Microsoft Windows xp | Shared Computer Toolkit

Manual de Microsoft Shared Computer Toolkit para Windows XP

Microsoft
Your potential. Our passion.™

Microsoft Shared Computer Toolkit para Windows XP, v1.0

La información contenida en este documento y en todos los documentos a los que se hace referencia en el mismo tiene únicamente una finalidad informativa, se proporciona TAL CUAL Y CON TODOS LOS DEFECTOS, y no debe entenderse como sustitutiva de un servicio personalizado y de la información que Microsoft Corporation podría desarrollar para un usuario concreto basándose en un entorno específico. El USUARIO ASUME TODO EL RIESGO DERIVADO DE CONFIAR EN ESTE DOCUMENTO Y EN LOS DOCUMENTOS A LOS QUE SE HACE REFERENCIA EN EL MISMO.

MICROSOFT NO OTORGA GARANTÍAS EXPRESAS, IMPLÍCITAS NI LEGALES SOBRE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO NI SOBRE LOS DOCUMENTOS A LOS QUE SE HACE REFERENCIA EN EL MISMO. Microsoft Corporation no otorga ninguna garantía ni se responsabiliza de que la información contenida en este documento o en cualquier documento al que se haga referencia en el mismo sea apropiada para cualquier situación. Microsoft Corporation no se hace responsable de los daños y las reclamaciones de los usuarios de este documento y de los documentos a los que se hace referencia en el mismo. La conservación y el uso de este documento, y de los documentos a los que se hace referencia en el mismo, constituyen una aceptación de estos términos y condiciones. Si no acepta estos términos y condiciones, Microsoft Corporation no le otorgará ningún derecho a usar ninguna parte de este documento ni de ningún documento al que se haga referencia en el mismo.

Contenido

Información general

Los equipos compartidos se suelen encontrar en colegios, bibliotecas, cibercafés, centros comunitarios y otras ubicaciones. Con frecuencia, se pide al personal sin formación técnica que administre los equipos compartidos además de cumplir sus responsabilidades principales.

Equipos compartidos
También se denominan, según su función, equipos de acceso público, quioscos de Internet, equipos de laboratorio y equipos instructivos.

La administración de equipos compartidos puede ser difícil, requerir mucho tiempo y resultar costosa. Sin restricciones, los usuarios pueden cambiar la apariencia del escritorio, volver a establecer la configuración del sistema e insertar spyware, virus y otros programas peligrosos.La reparación de equipos compartidos requiere gran cantidad de tiempo y trabajo.

La privacidad de los usuarios supone también un problema. Los equipos compartidos suelen utilizar cuentas compartidas en las que el historial de Internet, los documentos en línea y las páginas Web almacenadas en caché quedan disponibles de una persona a otra.

Microsoft® Shared Computer Toolkit para Windows® XP ofrece una forma sencilla y eficaz de defender equipos compartidos ante usuarios que no son de confianza y software malintencionado, restringir el acceso de los usuarios a los recursos de sistema y mejorar y simplificar la experiencia del usuario. El Toolkit se ejecuta en copias auténticas de Windows XP Professional, Windows XP Home Edition y Windows XP Tablet PC Edition.

En esta sección de información general se tratan los siguientes temas:

- Audiencia
- Resumen de las herramientas
- Entornos compatibles
- Resumen de los capítulos
- Convenciones de estilo
- Recursos y comunidad
- Descarga del Toolkit
- Información de soporte técnico

Audiencia

operadores
Personas responsables de la administración de los equipos compartidos.

Microsoft Shared Computer Toolkit para Windows XP está diseñado para personas que instalan, configuran y administran equipos compartidos en entornos públicos o privados.

En este manual, las personas encargadas de administrar equipos compartidos reciben la denominación de *operadores*. Los operadores de equipos compartidos pueden ser profesores, coordinadores tecnológicos, bibliotecarios o personal de un cibercafé, es decir, personas con conocimientos técnicos de principiante a experto.

Resumen de las herramientas

El Toolkit incluye las siguientes herramientas gráficas:

- **Protección de discos de Windows.** Protege la partición que contiene el sistema operativo Windows y otros programas (normalmente la unidad C:) contra las modificaciones permanentes realizadas durante una sesión de usuario. Los cambios efectuados en el disco se borran en cada reinicio, a no ser que el administrador decida guardarlos.
- **Restricciones del usuario.** Restringe el acceso de los usuarios a programas, opciones y elementos del menú Inicio, y bloquea los perfiles de usuario locales compartidos contra cambios permanentes.Esta herramienta se ha diseñado específicamente para entornos que no utilizan la directiva de grupo y el servicio de directorio de Active Directory®.
- **Introducción.** Proporciona acceso a la configuración y las utilidades del equipo, y facilita el aprendizaje rápido de los conceptos básicos del Toolkit a los operadores que no lo hayan utilizado antes.
- **Administrador de perfiles.** Crea y elimina perfiles de usuario. Con esta herramienta, puede crear perfiles de usuario en unidades alternativas para permitir que los perfiles conserven datos aunque Protección de discos de Windows esté activada. También se puede utilizar la herramienta para eliminar por completo perfiles que se han bloqueado con la herramienta Restricciones del usuario.
- **Accesibilidad**. Pone opciones y utilidades de accesibilidad de Windows, como StickyKeys, FilterKeys y Ampliador, a disposición de usuarios a los que se les ha restringido el acceso al Panel de control y a otras opciones de configuración del sistema.

El Toolkit también dispone de varias herramientas de línea de comandos. Además de las versiones de línea de comandos (en las que se pueden crear secuencias de comandos) de cada una de las herramientas gráficas, el Toolkit incluye las siguientes herramientas:

- **Accounts**. Permite habilitar, deshabilitar y mostrar las cuentas de usuario locales.
- **AutoDemo.** Configura un equipo con cuentas y perfiles para hacer una demostración del Toolkit. Este comando sólo debe ejecutarse en un equipo de demostración, porque configura cuentas y realiza otras funciones del Toolkit.
- **AutoLogon**. Configura una cuenta para iniciar sesión en el equipo automáticamente. Esta herramienta resulta muy útil si se utiliza un software de autenticación de terceros en lugar de la autenticación de Windows (lo cual es frecuente en algunas bibliotecas y cibercafés).
- **AutoRestart**. Configura una cuenta para que el programa se ejecute automáticamente cada vez que un usuario inicie sesión con dicha cuenta.
- **AutoRunOnce.** Configura una cuenta para que el programa se ejecute automáticamente la próxima vez que un usuario inicie sesión con dicha cuenta. Los inicios de sesión posteriores no se ven afectados.
- **CriticalUpdates**. Fuerza al equipo a descargar e instalar actualizaciones críticas sin esperar al siguiente ciclo de actualizaciones críticas de la herramienta Protección de discos de Windows.
- **ForceLogoff**. Permite cerrar sesiones de usuario o reiniciar el equipo.

Importante
Para activar Protección de discos de Windows deben cumplirse unos requisitos previos de partición especiales. Para obtener más información, consulte el capítulo 2, "Preparar el disco para Protección de discos de Windows".

- **SCTReport**. Crea un informe de Shared Computer Toolkit que el Soporte técnico de Microsoft puede utilizar para solucionar los problemas del Toolkit.
- **SleepWakePC**. Pone un equipo compartido en estado de suspensión a una hora concreta (para ahorrar energía) y lo reactiva para llevar a cabo las actualizaciones críticas programadas.
- **Welcome**. Elimina las cuentas mostradas en la pantalla de bienvenida para evitar que los usuarios se confundan o caigan en la tentación de utilizar las cuentas administrativas que aparecen en dicha pantalla.

Entornos compatibles

dominio
Equipos conectados a una red que comparten un directorio central que contiene cuentas de usuario e información de seguridad.

El Toolkit puede utilizarse en entornos de dominio o grupo de trabajo.

Grupos de trabajo

Todas las herramientas del kit han sido diseñadas para facilitar la administración de equipos individuales o que sean miembros de grupos de trabajo de Windows. El Toolkit no necesita una infraestructura de servidores. Puede usarlo en un equipo o en cientos de equipos sin necesidad de utilizar herramientas de administración basadas en servidores.

