

1. ÍNDICE

1. ÍNDICE	1
2. PROLOGO	6
3. PRESENTACIÓN	8
4. COPYRIGHT	9
5. CIFRADO: CONCEPTOS PREVIOS	10
5.1. CIFRADO DE FICHERO VS CIFRADO DE DISCO	10
5.1.1. CIFRADO A NIVEL DE FICHERO: EFS (ENCRYPTING FILE SYSTEM):	10
5.1.2. CIFRADO A NIVEL DE DISCO: BITLOCKER	14
5.2. ¿POR QUÉ SE UTILIZA MUCHO MÁS BITLOCKER QUE EFS?	16
5.3. CIFRAR DISCO VS NO CIFRAR DISCO	16
5.3.1. CIFRADO DE DISCOS: VENTAJAS	16
5.3.2. CIFRADO DE DISCOS: INCONVENIENTES	16
5.4. BITLOCKER: FVEK / VMK	17
6. BITLOCKER: SISTEMAS OPERATIVOS	18
7. BITLOCKER: PARTICIONES	19
8. BITLOCKER: SERVICIO	20
9. BITLOCKER: OPERACIONES BÁSICAS	21
9.1. ACCESO DIRECTO GUI	21
9.2. MODOS DE CIFRADO: UNIDAD DE SO	23
9.2.1. DESCRIPCIÓN	23
9.2.2. ¿DÓNDE SE CONFIGURAN? (WIN2008R2 / WIN7 O SUPERIOR)	25
9.2.3. ¿DÓNDE SE CONFIGURAN? (WIN2008 / VISTA)	26
9.2.4. ¿QUÉ MODO ES MÁS SEGURO?	27
9.2.5. USO DE PIN: ¿LOS USUARIOS LO PUEDEN CAMBIAR?	27
9.2.6. USO DE PIN: LONGITUD MÍNIMA Y PERMITIR CARACTERES	28
9.3. CIFRAR / DESCIFRAR UNIDAD C: (SISTEMA)	29
9.3.1. Vía GUI	29
9.3.2. Vía MANAGE-BDE	33
9.3.3. Vía POWERSHELL	35
9.4. VERIFICAR ESTADO	36
9.4.1. Vía GUI	36
9.4.2. Vía MANAGE-BDE	37
9.4.3. Vía POWERSHELL	37
9.5. SUSPENDER O REANUDAR CIFRADO	38
9.5.1. Vía GUI	39
9.5.2. Vía MANAGE-BDE	40
9.5.3. Vía POWERSHELL	40

9.5.4. WINDOWS 10, MEGA-ACTUALIZACIONES Y BITLOCKER	41
9.6. CIFRAR / DESCIFRAR RESTO DE UNIDADES	42
9.6.1. UNIDADES DE DATOS Y/O EXTRAÍBLES: NO ES POSIBLE UTILIZAR TPM	42
9.6.2. UNIDADES DE DATOS Y/O EXTRAÍBLES: ¿CÓMO DESBLOQUEAR LA UNIDAD?	43
9.6.3. UNIDADES DE DATOS Y/O EXTRAÍBLES: CIFRADO POR DEFECTO	44
9.6.4. UNIDADES DE DATOS Y/O EXTRAÍBLES: OPCIONES POST CIFRADO	44
9.6.5. UNIDADES DE DATOS Y/O EXTRAÍBLES: DESBLOQUEO AUTOMÁTICO	45
9.6.6. UNIDADES DE DATOS Y/O EXTRAÍBLES: LECTOR PARA XP / VISTA	48
9.7. VISOR DE EVENTOS	50
10. BITLOCKER: MÉTODOS DE CIFRADO	51
10.1. VER TIPO DE CIFRADO	51
10.2. CONFIGURACIÓN POR DEFECTO Y COMO CAMBIARLA	51
10.3. ¿VALE LA PENA CAMBIAR DE AES 128 A AES 256?	55
11. BITLOCKER: RENDIMIENTO	56
11.1. ¿HAY IMPACTO EN EL RENDIMIENTO?	56
11.2. LABORATORIOS	56
11.2.1. ENTORNO DE LABORATORIO:	56
11.2.2. ESCENARIO 1:	57
11.2.3. ESCENARIO 2:	59
11.2.4. CONCLUSIONES FINALES:	61
12. BITLOCKER: CIFRADO POR HARDWARE	61
12.1. PROCEDIMIENTO	61
12.2. VERIFICACIÓN	63
12.3. CONTROL DE QUÉ CIFRADO SE USA: HARDWARE O SOFTWARE	64
13. SECURE BOOT	66
13.1. SECURE BOOT: ¿QUÉ ES?	66
13.2. UEFI / BIOS (LEGACY)	66
13.2.1. CARACTERÍSTICAS MODO UEFI	67
13.2.2. UEFI VS BIOS (LEGACY)	67
13.2.3. CONVERSIÓN BIOS (LEGACY) A UEFI	69
13.3. SECURE BOOT Y BITLOCKER	71
13.4. SECURE BOOT: ¿CÓMO SABER SI ESTÁ ACTIVADO?	73
14. TPM	75
14.1. TPM: ¿QUÉ ES?	75
14.2. TPM: VERIFICAR SI ESTÁ ACTIVADO	75
14.3. AUTOPROVISIONADO TPM	79
14.4. MODO BLOQUEO TPM	80
14.4.1. MODO BLOQUEO: ¿QUÉ ES?	80
14.4.2. MODO BLOQUEO: ¿CUÁNTOS INTENTOS FALLIDOS?	80
14.4.3. MODO BLOQUEO: ¿CÓMO DESBLOQUEAR?	82
14.5. ELIMINAR DATOS EN TPM	83

