Windows Vista

Última modificación 2009/04

“In a world without walls and fences,
who needs windows and gates?”

2009 – Güimi (http://guimi.net)
Esta obra está bajo una licencia "Reconocimiento-Compartir bajo la misma licencia 3.0 España" de Creative Commons.
Para ver una copia de esta licencia, visite http://guimi.net/index.php?pag_id=licencia/cc-by-sa-30-es_human.html.

Reconocimiento tautológico: Todas las marcas pertenecen a sus respectivos propietarios.

Windows Vista

Índice de contenido

INTRODUCCIÓN

Fuentes: Wikipedia (http://www.wikipedia.org)

CARACTERÍSTICAS

Algunas de las características más anunciadas son:

- Windows Vista está concebido para garantizar compatibilidad total con EFI (*Extensible Firmware Interface*) y utiliza GPT (GUID Partition Table)
- Nueva API WinFX, orientada a reemplazar la API actual Win32.
- Windows Aero: Nueva interfaz gráfica que sustituye a la Interfaz gráfica de Windows XP (Luna). Incorpora características como la semitransparencia de las ventanas o el "Flip 3D".
- Windows Sidebar: (Barra lateral de Windows) es una nueva herramienta la cual se ubica en el costado derecho de la pantalla y en la cual hay pequeños programas o Gadgets los cuales permiten tener acceso a pequeñas herramientas sin necesidad de abrir una ventana.
- Windows Defender: Un sistema antispyware.
- Windows Mail: cliente de correo electrónico, reemplaza a Outlook Express.
- BitLocker: Cifrado de volúmenes de datos.
- User Account Control: (Control de cuenta de usuario) Sistema de seguridad que solicita permiso al usuario antes de realizar acciones de administrador.
- Windows Dreamscene: fondo de pantalla basado en un vídeo.
- Windows Software Protection Platform (WSPP): sustituye a Windows Genuine Advantage (WGA).
- Mejoras en el gestor de discos: Permite redimensionar particiones.
- Backup and Restore Center: Reemplaza a NTBackup. En las versiones "Home" solo permite copiar ficheros de usuario. En las versiones "profesionales" permite hacer una copia completa de modo similar a Ghost o partimage. No permite copiar/restaurar ficheros individuales (!).
- Windows Imaging Format (WIM): formato de imágenes de disco (como .ISO) basado en ficheros (no en sectores) que debe ser volcado sobre una partición formateada existente. Se puede utilizar el comando DiskPart para crear particiones. Un fichero WIM puede ser seccionado en ficheros .swm. El comando ImageX permite crear y editar ficheros WIM.

VERSIONES

Existen 6 versiones de Vista[1]. La versión "Starter Edition" es solo para "mercados emergentes", limita el número de aplicaciones concurrentes a 3, no está disponible para 64 bits y no dispone de ninguna de las nuevas herramientas y opciones de Vista. Las principales diferencias del resto de versiones se puede ver en la siguiente tabla:

	Home Basic	Home Premium	Business	Enterprise	Ultimate
Aero	No	X	X	X	X
Dominios	No	No	X	X	X
Remote Desktop	No	No	X	X	X
Complete PC Backup	No	No	X	X	X
BitLocker	No	No	No	X	X
Dreamscene	No	No	No	No	X

1 Además de dos versiones "embebidas": "Business" y "Ultimate"

SEGURIDAD EN WINDOWS VISTA

CONFIGURACIÓN DE POLÍTICAS DE SEGURIDAD

Extraído de: http://www.microsoft.com/latam/technet/windowsvista/security/security_group_policy_settings.mspx

Recomendaciones para la configuración de la directiva de contraseñas

(Conf. del equipo\Conf. de Windows\Conf. de seguridad\Directivas de cuenta\Directiva de contraseñas)

Parámetro	Valor predeterminado de Windows Vista	Valor predeterminado del contr. de dominio	GPO de dominio de VSG para EC	GPO de dominio de VSG para SSLF
Exigir historial de contraseñas	0 contraseñas recordadas	24 contraseñas recordadas	24 contraseñas recordadas	24 contraseñas recordadas
Vigencia máxima de la contraseña	42 días	42 días	90 días	90 días
Vigencia mínima de la contraseña	0 días	1 día	1 día	1 día
Longitud mínima de la contraseña	0 caracteres	7 caracteres	8 caracteres	12 caracteres
La contraseña debe cumplir los requisitos de complejidad	Deshabilitado	Habilitado	Habilitado	Habilitado
Almacenar contraseñas usando cifrado reversible	Deshabilitado	Deshabilitado	Deshabilitado	Deshabilitado

Recomendaciones para la configuración de la directiva de bloqueo de cuentas

(Conf. del equipo\Conf. de Windows\Conf. de seguridad\Directivas de cuenta\Directiva de bloqueo de cuentas)

Parámetro	Valor predeterminado de Windows Vista	Valor predeterminado del controlador de dominio	GPO de dominio de VSG para EC	GPO de dominio de VSG → SSLF
Duración del bloqueo de cuenta	No definido	No definido	15 minutos	15 minutos
Umbral de bloqueo de la cuenta	0 intentos de inicio de sesión no válidos	0 intentos de inicio de sesión no válidos	50 intentos de inicio de sesión no válidos	10 intentos de inicio de sesión no válidos
Restablecer recuentos de bloqueo de cuenta tras	No definido	No definido	15 minutos	15 minutos