Para usar el Toolkit en varios equipos, debe estar instalado en cada uno de ellos. Esto le permitirá configurar cada equipo como desee utilizando Restricciones del usuario, Protección de discos de Windows y el resto de herramientas. Los capítulos 1 a 7 describen el proceso completo para usar el Toolkit en equipos de grupo de trabajo.

Dominios

Active Directory
Servicio de directorio de Windows para administrar usuarios y equipos. Para obtener más información, visite el sitio Web oficial de Windows Server 2003 Active Directory (http://go.microsoft.com/fwlink/?LinkId=8596; puede que la página esté en inglés).

El Toolkit se ha diseñado para proteger equipos que forman parte de un dominio de Active Directory.

La herramienta Protección de discos de Windows puede utilizarse en entornos de dominio para proteger equipos contra cambios no deseados. Protección de discos de Windows funciona bien en equipos unidos en un dominio que ejecuten Windows XP.

La herramienta Restricciones del usuario no se ha diseñado para entornos de dominio. Si proporciona, o desea proporcionar, cuentas y contraseñas exclusivas a sus clientes o a equipos que ya forman parte de un dominio de Windows, la mejor solución es usar Active Directory con una directiva de grupo para restringir las actividades de los usuarios. Las directivas de grupo cuentan con las ventajas adicionales de ofrecer una mayor flexibilidad y permitir la administración central, mientras que la función de Restricciones del usuario es administrar únicamente cuentas compartidas locales.

Las restricciones de cuentas de dominio pueden administrarse centralmente mediante la plantilla de directivas de grupo incluida en el Toolkit, que dispone de la mayoría de las opciones de configuración y restricciones de que ofrece la herramienta Restricciones del usuario.

Los operadores de equipos unidos en un dominio deben leer también el capítulo 10, “Shared Computer Toolkit en entornos de domino”.

Resumen de los capítulos

Importante
Los primeros siete capítulos representan los pasos que debe seguir para instalar y utilizar el Toolkit y mejorar la seguridad de un entorno de equipos compartidos.

Los primeros siete capítulos del manual representan los procesos básicos que utilizará para instalar y usar el Toolkit y mejorar la seguridad de un entorno de equipos compartidos. El resto de los capítulos y el apéndice contienen información adicional que le ayudará a solucionar problemas, reproducir escenarios avanzados y conocer temas relacionados con el Toolkit.

Capítulo 1: Instalación

En este capítulo se enumeran los requisitos previos que debe reunir un equipo para instalar el Toolkit. También se explica cómo validar Windows XP mediante el programa Ventajas de Windows Original (http://go.microsoft.com/fwlink/?LinkId=53507; puede que la página esté en inglés), cómo instalar el Toolkit y cómo usar la herramienta Introducción.

Capítulo 2: Preparar el disco para Protección de discos de Windows

El contenido de este capítulo le ayudará a entender los requisitos necesarios para usar la herramienta Protección de discos de Windows. En él se describen los dos mejores métodos para garantizar suficiente espacio de disco sin asignar para Protección de discos de Windows:

- Usar una utilidad de partición de terceros como PartitionMagic 8.0 para cambiar el tamaño de una partición existente que contenga el sistema operativo Windows y los archivos de programa.
- Utilizar la instalación de Windows XP para configurar una partición primaria y dejar espacio no asignado en el disco.

Capítulo 3: Administración de perfiles.

En este capítulo se trata la creación de cuentas locales compartidas, la creación de perfiles para cada cuenta de usuario y la configuración de cada perfil mediante la personalización de la configuración de Windows, el menú Inicio y los programas. La herramienta Administrador de perfiles se utiliza para crear y copiar perfiles de usuario en un equipo compartido.

Capítulo 4: Restricciones del usuario

En este capítulo se describe cómo utilizar la herramienta Restricciones del usuario para restringir y bloquear perfiles de usuario en el equipo con el objeto de protegerlo de usuarios desconocidos o que no sean de confianza.

Capítulo 5: Experiencia de usuario restringida

En este capítulo se ilustra la experiencia que tendrá el usuario típico al utilizar una cuenta compartida que se haya restringido mediante la herramienta Restricciones del usuario.Proporciona un ejemplo de un escritorio restringido típico, una introducción a la herramienta Accesibilidad y una descripción de los recursos de usuario disponibles. También se explica cómo probar las cuentas de usuario iniciando una sesión por cada usuario para comprobar que las restricciones funcionan del modo deseado.

Capítulo 6: Protección de discos de Windows

En este capítulo se describe cómo activar la herramienta Protección de discos de Windows para borrar los cambios realizados en el disco cada vez que el equipo se reinicia y cómo programar la instalación de actualizaciones de software críticas.

También se describe cómo guardar los cambios realizados en el disco y cómo conservarlos cuando Protección de discos de Windows está activada.

Capítulo 7: Lista de comprobación de seguridad

Este capítulo contiene información importante para mejorar la seguridad de los equipos compartidos y su entorno más allá de lo que puede se automatizar mediante el Toolkit.

Capítulo 8: Solución de problemas

En este capítulo se ofrecen consejos para la solución de problemas de cada una de las herramientas del Toolkit.

Capítulo 9: Escenarios avanzados

Este capítulo se centra en los escenarios avanzados más comunes que pueden encontrarse los operadores al utilizar el Toolkit para administrar un entorno de equipos compartidos.

Capítulo 10: Shared Computer Toolkit en entornos de dominio

En este capítulo, se describe cómo utilizar el Toolkit en entornos en los que se dan alguna o varias de estas circunstancias:

- Uso de Active Directory y directivas de grupo
- Uso de servicios de distribución de software centrales
- Necesidad de proporcionar varios idiomas en cada equipo

Apéndice A: Conceptos técnicos elementales

En este apéndice se tratan diversas tecnologías y características cuyo conocimiento resulta importante para trabajar con el Toolkit.

Agradecimientos

Esta sección contiene la lista de las personas que han colaborado en el desarrollo de Shared Computer Toolkit.

Vínculos

Esta sección contiene la lista de las direcciones URL completas de todos los hipervínculos de este manual, destinada a los usuarios que lean la versión impresa.

Índice

En esta sección se muestran los términos más comunes utilizados en el manual con referencias a números de página.

Convenciones de estilo

En la siguiente tabla se enumeran las convenciones de estilo que se utilizan en el manual.

Elemento	Significado
Negrita	Se aplica el estilo de negrita a los nombres de archivo y a los elementos de la interfaz de usuario.
Cursiva o bien *<Cursiva>*	El estilo de cursiva se aplica a los caracteres que escribe el usuario y que éste puede modificar. Los caracteres en cursiva que aparecen entre llaves angulares son marcadores de posición que requieren valores específicos. Ejemplo: <*nombreDeArchivo.ext*> indica que el usuario debe sustituir el nombre en cursiva *nombreDeArchivo.ext* por otro nombre de archivo que sea adecuado para su configuración. La cursiva también se utiliza para representar nuevos términos. Ejemplo: Una *partición de disco* es un compartimento lógico en una unidad de disco física.
Fuente de texto en pantalla	Esta fuente define el texto que aparece en pantalla.
Texto del margen izquierdo	El margen izquierdo se utiliza para los términos y las definiciones.
Nota	Las notas contienen información que puede ayudarle a completar una tarea o comprender un concepto.
Importante	Los avisos con el título Importante contienen información esencial para completar una tarea. También pueden ser advertencias de que debe realizar o evitar una acción concreta.
Procedimientos	Los procedimientos aparecen en casillas sombreadas que destacan en la página.

Recursos y comunidad

El Toolkit incluye una serie de recursos que contienen información útil. Una vez instalado, tendrá a su disposición los siguientes recursos en la carpeta de programas de Microsoft Shared Computer Toolkit en el menú Inicio:

- **Manual de Shared Computer Toolkit**. Este manual proporciona instrucciones detalladas para instalar y utilizar el Toolkit. También contiene temas avanzados, prácticas recomendadas e información técnica.
- **Ayuda de Shared Computer Toolkit**. Los archivos de Ayuda incluidos en el Toolkit contienen información detallada acerca de las características y la funcionalidad de cada herramienta.
- **P+F del Toolkit**. Esta página Web proporciona respuestas a las preguntas más frecuentes acerca del Toolkit.
- **Recursos para administrar equipos compartidos.** Sitio Web y grupo de noticias que ayuda a que las organizaciones con equipos compartidos aprendan y colaboren entre sí; además, constituye un punto de encuentro para la comunidad de acceso compartido.