14.5.1. PROCEDIMIENTO A SEGUIR:	83
14.5.2. OTRAS FORMAS PARA ELIMINAR DATOS DEL TPM:	85
14.6. TPM OWNER PASSWORD	86
14.7. RECOPIRAR LOGS	88
14.8. BITLOCKER SIN TPM	90
14.8.1. CONFIGURACIÓN GUI	90
14.9. TPM EN MÁQUINAS VIRTUALES	93
14.9.1. VMWARE WORKSTATION	94
14.9.2. VMWARE ESXi	97
14.9.3. MICROSOFT HYPER-V	97

15. BITLOCKER: “CIFRAR ESPACIO UTILIZADO” VS “CIFRAR UNIDAD ENTERA” **99**

15.1. DIFERENCIAS ENTRE: “CIFRAR ESPACIO UTILIZADO” Y “CIFRAR UNIDAD ENTERA”	99
15.2. CONFIGURAR DESDE LÍNEA DE COMANDOS:	99
15.3. CONFIGURAR DESDE DIRECTIVA DE GRUPO (GPO):	100
15.4. ¿CÓMO VER SI SE HA CIFRADO CON UN MODO U OTRO?	101
15.5. PASAR A MODO CIFRAR TODO EL DISCO	101

16. BITLOCKER: COMPROBACIÓN DEL SISTEMA **102**

17. BITLOCKER: CLAVE DE RECUPERACIÓN **103**

17.1. ¿QUÉ ES Y PARA QUÉ SIRVE?	103
17.2. ¿CÓMO PUEDO SABER LA CLAVE DE RECUPERACIÓN ACTUAL?	104
17.3. FORZAR RECUPERACIÓN	105
17.4. GENERAR CLAVE DE RECUPERACIÓN NUEVA	105
17.5. CASOS EN QUE SE PIDE LA CLAVE DE RECUPERACIÓN	106
17.6. PCR	109
17.6.1. PCR: ¿QUÉ ES?	109
17.6.2. DEFINIR LOS PCR QUE QUEREMOS QUE ACTÚEN	109
17.6.3. NIVELES DE PCR: SO: VISTA, WIN2008, WIN7, WIN2008R2 O BIOS	111
17.6.4. NIVELES DE PCR: UEFI NATIVO	112
17.6.5. VER PCRS UTILIZADOS	114
17.6.6. CONSIDERACIONES FINALES	115
17.7. GUARDAR CLAVE RECUPERACIÓN EN AD	115
17.7.1. ESQUEMA DE AD	116
17.7.2. INSTALAR HERRAMIENTAS BITLOCKER EN AD	117
17.7.3. DIRECTIVAS DE GRUPO (GPO): WIN2008 Y VISTA	119
17.7.4. DIRECTIVAS DE GRUPO (GPO): A PARTIR DE WIN2008R2 Y WINDOWS 7	120
17.7.5. CIFRADO DESDE EL LADO CLIENTE Y GUARDAR EN AD	122
17.7.6. VISTA GUI BÁSICA: CLAVE DE RECUPERACIÓN GUARDADA EN AD	122
17.7.7. VISTA GUI AVANZADA: CLAVE DE RECUPERACIÓN GUARDADA EN AD	124
17.7.8. VER CLAVE DE RECUPERACIÓN GUARDADA EN AD VÍA POWERSHELL	127
17.7.9. GUARDAR EN AD DESPUÉS DEL CIFRADO	128
17.7.10. DELEGAR PERMISOS PARA VER LAS CLAVES DE RECUPERACIÓN GUARDADAS EN AD	130
17.7.11. EQUIPO DE AD CON CLAVE ALMACENADA: QUITAR, AÑADIR, RENOMBRAR...	136
17.8. GUARDAR CLAVE DE RECUPERACIÓN EN LA NUBE DE MICROSOFT	137
17.9. OTROS MÉTODOS DE ALMACENADO DE LA CLAVE DE RECUPERACIÓN	138