Recomendaciones para la configuración de la directiva de auditoría

(Conf. del equipo\Conf. de Windows\Configuración de seguridad\Directivas locales\Directiva de auditoría)

Parámetro	Valor predeterminado de Windows Vista	GPO de equipos de VSG para EC	GPO de equipos de VSG para SSLF
Auditar eventos de inicio de sesión de cuenta	Sin auditoría	Correcto	No definido
Auditar la administración de cuentas	Sin auditoría	Correcto	No definido
Auditar el acceso del servicio de directorio	Sin auditoría	No definido	No definido
Auditar eventos de inicio de sesión	Sin auditoría	Correcto	No definido
Auditar el acceso a objetos	Sin auditoría	Sin auditoría	No definido
Auditar el cambio de directivas	Sin auditoría	Correcto	No definido
Auditar el uso de privilegios	Sin auditoría	Sin auditoría	No definido
Auditar el seguimiento de procesos	Sin auditoría	Sin auditoría	No definido
Auditar eventos del sistema	Sin auditoría	Correcto	No definido

La diferencia de Windows Vista con versiones anteriores estriba en que, con Windows Vista, la administración de las directivas de auditoría es más precisa puesto que se incluyen cincuenta subcategorías de directivas de auditoría.
El Editor de objetos de directiva de grupo, como en anteriores versiones, permite configurar las categorías pero no permite configurar las nuevas subcategorías de manera individual. Al configurar cualquiera de las categorías de auditoría en Windows Vista con el Editor de objetos se configuran todas las subcategorías. En este caso, lo más probable es que se produzca un registro excesivo de auditoría que llene con rapidez los registros de eventos.
Para configurar cada subcategoría, hay que usar una herramienta de línea de comandos denominada *AuditPol.exe*.

Para borrar la configuración actual de directiva de auditoría:
```
auditpol /clear
```
Para establecer una configuración personalizada de directiva de auditoría, por ejemplo:
```
auditpol /set /subcategory:"logon" /success:enable /failure:enable
```
Para ver todas las categorías y subcategorías posibles:
```
auditpol /list /subcategory:*
```
Para copiar las políticas de auditoría:
```
auditpol /backup /file:EC-AuditPolicy.txt
```

CONTROL DE CUENTAS DE USUARIO (UAC)

Extraído de apuntes de Fernando Ferrer (http://fferrer.dsic.upv.es/)

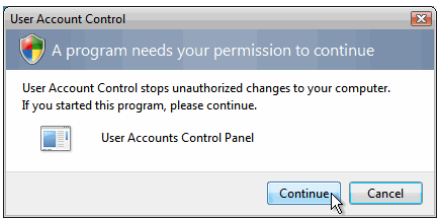
Breve recordatorio sobre versiones anteriores

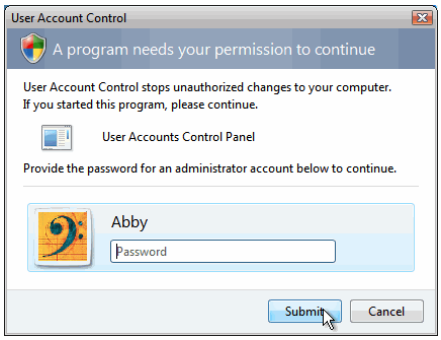
Por defecto, cuando se instalaba Windows XP, el asistente de configuración crea todas las cuentas como administradores locales. Este tipo de cuenta habilitaba a los usuarios el poder instalar, actualizar y ejecutar software ya que una cuenta de administrador posee todos los privilegios para acceder al sistema. Cuando un usuario es añadido al grupo de administradores locales, ese usuario tiene concedidos automáticamente los privilegios necesarios del sistema.
Como ya sabemos, los privilegios no deben confundirse con los permisos. Los permisos se aplican a los objetos, mientras que los privilegios a las cuentas de usuario.
Estos privilegios se acumulan en una ficha ("*token*") de acceso de usuario, el cual también contiene datos específicos del usuario con propósitos de autorización. Microsoft Windows utiliza estas fichas de acceso para saber que recursos un usuario puede acceder. Cada recurso en Windows tiene una lista de control de acceso (ACL) que representa una lista de entradas definiendo los usuarios y servicios que tienen permisos para acceder al recurso y que nivel de permisos tienen.
Los usuarios administradores, automáticamente tienen:

- Lectura/Escritura/Ejecución sobre todos los recursos
- Todos los privilegios del sistema Windows

UAC en Windows Vista

Sin embargo Windows Vista tiene una característica pre-definida que automáticamente reduce los potenciales agujeros de seguridad que pueda tener el sistema.
El Control de Cuenta de Usuario (UAC), obliga a los usuarios que son parte del grupo administradores locales a comportarse como si fueran usuarios normales sin privilegios administrativos. Siempre que un usuario perteneciente al grupo de administradores locales o incluso si es miembro de grupo Administradores del Dominio (en el caso de que el ordenador en cuestión pertenezca a un dominio de *Active Directory*) intente realizar una tarea que requiera privilegios administrativos, el sistema operativo interrumpe la operación para solicitar del usuario un reconocimiento previo a la ejecución de la tarea.
En el caso de que el usuario no sea un miembro del grupo local Administradores, y el usuario requiere privilegios para poder realizar la tarea encomendada, el sistema solicitará al usuario que introduzca las credenciales válidas de un administrador (esto es similar a lo que ocurre en Windows XP/2003 cuando se invoca al comando "*Run As*").