Para participar en las discusiones con otros operadores, visite el sitio Web del grupo de noticias de Windows Shared Access (http://go.microsoft.com/fwlink/?LinkId=54023; puede que la página esté en inglés). Este sitio Web se ha diseñado como ubicación para publicar preguntas, ayudar a otros usuarios y proporcionar comentarios e ideas para versiones futuras del Toolkit y el manual.

Para los usuarios, la instalación del Toolkit agrega dos nuevos recursos al menú Inicio de Todos los usuarios:

- **Recursos en línea para el uso de equipos públicos.** Sitio Web en línea que contiene vínculos a recursos dirigidos a niños, adolescentes y adultos para aprender a utilizar los equipos, obtener más información acerca de Windows XP y usar Internet de un modo seguro.
- **Accesibilidad**. Acceso directo a la herramienta Accesibilidad para que todos los usuarios tengan acceso a las características de accesibilidad de Windows, aunque tengan restringido dicho acceso.

Descarga del Toolkit

Para descargar el Toolkit, visite la página Microsoft Shared Computer Toolkit para Windows XP del sitio Web Centro de descarga de Microsoft (http://go.microsoft.com/fwlink/?LinkId= 47025; puede que la página esté en inglés).

Para descargar el Toolkit, se requiere la validación de Ventajas de Windows Original (http://go.microsoft.com/fwlink/?LinkId=53507; puede que la página esté en inglés).

Información de soporte técnico

La información de soporte técnico para Microsoft Shared Computer Toolkit para Windows XP está disponible a través de los siguientes recursos (puede que las páginas estén en inglés):

- Sitio Web de Shared Computer Toolkit (http://go.microsoft.com/fwlink/?LinkId=46755)
- Preguntas más frecuentes acerca de Shared Computer Toolkit (http://go.microsoft.com/fwlink/?LinkId=47836)
- Lista de problemas conocidos en la página de descarga de Shared Computer Toolkit (http://go.microsoft.com/fwlink/?LinkId=47025)
- Manual de Shared Computer Toolkit (http://go.microsoft.com/fwlink/?LinkId=51297), en particular el capítulo 9, "Solución de problemas"
- Grupo de noticias acerca del acceso compartido a Windows (http://go.microsoft.com/fwlink/?LinkId=54023) para exponer preguntas sobre productos y consultas de soporte técnico gratuitas.
- Póngase en contacto con el Servicio de soporte técnico (PSS) mediante la dirección URL http://go.microsoft.com/fwlink/?LinkId=52267 si desea obtener asistencia de pago o si ya ha suscrito un acuerdo de soporte técnico. Utilice el Id. de producto de Shared Computer Toolkit cuando se ponga en contacto con el PSS: 77695-100-0001260-04309.

Otros recursos de soporte técnico

Otros recursos de soporte técnico relacionados con equipos compartidos, seguridad y Windows XP (puede que las páginas estén en inglés):

- Recursos para administrar equipos compartidos (http://go.microsoft.com/fwlink/?LinkId=39998)
- Ayuda y compatibilidad con la seguridad para profesionales de TI (http://go.microsoft.com/fwlink/?LinkId=53508)
- Opciones de soporte técnico para usuarios de Windows XP (http://go.microsoft.com/fwlink/?LinkId=8932)

Capítulo 1: Instalación

En este capítulo se tratan los siguientes temas:

- Requisitos de software
- Recomendaciones de software
- Instalar el Toolkit desde el Centro de descarga
- Instalar el Toolkit desde el CD
- Trabajar con software de bloqueo de secuencias de comandos
- Introducción
- Desinstalar el Toolkit

Importante
Para instalar el Toolkit debe reunir los siguientes requisitos de software.

Requisitos de software

Para instalar Microsoft® Shared Computer Toolkit para Windows® XP, se necesitan los siguientes requisitos:

- Windows XP Professional, Windows XP Home Edition o Windows XP Tablet PC Edition.
- Windows XP Service Pack 2 (SP2) (http://go.microsoft.com/fwlink/?LinkId=26348; puede que la página esté en inglés).
- Acceso a Internet para realizar la validación de Ventajas de Windows Original (http://go.microsoft.com/fwlink/?LinkId=53507; puede que la página esté en inglés).
- El Servicio de limpieza del subárbol de perfiles de usuario (http://go.microsoft.com/fwlink/?LinkId=27031; puede que la página esté en inglés) debe estar instalado y en ejecución. Este servicio garantiza que los perfiles se descargan por completo tras el cierre de sesión, lo cual es necesario para el correcto funcionamiento del Toolkit.
- El sistema de archivos del equipo debe ser NTFS. FAT32 y otros sistemas archivos no cumplen los requisitos de seguridad de equipos compartidos.Si el equipo no utiliza NTFS, consulte el artículo 307881 de Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=53509; puede que la página esté en inglés) para saber cómo convertirlo a NTFS antes de instalar el Toolkit.

  El Toolkit requiere que la partición de Windows, el directorio Archivos de programa y la ubicación predeterminada de Documents and Settings estén en volúmenes NTFS. Normalmente esta ubicación suele ser la unidad C:,en cuyo caso dicha unidad deberá emplear el sistema NTFS. Para obtener más información, consulte el sitio sobre las ventajas de usar el sistema NTFS en el sitio Web del kit de recursos de Windows XP (http://go.microsoft.com/fwlink/?LinkId=54026; puede que la página esté en inglés).

Importante
Los iconos de herramientas del menú Inicio sólo aparecerán en la cuenta en la que se instale el Toolkit.

Nota
Es necesario tener acceso a Internet para realizar la validación de Ventajas de Windows Original.

Además, las secuencias de comandos de Windows y el Instrumental de administración de Windows (WMI) deben funcionar correctamente. El instalador garantiza que todos estos requisitos se cumplan y, en caso contrario, ofrece orientación.

Tanto si descarga el Toolkit de Microsoft como si lo instala desde el CD, se requiere acceso a Internet para realizar una validación de Ventajas de Windows Original (http://go.microsoft.com/fwlink/?LinkId=53507; puede que la página esté en inglés). La validación es necesaria para que la herramienta funcione.

Recomendaciones de software

Importante
Puede que algunos programas de seguridad detecten un error de secuencia de comandos malintencionada o sospechosa durante la instalación y utilización del Toolkit. Si esto ocurre, deberá autorizar la ejecución de las secuencias de comandos del Toolkit. Para obtener más información, consulte el capítulo 8, "Solución de problemas".

Shared Computer Toolkit no quitará ni detendrá software malintencionado si ya se encuentra en el equipo. El equipo debe ser de confianza antes de instalar el Toolkit.

Microsoft recomienda instalar el siguiente software:

- Todas las actualizaciones críticas más recientes del sitio Web de Microsoft Update (http://go.microsoft.com/fwlink/?LinkId=17289; puede que la página esté en inglés).
- Asegúrese de que en el equipo no hay software malintencionado mediante la instalación y ejecución de software antivirus y antispyware actualizado.
- Adobe Acrobat Reader (http://go.microsoft.com/fwlink/?LinkId=57398; puede que la página esté en inglés) para ver la versión PDF de este manual.
- Los controles Microsoft ActiveX® y los programas y de confianza que puedan necesitar los clientes.

Algunos programas no son adecuados para los equipos compartidos en algunos escenarios de uso concretos. Considere la posibilidad de no instalar o quitar los siguientes tipos de programas de los equipos compartidos:

- Utilidades de búsqueda de escritorio, ya que pueden revelar información acerca del equipo que no desee que vean los usuarios.
- Clientes de correo electrónico que necesiten configuración, como Microsoft Outlook® o Outlook Express, ya que puede que a los usuarios les lleve demasiado tiempo utilizarlos.
- Componentes de Windows, como Servicios Microsoft Fax y Servicios de Internet Information Server (IIS).

