen.....	281
1. Windows y malware.....	281
Antivirus y el manejo de las expectativas	283
Despedida y cierre.....	287
Apéndice A:	
Configurar Latch para Windows.....	289
1. Instalación y configuración del plugin en Windows	289
2. Utilizando Latch.....	291
Apéndice B:	
Configurar Latch AntiRansomware.....	293
1. Instalación y funcionamiento	293
Apéndice C:	
Configurar Latch Event Monitor y Latch USB.....	297
1. Cómo añadir y configurar un evento.....	301
2. Latch USB Monitor.....	302
Cómo funciona Latch USB Monitor	302
Cómo se instala.....	303
3. Cómo añadir y configurar un servicio en Latch USB Monitor	303
Índice de imágenes	305
Índice alfabético	311
Otros libros publicados.....	315