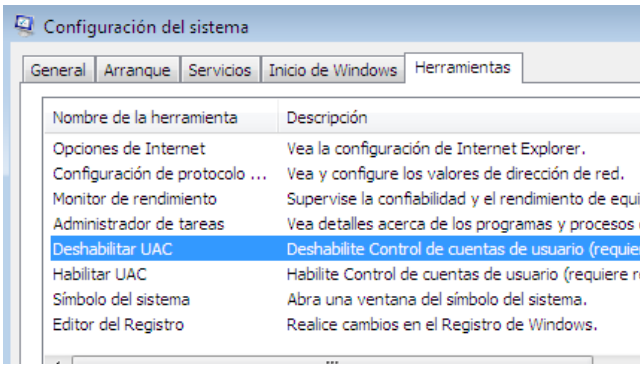


Deshabilitar UAC

Aunque UAC aumenta la seguridad de Windows Vista, seguramente bajo ciertas circunstancias como usuario avanzado, querrás deshabilitarlo, aunque la recomendación es que te acostumbres a él. De todas formas, a continuación se detallarán los pasos para poder hacerlo.

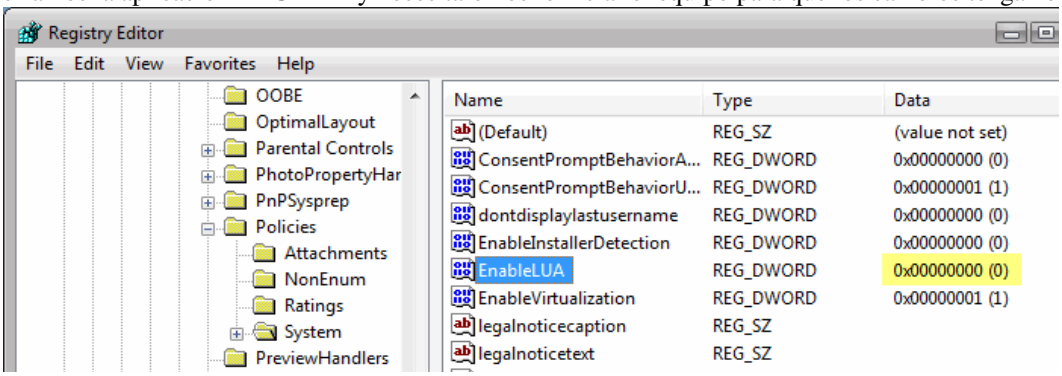
Método 1: MSCONFIG

1. Lanza MSCONFIG desde el menú Ejecutar.
2. Haz click en la pestaña herramientas. Busca la entradad Deshabilitar UAC y marcala
3. Presiona el botón Aceptar.
4. Una consola CMD aparecerá y cuando esta termine se puede cerrar.
5. Cierra MSCONFIG. Necesitaremos reinicar el sistema para que los cambios surtan efecto.



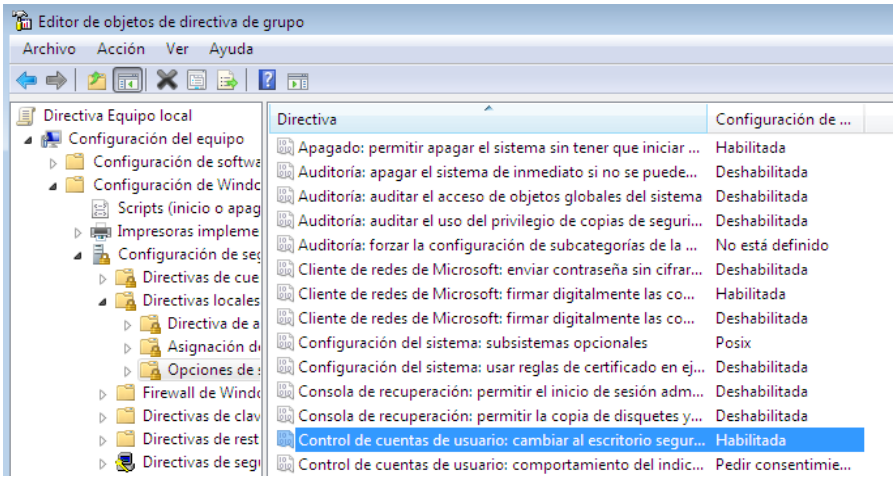
Método 2: Regedit.exe

1. Ejecutamos regedit.exe
2. En el editor del registro navegamos hasta que encontremos la clave de registro:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
3. Hay que localizar la clave EnableLUA (DWORD) y asignarle un valor igual a 0.
4. Cerramos la aplicación REGEDIT y necesitaremos reiniciar el equipo para que los cambios tengan efecto.