Instalar el Toolkit desde el Centro de descarga

Administrador del Toolkit
Cuenta administrativa que se utiliza para instalar y usar Shared Computer Toolkit.

Puede descargar el Toolkit desde el sitio Web del Centro de descarga de Microsoft (http://go.microsoft.com/fwlink/?LinkId=47025; puede que la página esté en inglés).

Para descargar e instalar el Toolkit

1. Inicie sesión como *administrador del Toolkit*, una cuenta administrativa local que utilizará las herramientas del Toolkit.
2. Descargue el archivo de instalación **Shared_Computer_Toolkit_ENU.msi** del sitio Web de Shared Computer Toolkit (http://go.microsoft.com/fwlink/?LinkId=47025; puede que la página esté en inglés).

3. Si se le pide, valide primero su copia de Windows XP en el sitio Web Ventajas de Windows Original (http://go.microsoft.com/fwlink/?LinkId=53507; puede que la página esté en inglés).
4. Haga doble clic en el archivo de instalación descargado para iniciar la instalación.
5. Revise la página del contrato de licencia y, si está de acuerdo con los términos y condiciones, haga clic en **Acepto los términos del Contrato de licencia** y en **Siguiente**.
6. En la página Información sobre el usuario, puede hacer clic en **Registrarse ahora** para llevar a cabo el proceso de registro opcional.
7. En la página Carpeta de instalación, haga clic en **Siguiente**.
8. En la página Preparado para instalar, haga clic en **Instalar**.
9. En la página de instalación completada, haga clic en **Finalizar** para salir. Si deja activada la casilla de verificación **Ver Introducción**, debe abrirse la herramienta Introducción.

Instalar el Toolkit desde el CD

Si ha recibido el Toolkit en un CD con una copia física del manual, puede instalarlo desde dicho CD.

Para instalar el Toolkit desde el CD

1. Inicie sesión como *administrador del Toolkit*, una cuenta administrativa local que utilizará las herramientas del Toolkit.
2. Inserte el CD en la unidad de CD-ROM del equipo. Si el CD no se inicia automáticamente, busque el archivo **AutoRun.hta** y haga doble clic en él.
3. Si es necesario, haga clic en el vínculo de Ventajas de Windows Original (http://go.microsoft.com/fwlink/?LinkId=53507; puede que la página esté en inglés) para realizar el proceso de validación.
4. Haga clic en **Instalación del Toolkit**.
5. Revise la página del contrato de licencia y, si está de acuerdo con los términos y condiciones, haga clic en **Acepto los términos del Contrato de licencia** y en **Siguiente**.
6. En la página Información sobre el usuario, puede hacer clic en **Registrarse ahora** para llevar a cabo el proceso de registro opcional.
7. En la página Carpeta de instalación, haga clic en **Siguiente**.
8. En la página Preparado para instalar, haga clic en **Instalar**.
9. En la página de instalación completada, haga clic en **Finalizar** para salir. Si deja activada la casilla de verificación **Ver Introducción**, debe abrirse la herramienta Introducción.

Trabajar con software de bloqueo de secuencias de comandos

Nota
Algunos programas de bloqueo no permiten la aprobación permanente de secuencias de comandos. Si no puede aprobar permanentemente las secuencias de comandos del Toolkit, desactive el bloqueo.

Existen muchas herramientas de seguridad, protección del sistema y antispyware que bloquean el acceso a secuencias de comandos para proteger el equipo. Si reconoce una secuencia de comandos como perteneciente a Shared Computer Toolkit, deberá autorizar su ejecución o de lo contrario se producirá un comportamiento inesperado.

Para garantizar un correcto funcionamiento del Toolkit y las actualizaciones críticas utilizando un software de bloqueo de secuencias de comandos, permita la ejecución de éstas ejecutando el archivo **RunAllScripts.bat** desde la carpeta Scripts de la instalación y apruebe cada una de las secuencias de comandos como administrador del Toolkit.

A fin de habilitar la ejecución de las secuencias de comandos que requiere el Toolkit para los usuarios, consulte la sección "Configurar perfiles de usuario locales" del capítulo 3, "Administración de perfiles".

Introducción

Una vez finalizado el proceso de instalación, la herramienta Introducción se abrirá (a menos que haya desactivado la casilla de verificación **Ver Introducción** durante la instalación). Introducción también se abre de manera predeterminada cada vez que se inicia sesión en el equipo compartido con la cuenta de administrador del Toolkit, que es la cuenta utilizada para instalar el Toolkit. La herramienta Introducción ofrece información general y accesos directos a las herramientas y recursos disponibles en el Toolkit. Introducción proporciona los siguientes pasos y consejos para ayudarle a iniciarse rápidamente en la utilización del Toolkit:

- **Paso 1. Preparar el disco para Protección de discos de Windows**. En esta sección, la herramienta Introducción indica si el disco del equipo compartido está configurado correctamente para Protección de discos de Windows. Si no, ofrece consejos para configurar el disco. Muestra además si la herramienta Protección de discos de Windows está actualmente activada o desactivada. También puede obtener más información sobre cómo preparar un disco para Protección de discos de Windows en el capítulo 2, “Preparar el disco para Protección de discos de Windows”.
- **Paso 2. Seleccionar la configuración de seguridad del equipo**. En esta sección se proporcionan opciones de gran valor para mejorar la seguridad del equipo compartido. A diferencia de las restricciones disponibles en la herramienta Restricciones del usuario, que se aplican por usuario, las opciones de esta sección se aplican a cualquiera que utilice el equipo compartido. Entre las opciones que se pueden seleccionar en esta sección se incluyen:
    - **Impedir que los nombres de cuenta se guarden en el diálogo de inicio de sesión CTRL+ALT+SUPR**. De manera predeterminada, Windows muestra el nombre del usuario utilizado por última vez para iniciar sesión en Windows en el cuadro de diálogo de inicio de sesión tradicional que se abre al presionar CTRL+ALT+SUPR en la pantalla de bienvenida de Windows.
    - **Hacer que Windows almacene contraseñas en un formato seguro (sin usar LMHash)**. Esta configuración mejora la seguridad del almacenamiento de las contraseñas mediante la deshabilitación del

hash LanMan de cada una de ellas. El hash LanMan (o LMHash) es un mecanismo de cifrado que se utiliza para la compatibilidad con versiones anteriores y que se puede descifrar con facilidad.

- **Impedir que Windows almacene credenciales de dominio o Passport en la caché de los perfiles de usuario**. Si se activa esta casilla de verificación, los usuarios deben especificar sus credenciales de dominio y Passport cada vez que se les solicite. Windows no las guarda entre sesiones de usuarios.
- **Impedir que los usuarios creen archivos y carpetas en la unidad del sistema de Windows**. Esta configuración cambia la lista de control de acceso (ACL) en la raíz de C: para impedir que los usuarios creen archivos y carpetas dentro de la misma. Esta configuración no afecta a las ACL de las demás carpetas.
- **Impedir el inicio de sesión para los perfiles de usuario bloqueados (o itinerantes) que no se puedan encontrar**. Normalmente, Windows crea un nuevo perfil de usuario (posiblemente sin restricciones) cuando una persona intenta iniciar sesión con un perfil que Windows no encuentra. Dicha opción evita que esto suceda.
- **Quitar copias almacenadas en caché de perfiles de usuario bloqueados (o itinerantes) con el fin de mejorar la privacidad y ahorrar espacio en disco**. Cuando se selecciona esta opción, Windows no guarda los perfiles de usuarios bloqueados (o itinerantes). De este modo, se evita que otras personas puedan examinar los perfiles de los usuarios que hayan iniciado una sesión anteriormente.
- **Quitar las opciones de inicio de sesión Apagar y Apagar equipo**. Esta opción quita la posibilidad de desactivar el equipo desde el menú Inicio y la pantalla de bienvenida de Windows.
- **Impedir que los documentos de Microsoft Office se abran dentro de Internet Explorer**. Esta opción garantiza que las aplicaciones de Office alberguen sus propios documentos para que la restricción de software de Microsoft Office funcione correctamente.
- **Usar la Pantalla de bienvenida para simplificar el proceso de inicio de sesión para los usuarios**. Esta opción activa la pantalla de bienvenida de Windows, que muestra una lista de las cuentas de usuario disponibles en el equipo al iniciarse Windows.
- **Quitar al <*administrador del Toolkit*> de la Pantalla de bienvenida**. Esta opción evita que la cuenta de administrador del Toolkit (la que se utiliza para instalarlo y administrarlo) se muestre en la pantalla de bienvenida. Puede presionar CTRL+ALT+SUPR dos veces para tener acceso al cuadro de diálogo de inicio de sesión tradicional, donde puede escribir directamente el nombre de usuario y la contraseña para iniciar sesión con cualquier cuenta de usuario no mostrada en la pantalla de bienvenida.