18. ACCEDER OFFLINE A UN DISCO CIFRADO	140
18.1.1. DESDE WINDOWS	140
18.1.2. DESDE LINUX	141
19. BITLOCKER EN DISCO VIRTUAL (VHDX)	143
19.1. ¿PARA QUÉ SIRVE?	143
19.2. CONFIGURACIÓN GUI	143
19.2.1. CREAR VHDX	143
19.2.2. VHDX: INICIALIZAMOS, FORMATEAMOS Y ASIGNAMOS LETRA DE UNIDAD	145
19.2.3. VHDX: CIFRAMOS	146
19.2.4. VHDX: MONTAR DISCO	147
19.3. CONFIGURACIÓN LÍNEA DE COMANDOS	147
19.4. VHDX AUTOMOUNT	149
20. BITLOCKER REPAIR TOOL	150
20.1. USO Y REQUISITOS	150
20.2. EJEMPLOS DE USO	151
20.2.1. REPAIR-BDE UTILIZANDO PASSWORD	151
20.2.2. REPAIR-BDE UTILIZANDO CLAVE DE RECUPERACIÓN	152
20.2.3. REPAIR-BDE UTILIZANDO CLAVE EN USB	152
21. BITLOCKER: AUTOMATIZACIÓN	153
21.1. ESCENARIO	153
21.2. IMPLEMENTACIÓN	153
21.2.1. DIRECTIVAS DE GRUPO (GPO)	153
21.2.2. AD: INSTALAR VISOR DE CONTRASEÑAS BITLOCKER	161
21.2.3. PRUEBA WINRM	162
21.2.4. SCRIPT	163
22. BITLOCKER: CIFRADO DE DISPOSITIVO (DEVICE ENCRYPTION)	164
22.1. ¿QUÉ ES?	164
22.2. ¿CUÁNDO SE PRODUCE?	164
22.3. ¿DÓNDE SE GUARDA LA CLAVE DE RECUPERACIÓN DE BITLOCKER?	166
22.3.1. SI EL EQUIPO NO ESTÁ UNIDO AL DOMINIO:	166
22.3.2. SI EL EQUIPO ESTÁ AÑADIDO AL DOMINIO:	167
22.3.3. SI EL EQUIPO INICIA SESIÓN EN UNA CUENTA DE AZURE AD:	167
22.4. ¿CÓMO SE DESACTIVA ESTA FUNCIONALIDAD?	168
22.5. REQUISITOS	169
22.6. WINDOWS 10 HOME	171
23. MICROSOFT BITLOCKER ADMINISTRATION AND MONITORING (MBAM)	171
23.1. UTILIDAD Y REQUISITOS	171
23.2. INSTALACIÓN SERVIDOR	172
23.2.1. ESCENARIO	172

23.2.2. ACTIVE DIRECTORY	172
23.2.3. SPN (SERVICE PRINCIPAL NAME)	174
23.2.4. IIS	175
23.2.5. SQL SERVER: INSTALACIÓN	176
23.2.6. SQL SERVER: CONFIGURACIÓN	177
23.2.7. INSTALAR SERVIDOR MBAM	178
23.2.8. MBAM: CONFIGURACIÓN	179
23.2.9. MBAM: CONFIG USUARIOS/BASE DE DATOS	180
23.2.10. MBAM: CONFIG INFORMES	181
23.2.11. MBAM: CONFIG WEB	183
23.3. RESULTADO POST-INSTALACIÓN	185
23.4. INSTALACIÓN CLIENTE	186
23.5. PLANTILLAS ADMINISTRATIVAS	187
24. PRÓXIMAS PUBLICACIONES	190

Puedes adquirir este libro en la editorial LULU:

<http://www.lulu.com/shop/search.ep?contributorId=1107000>

Como continuación de estos libros sobre administración de sistemas IT, dispones del blog:

SYSADMIT

<http://www.sysadmit.com>