Método 3: Políticas de Grupo

Se puede obtener el mismo resultado aplicando una política de grupo bien local o de dominio (que sería preferible para redes corporativas donde el cambio se debe realizar a múltiples ordenadores).
En el editor de políticas deberás de ir hasta
`Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options`



BITLOCKER

Fuentes: http://technet.microsoft.com/es-es/library/cc766295.aspx y
http://technet.microsoft.com/es-es/library/cc732774.aspx#BKMK_SystemDesign
http://en.wikipedia.org/wiki/Bitlocker

Introducción

BitLocker es un sistema de cifrado de volumen de las ediciones "Enterprise" y "Ultimate" de Windows Vista que cifra los datos de un volumen para que no puedan ser accedidos sin la autorización del sistema, ni siquiera conectando el volumen a otro equipo. Cuando se inicia el sistema si BitLocker detecta alguna anomalía entra en modo recuperación y es necesaria la contraseña de recuperación para volver a obtener acceso a los datos.
La seguridad de BitLocker se puede implementar mediante un microchip TPM (Módulo de Plataforma Segura) una BIOS con TCG (Trusted Computing Group) o un lápiz USB actuando como llave (BIOS debe ser capaz de leer el USB antes de que arranque el sistema). Se permiten las siguientes combinaciones:

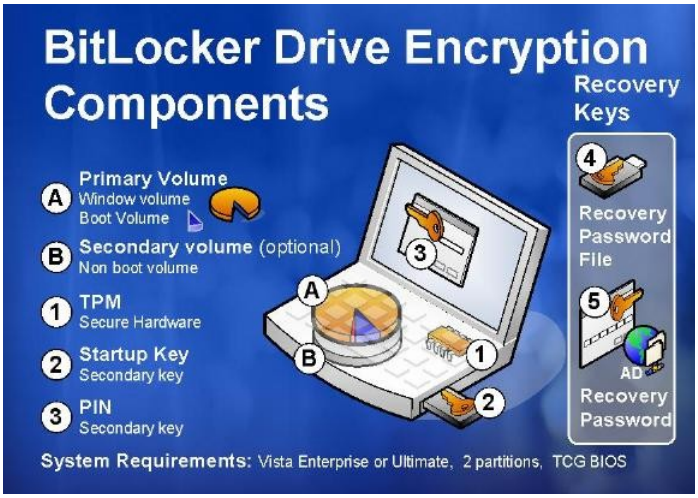
- Solo TPM (Modo trasparente al usuario. No protege frente a robos del equipo completo.)
- TPM + PIN
- TPM + PIN + USB
- TPM + USB
- USB

Para que funcione BitLocker, deben existir al menos dos particiones en el disco duro.:

- La primera partición es el volumen del sistema (S). Este volumen contiene la información de arranque en un espacio no cifrado.
- La segunda partición es el volumen del sistema operativo (C). Este volumen está cifrado y contiene el sistema operativo y los datos de usuario.

Si ya está instalado Windows Vista en una partición simple, puede utilizar la "Herramienta BitLocker de Preparación de la Unidad" para configurar los volúmenes necesarios para BitLocker. Esta herramienta automáticamente crea una partición "S:" de 1,5 GB, mueve los ficheros de arranque y la marca como partición de arranque.

BitLocker cifra el volumen mediante el algoritmo AES en modo CBC[2] con una clave de 128/256 bits para cifrar los volúmenes. Microsoft llama a esta clave "clave de cifrado del volumen completo". Esta clave es a su vez almacenada cifrada con otra clave ("clave maestra de volumen") mediante el algoritmo RSA si se usa TPM o mediante el algoritmo AES si se usa clave de inicio.
Con objeto de evitar los ataques por manipulación de datos cifrados se incorpora un difusor adicional independiente de AES-CBC (Elephant).
Al utilizar un cifrado asimétrico para cifrar la clave de un cifrado simétrico permite regenerar claves fácilmente sin tener que descifrar y cifrar de nuevo todo el volumen.
Además en instalaciones con Active Directory puede utilizarse otra clave añadida para cifrar la clave AES, lo que permite a los usuarios autorizados del directorio acceder al volumen.



Si se deshabilita BitLocker temporalmente (por ejemplo, para actualizar el BIOS o para mover el volumen a otra máquina), el volumen del sistema operativo sigue cifrado, pero la clave maestra de volumen se almacena sin cifrar en el disco duro. Esto anula la seguridad de BitLocker.