Importante

Presione CTRL+ALT+SUPR dos veces para obtener acceso al cuadro de diálogo de inicio de sesión tradicional. Ello le permitirá iniciar sesión en las cuentas no mostradas en la pantalla de bienvenida.

- **Paso 3. Crear una cuenta pública para el acceso compartido**. En esta sección se ofrece orientación para crear una cuenta de usuario local limitada que se utilizará para el acceso compartido al equipo. En muchos equipos compartidos, existe una sola cuenta de usuario que comparten todos los que utilizan el equipo. En esta sección, se ofrece un método de acceso directo a la herramienta Cuentas de usuarios con la que se crea la cuenta.

- **Paso 4. Configurar el perfil de usuario público**. En esta sección se ofrece orientación para iniciar sesión con la nueva cuenta pública y establecer la configuración de Windows, las impresoras y los programas de la cuenta.Una vez configurado el perfil de usuario público, es necesario cerrar la sesión y volver a iniciarla como administrador del Toolkit para seguir con la herramienta Introducción.
- **Paso 5. Restringir y bloquear el perfil de usuario público**. Esta sección proporciona acceso directo a la herramienta Restricciones del usuario y orientación para utilizar la herramienta a fin de bloquear y restringir el perfil de usuario público.
- **Paso 6. Probar el perfil de usuario público**. En esta sección se ofrece orientación para iniciar sesión en el perfil de usuario público y poder probar la eficacia de la configuración y las restricciones de la cuenta. Una vez probado el perfil de usuario público, es necesario cerrar la sesión y volver a iniciarla como administrador del Toolkit para seguir con la herramienta Introducción.
- **Paso 7. Activar Protección de discos de Windows**. Esta sección proporciona acceso directo a la herramienta Protección de discos de Windows, junto con orientación para activar dicha herramienta y configurarla para descargar e instalar actualizaciones críticas.
- **Paso 8. ¡Listo! Obtenga ahora más información acerca del Toolkit**. En esta sección se ofrecen vínculos al Manual de Shared Computer Toolkit y la Ayuda de Shared Computer Toolkit.

Desinstalar el Toolkit

Puede desinstalar el Toolkit en cualquier momento mediante la característica Agregar o quitar programas del Panel de control. No obstante, determinadas características del Toolkit no estarán disponibles una vez desinstalado el Toolkit, como todos los aspectos de Protección de discos de Windows.

Si la herramienta Protección de discos de Windows está activada, el proceso de desinstalación guardará los cambios en el disco y reiniciará el equipo; éste es el comportamiento esperado.

Antes de desinstalar el Toolkit, desactive las siguientes características específicas en todos los perfiles de usuario que las utilicen:

- **Temporizadores de la sesión**. Debe desactivar los temporizadores para el cierre de sesión obligatorio y el cierre de sesión por inactividad (asegúrese de que cada una de las entradas está en blanco) en la sección Configuración general de la herramienta Restricciones del usuario.
- **Reiniciar al cerrar sesión**. Desactive la casilla de verificación de esta opción en la sección Configuración general de la herramienta Restricciones del usuario.
- **AutoRestart.** Deshabilite esta herramienta de línea de comandos, si la ha utilizado para reiniciar automáticamente un programa específico.

Las características siguientes seguirán disponibles una vez desinstalado el Toolkit:

- **Restricciones recomendadas para cuentas compartidas**. Las restricciones seleccionadas en la sección Restricciones recomendadas para cuentas compartidas de la herramienta Restricciones del usuario siguen en vigor.

- **Restricciones opcionales**. Las restricciones seleccionadas en la sección Restricciones opcionales de la herramienta Restricciones del usuario siguen en vigor.
- **Perfiles bloqueados**. Los perfiles bloqueados con la herramienta Restricciones del usuario permanecerán bloqueados.
- **Configuración de AutoLogon**. Cualquier cuenta configurada para iniciar sesión automáticamente con la herramienta de línea de comandos AutoLogon seguirá en vigor.
- **Introducción**. Las opciones de seguridad de equipo seleccionadas en la herramienta Introducción seguirán funcionando.
- **Welcome**. La configuración especificada con la herramienta de línea de comandos Welcome seguirá funcionando.

Para desinstalar el Toolkit y devolver la mayoría de las opciones a su configuración original:

1. Utilice el paso 2 de la herramienta Introducción para quitar las opciones de seguridad aplicadas después de la instalación.
2. Utilice la herramienta Restricciones del usuario para desbloquear y quitar restricciones de todos los perfiles de usuario.
3. Utilice la herramienta Administrador de perfiles para eliminar los perfiles de usuario que no piense conservar. De este modo, quitará todos los documentos y carpetas almacenados para el perfil de usuario afectado.
4. Elimine las cuentas de usuario que no piense utilizar.
5. Si ha utilizado las herramientas de línea de comandos de Shared Computer Toolkit para realizar cambios de configuración en el sistema, use dichas herramientas para deshacer los cambios que desee.
6. Haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Desinstalar Shared Computer Toolkit**.

La desinstalación quitará Protección de discos de Windows y Shared Computer Toolkit. Puede seguir utilizando el sistema con el resto de cuentas y perfiles de usuario de Windows.

Conservar los documentos del usuario

Si desea conservar los documentos del usuario al eliminar un perfil o las carpetas de éste (como se describe en la sección anterior), puede copiarlos en una ubicación segura o utilizar el Asistente para transferencia de archivos y configuraciones para almacenar los documentos hasta que se establezca la nueva carpeta de perfiles.

Para abrir el Asistente para transferencia de archivos y configuraciones, haga clic en **Inicio**, seleccione **Accesorios**, **Herramientas del sistema** y, a continuación, **Asistente para transferencia de archivos y configuraciones**.

Capítulo 2: Preparar el disco para Protección de discos de Windows

Nota
Si le resulta difícil entender los términos de este capítulo, consulte la sección "Discos y particiones" del Apéndice A, "Conceptos técnicos elementales".

La herramienta Protección de discos de Windows protege el sistema operativo Microsoft® Windows® XP y los archivos de programa contra los cambios permanentes que se realicen en la *partición de Windows* (normalmente la unidadC:). Si la herramienta Protección de discos de Windows está activada, los usuarios pueden trabajar con normalidad y el funcionamiento de Windows es el habitual. Sin embargo, los cambios realizados en el disco no se llevan a cabo realmente en la partición de Windows, sino que se almacenan temporalmente en otra ubicación.

Al reiniciar el equipo, Protección de discos de Windows devuelve la partición de Windows a su estado original y borra los cambios realizados desde el último reinicio. Se trata de una característica de seguridad muy útil para los equipos compartidos.

La herramienta Protección de discos de Windows requiere una preparación especial del disco duro del equipo que se explica en los siguientes temas:

- Requisitos de Protección de discos de Windows
- Cambiar el tamaño de una partición existente

O bien

- Tamaño del disco durante la instalación de Windows XP

Requisitos de Protección de discos de Windows

Nota
Una alternativa a aumentar el tamaño de la partición de protección para grabar CD y DVD es configurar el software de grabación de discos para colocar sus archivos temporales en la partición de Windows.

La herramienta Protección de discos de Windows requiere un mínimo de 1 GB de espacio de disco sin asignar. Este espacio de disco no asignado se convertirá en la *partición de protección*, cuya función es almacenar temporalmente los cambios del disco cuando está activada la herramienta Protección de discos de Windows. Algunas operaciones, como la grabación de CD y DVD, necesitan grandes cantidades de espacio de disco (el doble de tamaño del proyecto que se escribe en el disco). Tenga esto en cuenta y asegúrese de que hay suficiente espacio no asignado en el disco cuando configure los equipos que se van a dedicar a estas funciones.

