Índice

Prólogo **13**

Preliminares **15**
1. ¿Era mi abuela una experta en seguridad? 15
2. Objetivos 17
3. Herramientas básicas para este libro 19
4. Descargo de responsabilidad 20

Capítulo I
Seguridad física **21**
1. BIOS 21
   - Contraseñas en la BIOS 21
   - Eludir las contraseñas 22
   - DEP, XD, ND, Enhanced Virus Protection 24
   - Otras opciones 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 65

LM y NTLM 65
Tipos de ataque 68
Syskey 73
Usuarios en Windows 76
Grupos en Windows 78
NTFS se compone de ACL 79
NTFS 81
Permisos en carpetas especiales 92
Opciones de seguridad 100
Privilegios 102
4. Configuración y mantenimiento 102
Cortafuegos 102

Capítulo III
Seguridad del software 119
1. Prevenir el código dañino 119
Comprobar la integridad de ficheros 119
2. Bloquear el código dañino 134
DEP 134
ASLR 141
3. Bloquear el código en general 153
Directivas de restricción de software 153
AppLocker 160

Capítulo IV
Seguridad del software (en Windows 10) 165
1. En el principio fue EMET 165
Windows Defender Exploit Guard 166
AMSI : Anti Malware Scan Inteface 182

Capítulo V
Seguridad del navegador 185
1. El modo protegido 185
Niveles de integridad 185
2. Bastionado y nuevas funcionalidades 199
Amenazas del navegador 199

Zonas de seguridad 201
Control de adjuntos 206
Protección de rastreo 213
WAPD 214

Capítulo VI
Seguridad de los datos 225

1. TrueCrypt 225
   Qué es EFS y cómo funciona 227
   Copias de seguridad por archivo 230
   Copias de seguridad en general 230
   Agentes de recuperación 232
   Curiosidades EFS 234
   Inconvenientes de EFS 235
2. Cifrado de datos con BitLocker 236
   BitLocker con y sin TPM 236
   Contraseñas en BitLocker 238
   Ventajas e inconvenientes de BitLocker 239
3. Borrado de datos 241

Capítulo VII
Recuperación de pequeños desastres 243

1. Modo a prueba de fallos 243
   Cómo funciona 244
   El modo seguro en los Windows más modernos 8 246
2. Consola de recuperación 247

Resumen 251

1. Windows y malware 251
   Antivirus y el manejo de las expectativas 253

Despedida y cierre 257

Apéndice A:
Configurar Latch para Windows 259

1. Instalación y configuración del plugin en Windows 259

2. Utilizando Latch....261

Apéndice B:
Configurar Latch AntiRansomware....263
1. Instalación y funcionamiento....263

Apéndice C:
Configurar Latch Event Monitor y Latch USB....267
1. Cómo añadir y configurar un evento....271
2. Latch USB Monitor....272
Cómo funciona Latch USB Monitor....272
Cómo se instala....273
3. Cómo añadir y configurar un servicio en Latch USB Monitor....273

Índice alfabético....275

Índice de imágenes....279