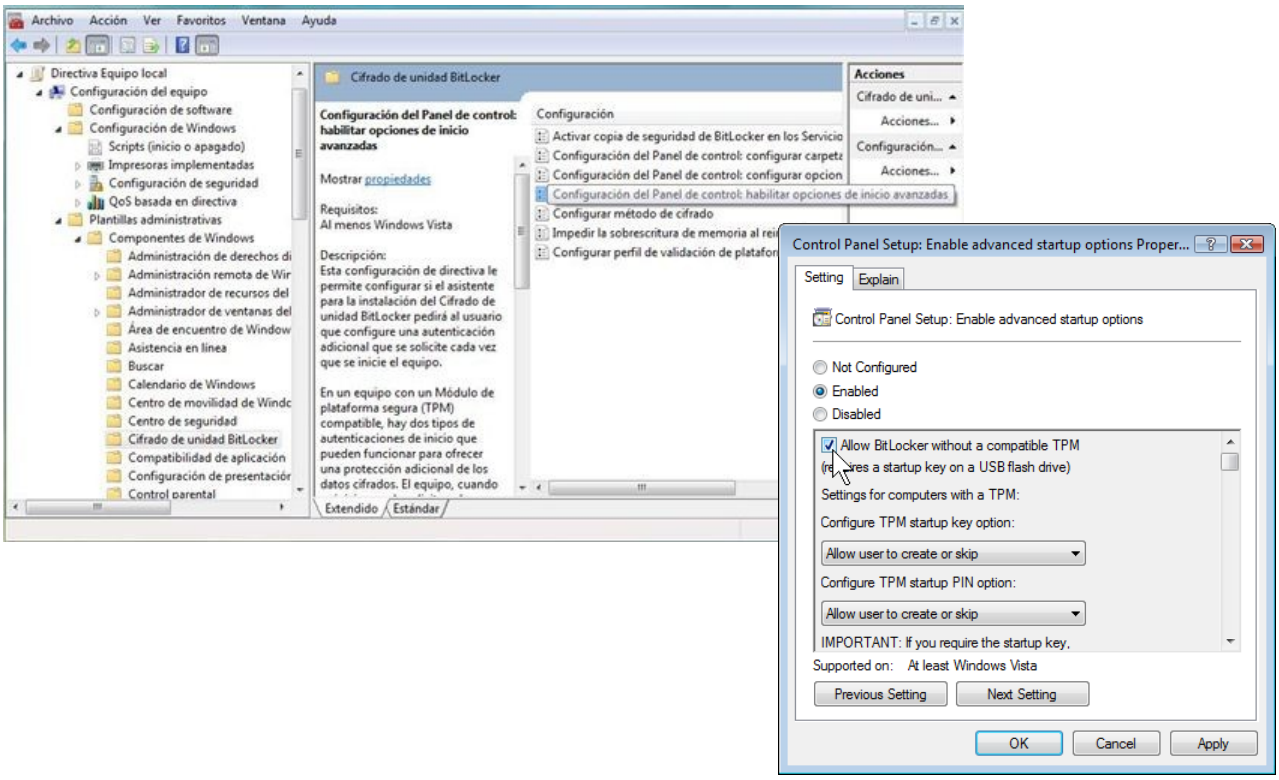
Una vez que BitLocker autentica el acceso al volumen del sistema operativo protegido, un controlador de filtro de la pila del sistema de archivos de Windows Vista (fveol.sys) cifra y descifra sectores del disco de forma transparente a medida que se escriben y se leen datos del volumen protegido.

2 CBC (*Cipher-Block Chaining*) es el modo más utilizado de cifrado por bloques en contraposición al más simple y antiguo ECB (*Electronic CodeBook*). Su principal inconveniente es que el cifrado y descifrado es secuencial y no puede paralelizarse, mientras que en ECB el mensaje se divide en bloques que se cifran separadamente.

Opciones de inicio avanzadas de BitLocker

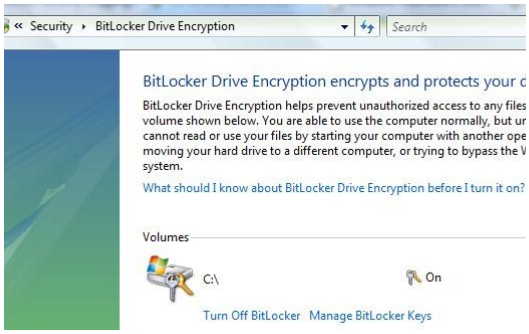
En un escenario sin TPM es necesario utilizar las opciones de inicio avanzadas para ubicar la clave de inicio en una unidad flash USB insertada en el equipo antes de encenderlo. BIOS debe ser capaz de leer unidades flash USB en el entorno previo al sistema operativo (en el momento del inicio).
Las opciones de inicio avanzadas también permiten agregar un NIP (Número de Identificación Personal) como segundo factor de autenticación a la protección TPM estándar.

1. Haga clic en Inicio, escriba **gpedit.msc** en el cuadro Iniciar búsqueda y a continuación presione ENTRAR.
2. Puede aparecer el Control de Cuentas de Usuario.
3. En el árbol de consola **Editor de objetos de directiva de grupo**, haga clic en Directiva de equipo local → Plantillas administrativas → Componentes de Windows → Cifrado de unidad BitLocker.
4. Haga doble clic en el parámetro **Configuración del panel de control: Habilitar opciones de inicio avanzadas**.
5. Seleccione la opción Habilitado, active la casilla "**Permitir BitLocker sin un TPM compatible**" y, a continuación, haga clic en Aceptar.
6. Cierre el Editor de objetos de directiva de grupo.
7. Para que la directiva de grupo se aplique inmediatamente, haga clic en Inicio, escriba **gpupdate.exe /force** en el cuadro Iniciar búsqueda y, a continuación, presione ENTRAR. Espere a que el proceso finalice.