Para activar la herramienta Protección de discos de Windows, debe cumplir los siguientes requisitos:

Nota
También puede crear la partición de protección en el espacio libre de una partición extendida, o bien puede utilizar el espacio no asignados de un segundo disco físico. Para obtener más información acerca de estas técnicas, consulte la sección “Administrar la partición de protección” al final de este capítulo.

- Asegúrese de que al menos 1 GB o aproximadamente un 10% de la *partición de Windows* (el mayor de los dos valores) está disponible como espacio de disco no asignado.
- El espacio de disco no asignado debe ser *posterior* a una partición primaria, no puede figurar al principio del disco.
- El disco que contiene espacio no asignado no puede tener más de tres particiones primarias.
- La partición de Windows debe ser un disco básico. La herramienta Protección de discos de Windows no admite discos dinámicos.

Puede usar la utilidad Administración de discos para ver las particiones actuales del disco duro.

Para usar la utilidad Administración de discos de Windows XP a fin de ver las particiones actuales:

1. Inicie sesión como administrador del Toolkit.
2. Si la herramienta Introducción no se abre automáticamente, haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Introducción**.
3. En el paso 1 de la herramienta Introducción, haga clic en el vínculo **Abrir Administración de discos** al final del tema. También se incluye un acceso directo a la Administración de discos en la sección **Acceso rápido**, cerca de la parte superior de la ventana Introducción.

Otro método es hacer clic con el botón secundario en **Mi PC** y, a continuación, seleccionar Administración de discos.

Nota

Si deja una cantidad de espacio no asignado equivalente al tamaño de la partición de Windows, la herramienta Protección de discos de Windows no tendrá ninguna restricción de espacio en disco y podrá realizar un seguimiento de todos los cambios realizados en la partición de Windows.

Nota

La mayoría de los equipos compartidos no ofrecen a los usuarios ninguna forma de almacenar datos persistentes localmente, pero en algunos entornos puede resultar conveniente ofrecer esta posibilidad. En el capítulo 9, “Escenarios avanzados”, se describen distintas alternativas para almacenar datos de usuario persistentes cuando la herramienta Protección de discos de Windows está activada.

En la ilustración siguiente, se muestra la utilidad Administración de discos de un equipo con un único disco duro de 40 GB. En el disco duro, hay una partición de Windows de 36 GB (la unidad C:) y 4 GB de espacio de disco no asignado para Protección de discos de Windows.

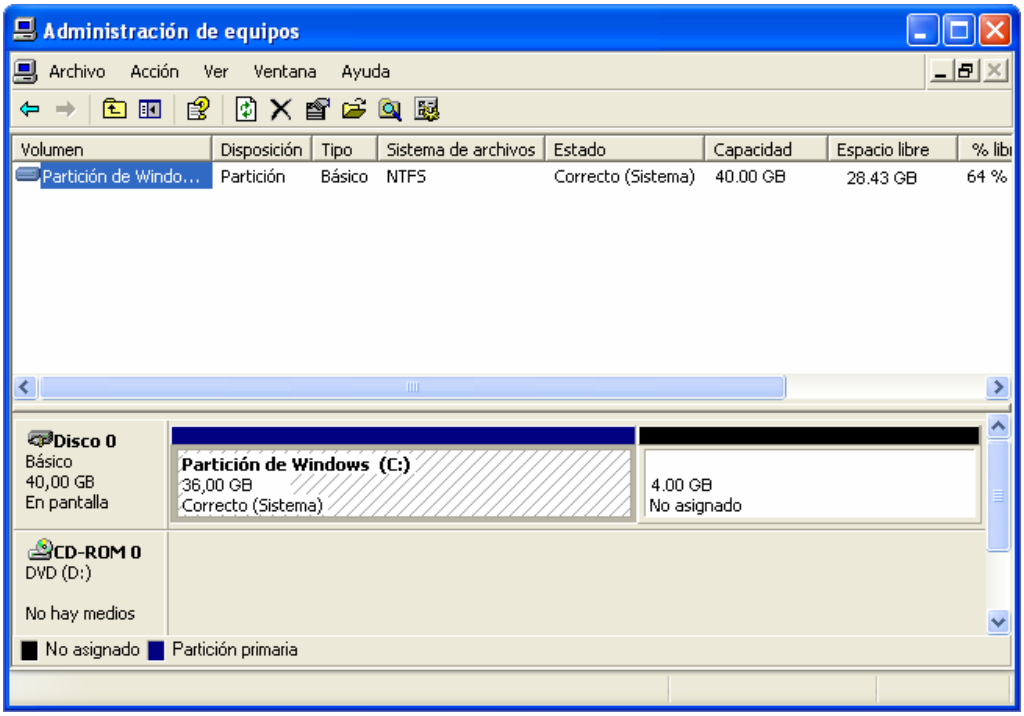

Figura 2.1 El espacio de disco no asignado debería ser 1 GB o aproximadamente un 10% del tamaño de la partición de Windows (el mayor de los dos valores)

Nota
Algunas tareas, como la creación o copia de CD requieren una gran cantidad de espacio de disco temporalmente. Si el equipo se va a emplear para realizar estar tareas, asegúrese de que hay suficiente espacio en disco no asignado antes de crear la partición de protección para que pueda dar cabida al contenido completo de dos CD o DVD.

Para calcular el espacio de disco no asignado necesario:

Para determinar la cantidad necesaria de espacio no asignado, puede seguir uno de los siguientes procedimientos:

- **La partición de Windows ocupa todo el disco.** Divida el tamaño del disco en GB entre 10. Si el resultado es más de 1 GB, ése es el tamaño de espacio en disco no asignado necesario.
- **La partición de Windows ocupa una parte del disco.** Divida el tamaño de la partición de Windows entre 10. Si el resultado es más de 1 GB, ése es el tamaño de espacio en disco no asignado necesario.

Si la herramienta que utiliza para cambiar el tamaño de las particiones calcula el espacio en MB, multiplique las cifras calculadas por 1024 para convertir los gigabytes en megabytes.

La tabla siguiente, contiene varios ejemplos de configuración de disco duro:

Disco duro	Partición de la unidad C:	Espacio de disco no asignado (1 GB = 1024 MB)
30 GB	27 GB	3 GB (3072 MB)
7	72 GB	8 GB (8192 MB)
120 GB	108 GB	12 GB (12.288 MB)
250 GB	225 GB	25 GB (25.600 MB)

Cambiar el tamaño de una partición existente

Nota
Microsoft no ofrece soporte técnico para los productos de partición de discos de terceros. Para obtener asistencia acerca de cualquier problema relacionado con estos productos, póngase en contacto con su fabricante.

La mayoría de los equipos no se comercializan con espacio en disco no asignado. Lo normal es que el disco tenga una única partición, que suele ser la unidad C:. En esta sección, se ofrecen dos opciones para crear el espacio en disco sin asignar necesario para la herramienta Protección de discos de Windows.

Si el equipo ya tiene instalado Windows XP y no desea volver a instalar y configurar Windows y los demás programas, necesitará una utilidad de disco de terceros para cambiar el tamaño de la partición de Windows y dejar espacio de disco no asignado para Protección de discos de Windows.

En esta sección, se describe cómo utilizar Symantec Norton PartitionMagic 8.0 (http://go.microsoft.com/fwlink/?LinkId=47542; puede que la página esté en inglés) para crear el espacio en disco no asignado necesario para la herramienta Protección de discos de Windows.

También puede utilizar TeraByte Unlimited BootIt Next Generation (http://go.microsoft.com/fwlink/?LinkId=46756; puede que la página esté en inglés). Puede obtener instrucciones completas y descargar una copia de prueba en el sitio Web de TeraByte Unlimited (http://go.microsoft.com/fwlink/?LinkId=46756).

Nota
Inicie PartitionMagic 8.0 arrancando el equipo desde el CD del programa, no iniciando el programa desde Windows. Asimismo, es recomendable realizar una copia de seguridad completa antes de llevar a cabo este procedimiento.

Puede encontrar otras utilidades de partición de discos en el sitio Web Windows Marketplace (http://go.microsoft.com/fwlink/?LinkId=54604; puede que la página esté en inglés).