Cifrado de unidad BitLocker

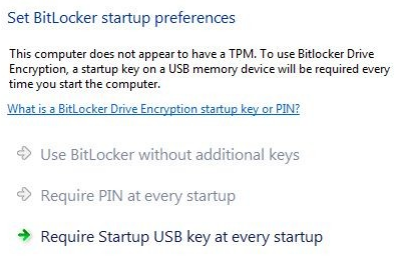
1. Haga clic en **Inicio → Panel de Control → Seguridad → Cifrado de unidad BitLocker**.
2. Puede aparecer el Control de Cuentas de Usuario.
3. En la página Cifrado de unidad BitLocker, haga clic en **Activar BitLocker** en el volumen del sistema operativo.
   1. Si el equipo dispone de TPM y no está inicializado, aparece el asistente para Inicializar el hardware de seguridad de TPM. Siga las instrucciones para inicializar el TPM y reinicie el equipo.
   2. Si el equipo no dispone de TPM pero ha activado Bitlocker sin TPM, en la página "Establecer preferencias de inicio de BitLocker", active la opción "Requerir llave de inicio USB en cada inicio". En la página Guardar la clave de inicio, elija la ubicación de la unidad flash USB y, a continuación, haga clic en Guardar.



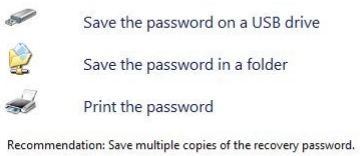
4. En la página **Guardar la contraseña de recuperación**, encontrará las siguientes opciones:
   1. Guardar la contraseña en una unidad USB. Guarda la contraseña en una unidad flash USB.
   2. Guardar la contraseña en una carpeta. Guarda la contraseña en una unidad de red u otra ubicación.
   3. Imprimir la contraseña. Imprime la contraseña.

   Utilice una o más de estas opciones para conservar la contraseña de recuperación (48 dígitos decimales). Cuando haya terminado de guardar la contraseña de recuperación, haga clic en Siguiente.
   Importante: La contraseña de recuperación es obligatoria en el momento de mover una unidad cifrada a otro equipo o cuando se realizan cambios en la información de arranque del sistema. Esta contraseña de recuperación es única y sólo sirve para este cifrado de BitLocker concreto. Para una mayor seguridad, guarde las contraseñas de recuperación en un lugar diferente del equipo.
5. En la página **Cifrar el volumen de disco seleccionado**, confirme que la casilla "Ejecutar la comprobación del sistema de BitLocker" está activada y después haga clic en Continuar.
   Confirme que desea **reiniciar el equipo** haciendo clic en Reiniciar ahora. El equipo se reinicia y BitLocker comprueba si el equipo es compatible con BitLocker y está preparado para cifrar. De no ser así, se muestra un mensaje de error que alerta del problema.
6. **Si está preparado para cifrar, aparece la barra de estado Cifrado en curso**. Una vez terminado este procedimiento, se ha cifrado el volumen del sistema operativo y se ha creado una contraseña de recuperación única para este volumen.
   1. Si utiliza TPM no observará ningún cambio la próxima vez que inicie sesión. Si alguna vez cambia el TPM o no se puede acceder a él, si se producen cambios en archivos clave del sistema, o si alguien intenta arrancar el equipo desde un disco para sortear al sistema operativo, el equipo conmutará a modo de recuperación hasta que se suministre la clave de recuperación.
   2. Si utiliza una clave de inicio en unidad flash en vez de TPM, la próxima vez que encienda el equipo, la unidad flash USB debe estar conectada en un puerto USB del equipo. Si no lo está, no podrá obtener acceso a los datos del volumen cifrado. Si no tiene la unidad flash USB con la clave de inicio, necesitará entrar en el modo de recuperación y proporcionar una contraseña de recuperación para poder tener acceso a los datos.

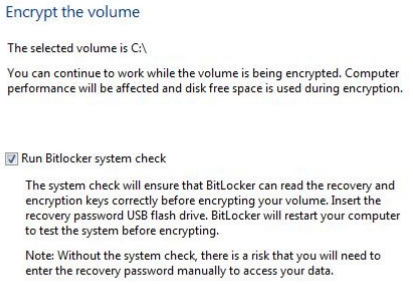
Paso 3.2



Paso 4



Paso 5



Recuperación de datos protegidos con Cifrado de unidad BitLocker

BitLocker bloquea el equipo cuando no se dispone de una clave de cifrado de disco. Posibles causas:

- Se produce un error relacionado con TPM.
- Se modifica uno de los archivos de arranque inicial.
- Se desactiva el TPM involuntariamente y el equipo de apaga.
- Se borra el TPM involuntariamente y el equipo de apaga.
- BitLocker depende de una clave de inicio en unidad Flash que no está disponible.

Cuando se bloquea un equipo, el procedimiento de inicio se interrumpe muy pronto, antes de arrancar el sistema operativo. Debe usar la contraseña de recuperación de una unidad flash USB o escribir la contraseña de recuperación utilizando las teclas de función. Las teclas F1 a F9 representan los dígitos de 1 al 9, y F10 representa el 0.

1. Encienda el equipo.
2. Si el equipo está bloqueado, aparecerá la Consola de recuperación de Cifrado de unidad BitLocker.
3. Se le pedirá que inserte la unidad flash USB que contiene la contraseña de recuperación.
4. Si tiene la unidad flash USB con la contraseña de recuperación, insértela y a continuación presione ESC. El equipo se reiniciará automáticamente. No es necesario que escriba la contraseña de recuperación manualmente.
5. Si no tiene la unidad flash USB con la contraseña de recuperación, presione ENTRAR.
6. Se le solicitará que escriba la contraseña de recuperación manualmente.
7. Si conoce la contraseña de recuperación, escríbala y después presione ENTRAR.
8. Si no conoce la contraseña de recuperación, presione ENTRAR dos veces y apague el equipo.

Si guardó la contraseña de recuperación en un archivo en una carpeta de otro equipo o en un medio extraíble, el archivo que contiene la clave de recuperación utiliza un Identificador de contraseña como nombre de archivo. Busque el Id. de contraseña en la consola de recuperación del equipo bloqueado. Abra el archivo y localice la contraseña de recuperación dentro del mismo.

Comprobación de la recuperación de datos

1. Haga clic en Inicio → Todos los programas → Accesorios → Ejecutar.
2. Escriba **tpm.msc** en el cuadro Abrir y, a continuación, haga clic en Aceptar. Aparece la Consola de administración de TPM.
3. Debajo de Acciones, haga clic **en Desactivar TPM**.
4. Proporcione la contraseña de propietario de TPM, en caso necesario.
5. Cuando en el panel Estado del panel de tareas Administración de TMP en el equipo local se lea "El TPM está desactivado y le han dejado sin propietario", cierre dicho panel de tareas.
6. Reinicie el equipo.
7. Cuando se reinicia el equipo se le pedirá la contraseña de recuperación porque ha cambiado la configuración de arranque desde que cifró el volumen.

Desactivación del Cifrado de unidad BitLocker

1. Haga clic en Inicio, en Panel de Control → Seguridad → Cifrado de unidad BitLocker.
2. Desde la página de Cifrado de unidad BitLocker, busque el volumen para el que desea desactivar BitLocker y haga clic en "**Desactivar Cifrado de unidad BitLocker**".
3. Desde el cuadro de diálogo ¿Qué nivel de descifrado desea? haga clic en Deshabilitar Cifrado de unidad BitLocker o en Descifrar volumen, según sea necesario. Una vez terminado este procedimiento, o bien se ha deshabilitado BitLocker o se ha descifrado el volumen del sistema operativo.

OTRAS CONFIGURACIONES EN WINDOWS VISTA

CONFIGURACIÓN BCD

Extraído de apuntes de Fernando Ferrer (http://fferrer.dsic.upv.es/)

Modificar los datos del Arranque

Para poder modificar los datos de arranque de Windows Vista, Microsoft ha creado una utilidad en línea de comandos denominada `bcdedit`, que permite manipular el almacén de datos de configuración de arranque (BCD). Con esta utilidad se puede definir el orden de arranque de los diferentes sistemas operativos que estén instalados en el PC. La primera operación que habría que realizar es una copia de seguridad de los datos actuales, por si acaso se produce algún problema al manipular el almacén BCD con dicha utilidad.

```
bcdedit /export "D:\BCD Backup.txt"
```

Para mostrar la configuración inicial, utilizaríamos el comando "`bcdedit.exe /enum`":

```
Windows Legacy OS Loader
------------------------------------
dentifier              {ntldr}
device                  partition=D:
path                   \ntldr
description             Earlier Version of Windows

Windows Boot Loader
----------------------------
dentifier              {current}
device                  partition=C:
path                   \Windows\system32\winload.exe
description             Microsoft Windows Vista
locale                  en-US
inherit                {bootloadersettings}
osdevice                partition=C:
systemroot              \Windows
resumeobject            {6a8c2621-1af5-11dc-aaf1-dc87ae6e3f88}
nx                     OptIn

Windows Boot Loader
----------------------------
dentifier              {c15d0020-1aec-11dc-b49c-9726d7e2da89}
device                 partition=G:
path                   \Windows\system32\winload.exe
description            Microsoft Windows Vista
locale                   en-US
inherit                {bootloadersettings}
osdevice               partition=G:
systemroot              \Windows
resumeobject            {c15d0021-1aec-11dc-b49c-9726d7e2da89}
nx                     OptIn
```

Algunas opciones útiles de `bcdedit` ya las hemos visto. A continuación mostraremos algunos otros ejemplos de manipulación del registro BCD:.