Para cambiar el tamaño de una partición usando PartitionMagic 8.0:

1. Inserte el CD de PartitionMagic en la unidad de CD-ROM del equipo.
2. Si el programa se inicia automáticamente, haga clic en **Salir**.

3. Haga clic en **Inicio**, en **Apagar equipo** y, después, haga clic en **Reiniciar**. Asegúrese de que el equipo se inicie desde el CD de PartitionMagic.
4. Una vez iniciado PartitionMagic, en el símbolo del sistema, escriba **1** para Norton PartitionMagic y, a continuación, seleccione el idioma que desee emplear.
5. En la ventana principal del programa (que se muestra en la ilustración siguiente), elija un disco duro haciendo clic en el menú desplegable de la barra de herramientas principal En el ejemplo de la ilustración siguiente, se muestra un disco duro de 40 GB con una única partición primaria.

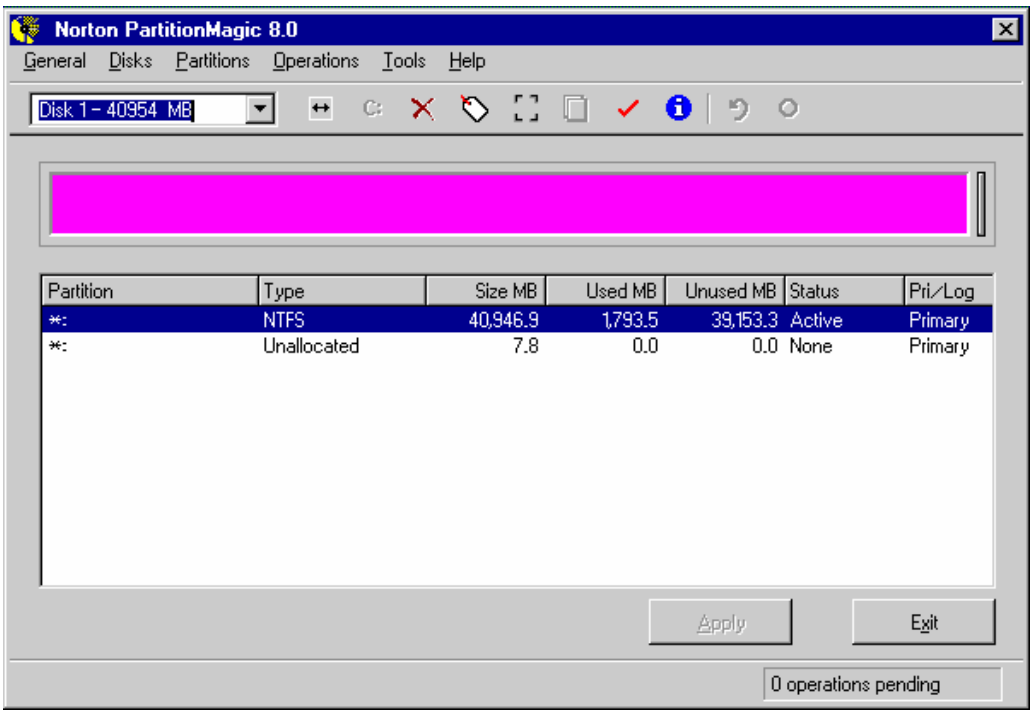

Figura 2.2 *Ventana principal de PartitionMagic 8.0*

Nota

Asegúrese de que deja suficiente espacio para Windows XP y todos los programas necesarios; se suele dejar como mínimo 10 GB para la partición de Windows. En este ejemplo, el tamaño de la partición de 40 GB se cambia a 36 GB.

6. Haga clic en la partición cuyo tamaño desee cambiar, haga clic en **Operations** y, a continuación, haga clic en **Resize/Move**.
7. En el cuadro de diálogo **Resize/Move Partition** (véase la ilustración siguiente), en el cuadro **Free Space After**, escriba la cantidad de espacio no asignado que se va a reservar. Use esta fórmula: Número de GB * 1024. En el ejemplo siguiente, 4096 (4*1024). No es necesario que sea una cantidad exacta, basta con que sea superior a 1024 (1 GB).

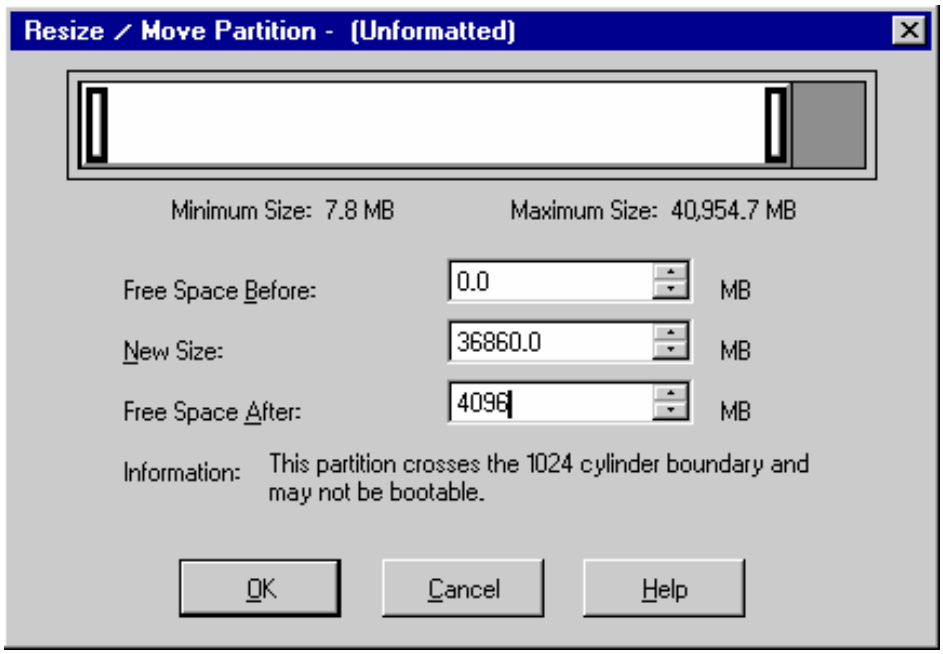

Figura 2.3 *Cambiar el tamaño de una partición en PartitionMagic 8.0*

Nota
En su interfaz de usuario, PartitionMagic 8.0 se refiere al espacio en disco no asignado como **Free Space After.**

8. Haga clic en **OK** y, a continuación, en **Apply** para cambiar el tamaño de la partición. Este proceso tardará unos minutos en completarse.
9. Una vez finalizado, haga clic en **Exit**, extraiga el CD, reinicie el equipo e inicie sesión en Windows como administrador del Toolkit.
10. Durante el minuto posterior al inicio de sesión en Windows, aparecerá el diálogo **Cambio de configuración del sistema** preguntándole si desea reiniciar el equipo. Haga clic en **No**.

El equipo está listo para activar la herramienta Protección de discos de Windows.

Una vez completados estos pasos, vaya al capítulo 3, “Administración de perfiles”.

Importante
La eliminación de particiones destruirá todos los datos de dicha partición. Use este método sólo si no necesita conservar ninguna información contenida en el equipo y está dispuesto a volver a instalar Windows y los demás programas y controladores.

Tamaño del disco durante la instalación de Windows XP

Si tiene intención de realizar una instalación limpia de Windows XP, la mejor forma de preparar el disco duro para la herramienta Protección de discos de Windows es crear una partición primaria del tamaño adecuado durante la configuración de Windows XP. Esta opción sólo es apropiada si está dispuesto a sobrescribir todos los programas, opciones de configuración y archivos que haya en el disco duro del equipo.