Si queremos cambiar el texto mostrado por la entrada de Windws XP:

```
bcdedit /set {ntldr} description "Windows XP"
```

Para cambiar el de la selección actual:

```
bcdedit /set {current} description "Mi Windows Vista"
```

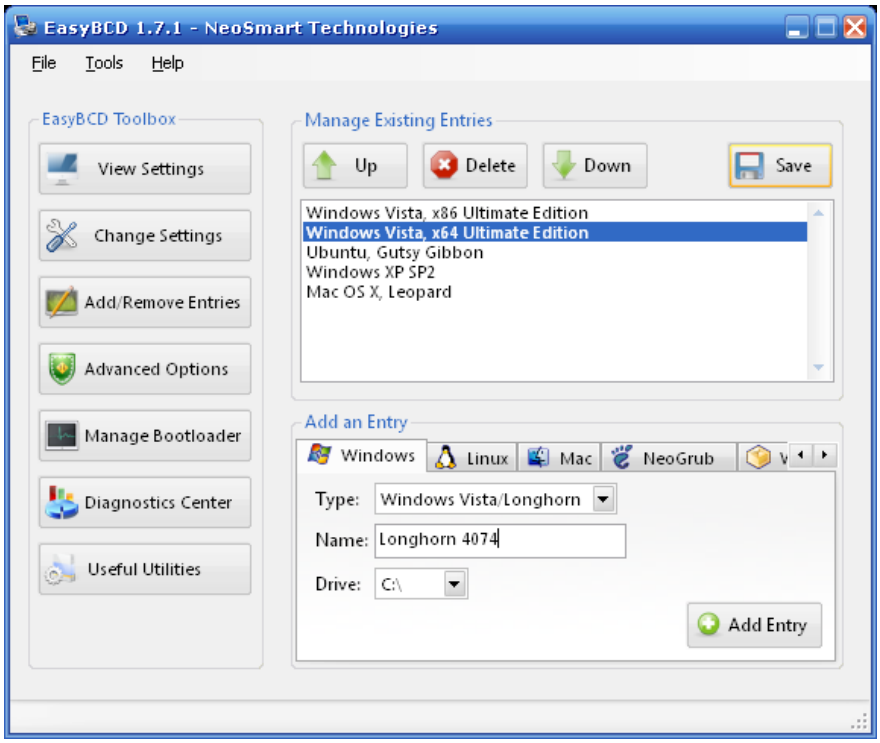
Para cambiar cualquier entrada sería suficiente con saber el identificador:

```
bcdedit /set {c15d0021-1aec-11dc-b49c-9726d7e2da89} description "Windows Vista Mio ;-)"
```

Si por cualquier motivo perdiéramos el registro BCD y tuviéramos que recuperarlo, lo mejor sería iniciar con el DVD de Windows Vista y la fase de recuperación para que escriba un nuevo registro y a partir de aquí manipular el BCD para añadir la entrada de Windows XP con los siguientes comandos:

```
bcdedit /create {ntldr} /d "Windows XP"
bcdedit -set {ntldr} device partition=D:
bcdedit -set {ntldr} path \ntldr
bcdedit -displayorder {ntldr} -addfirst
bcdedit /default {ntldr}
```

Si simplemente queremos cambiar el orden en que se arranquen los distintos sistemas operativos que tenemos en el PC, la utilidad MSCONFIG.EXE es suficiente.
Existe tambien como ya comentamos una utilidad gratuita para manipular el registro BCD denominada EasyBCD (http://neosmart.net/dl.php?id=1)



ACTIVACIÓN DE WINDOWS VISTA

Vista necesita activarse en el plazo de 30 días tras su instalación. El comando para ello es slmgr.vbs (*Software License Manager*). La versión Bussines debe activarse cada 180 días, para lo que existen servidores de licencias (KMS: *Key Management Server*).
Si cambia el *hardware* de la máquina el equipo debe ser activado de nuevo, dando el sistema un plazo de 15 días para ello. Aparentemente esto se puede forzar pidiendo al sistema que refresque la información del sistema mediante `"rundll32 slc.dll,SLReArmWindows"`

Sintaxis del comando (debe ejecutarse con permisos de administrador):

```
slmgr.vbs [MachineName [User Password]] <Option>
```

- `MachineName`: Nombre de la máquina remota (por omisión es la máquina local)
- `User`: Cuenta con privilegios en la máquina remota
- `Password`: Clave de la cuenta

Opciones:

-ipk <product key>	Install product key (replaces existing key)
-ato	Activate Windows
-dli [Activation ID | All]	Display license information (default: current license)
-rearm	Reset the licensing status of the machine (Nuevo plazo de activación de 30 días. Se puede usar un máximo de 4 veces -120 días-)
-upk	Uninstall product key
-dlv [Activation ID | All]	Display detailed license information (default: current license)
-xpr	Expiration date for current license state
-cpky	Clear product key from the registry (prevents disclosure attacks)
-ilc <License file>	Install license
-rilc	Re-install system license files
-dti	Display Installation ID for offline activation
-atp <Confirmation ID>	Activate product with user-provided Confirmation ID
-skms <KMS name>	Set KMS server name
-skms <KMS port>	Set KMS server port number (default 8090)
-skms <KMS name:port>	Set KMS server name and port number in single command
-ckms	Clear KMS server name and port number to default

Al parecer Windows Vista no necesita ser activado si está instalado en equipos portátiles de algunos fabricantes con una clave de instalación específica. Existen herramientas para hacer creer al sistema que se encuentra en esa situación y por tanto que se encuentre activado [1].
Por otra parte existen herramientas para probar por fuerza bruta números de licencia [2].

[1] http://www.quemiras.es/general/como-activar-windows-vista.htm
[2] http://keznews.com/2431_Vista_Brute_Force_Keygen