Una vez iniciada la instalación de Windows XP (que puede realizar arrancando el equipo con el CD de instalación de Windows XP en la unidad de CD-ROM), y después de aceptar el contrato de licencia de Microsoft Windows XP, aparecerá la siguiente página en pantalla:

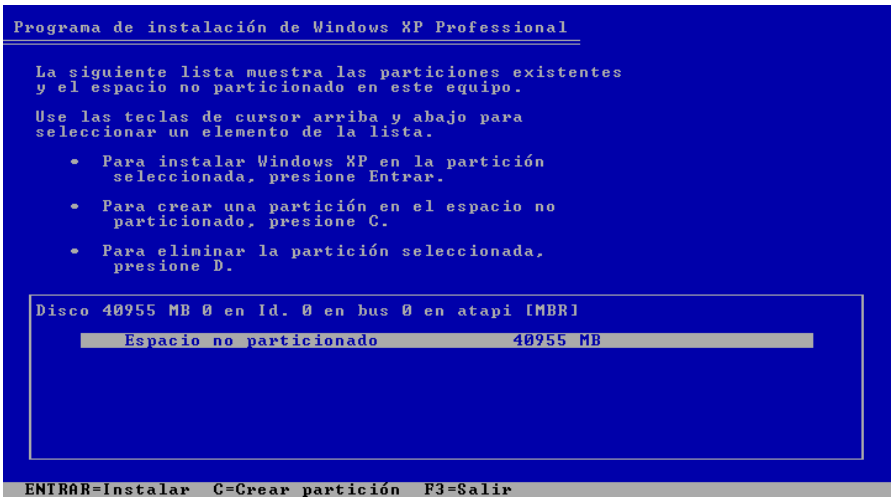

Figura 2.4 *Configurar particiones durante la instalación de Windows XP*

Para establecer el tamaño de una partición durante la instalación de Windows XP:

1. En el ejemplo de la ilustración anterior, hay un único disco duro con 40 GB (40.955 MB) de espacio no asignado. Para crear una partición, presione **C** para que se muestre la página que aparece en la ilustración siguiente. En esta página, se muestra el tamaño mínimo y máximo que se puede asignar a una nueva partición.
2. Escriba el tamaño apropiado para la partición que desea crear en MB y, a continuación, presione ENTRAR. Por ejemplo, para crear una partición de 36 GB, debe escribir 36864 (36 * 1024). La herramienta Protección de discos de Windows utilizará el espacio no asignado restante.
3. Utilice las teclas de flecha para seleccionar la partición en la que desea instalar Windows (si no está ya seleccionada) y presione ENTRAR.
4. Use las teclas de flecha para seleccionar la opción **Formatear la partición utilizando el sistema de archivos NTFS (rápido)** y, a continuación, presione ENTRAR.
5. El programa de instalación de Windows XP copiará los archivos necesarios y reiniciará el equipo. Continúe con la instalación de Windows.

Importante

Cree la partición C: sólo durante la instalación de Windows. Puede crear una partición persistente opcional mediante la herramienta Administración de discos una vez terminada la instalación de Windows. Este procedimiento se trata en el capítulo 9, "Escenarios avanzados".

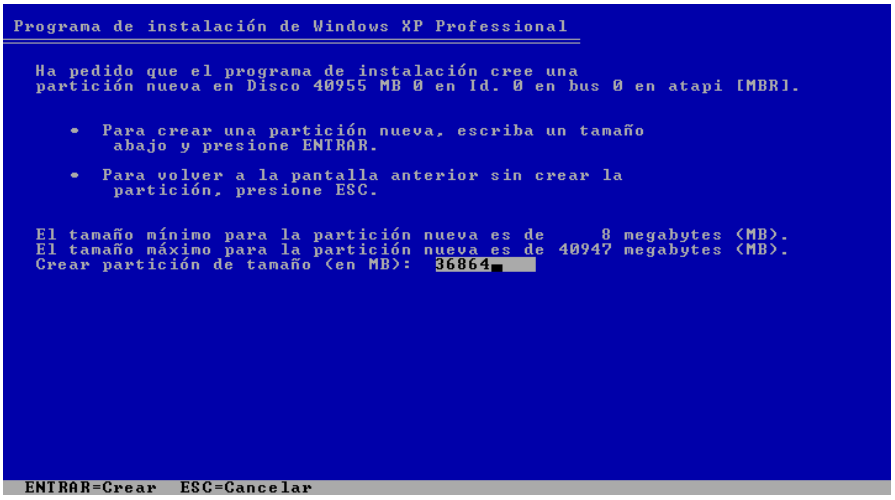

Figura 2.5 *Crear una nueva partición durante la instalación de Windows XP*

Capítulo 3: Administración de perfiles

Una vez preparado el equipo e instalado Microsoft® Shared Computer Toolkit para Windows® XP, debe atender las necesidades de los usuarios. Para ello, es necesario crear cuentas de usuario y personalizar cada uno de sus perfiles.

En este capítulo, aprenderá a realizar las siguientes tareas:

- Crear cuentas de usuario locales limitadas
- Configurar perfiles de usuario locales
- Actividad opcional: personalizar el menú Inicio de Todos los usuarios
- Actividad opcional: personalizar el menú Inicio de un usuario

perfil de usuario
Conjunto de carpetas, archivos y opciones de configuración que definen el entorno del usuario.

Un *perfil de usuario* es un conjunto de carpetas, archivos y opciones de configuración que define el entorno de un usuario que inicia sesión con una cuenta de usuario determinada; cada una de estas cuentas tiene un perfil asociado. Normalmente, un perfil de usuario no se crea hasta que el usuario inicia sesión por primera vez en el equipo con una nueva cuenta de usuario. Si se produce este inicio de sesión, Windows creará automáticamente un nuevo perfil de usuario para esa cuenta.

Crear cuentas de usuario locales limitadas

Nota
Las cuentas de usuario locales se utilizan en equipos independientes o que forman parte de un grupo de trabajo. Si el equipo forma parte de un domino de Active Directory, consulte el capítulo 10, “Shared Computer Toolkit en entornos de domino”, para obtener más información.

El primer paso es crear cuentas para los usuarios del equipo. Según el entorno de que se trate, podrá crear:

- **Una cuenta individual para cada usuario**. Esta solución puede resultar útil si hay relativamente pocos usuarios, se dispone de un único equipo y cada usuario tiene necesidades distintas. Si hay muchos usuarios y equipos, las creación de cuentas individuales resulta un método poco ágil. Considere la posibilidad de usar el servicio de directorio Active Directory®.
- **Una única cuenta para que la utilicen todos los usuarios**. Es lo que se denomina una cuenta compartida.
- **Unas cuantas categorías de cuentas para que las utilicen todos los usuarios**. Por ejemplo, en un entorno de biblioteca, podría crear una cuenta para los niños y otra para los adultos.

La estructura de las cuentas depende de la situación, pero normalmente cuantas menos cuentas haya, menor será el esfuerzo de administración necesario.

Si tiene intención de seguir un planteamiento de clonación o creación de imágenes en el entorno, puede crear una selección completa de distintas cuentas de usuario en el equipo de referencia. A continuación, después de clonar el equipo original varias veces, deshabilite las cuentas que no se utilicen en cada equipo clonado. Con ello, se reducirá el número de imágenes del equipo original que debe administrar. Para obtener más información sobre la clonación, consulte el capítulo 9, “Escenarios avanzados”.

Nota
Windows XP Professional también admite grupos en los que se pueden conceder varios permisos y derechos, lo que proporciona una configuración mucho más flexible de las cuentas de usuario. No obstante, a los usuarios de un equipo compartido sólo se les debe conceder acceso a cuentas de usuario limitadas siempre que sea posible.

Windows XP admite dos tipos primarios de cuentas de usuario locales:

- **Administrador del equipo**. La cuenta de administrador del equipo tiene los derechos necesarios para instalar y desinstalar software y controladores de dispositivos, cambiar las opciones de configuración de Windows, crear y eliminar usuarios, y cambiar la configuración de seguridad. Para administrar las opciones de Windows y del Toolkit, se necesita una cuenta administrativa.
- **Limitada**. Las cuentas limitadas no tienen derecho a realizar ninguna de las acciones de las cuentas de administrador enumeradas anteriormente de manera predeterminada. De forma predeterminada, las cuentas de usuario limitadas pueden ejecutar programas, obtener acceso a Internet y a redes locales, cambiar la configuración del escritorio, crear archivos y carpetas, y realizar otras actividades diarias.

Al crear las cuentas, debe crear cuentas de usuario limitadas. A continuación, utilice la herramienta Restricciones del usuario del Toolkit para restringir aún más las actividades de esos usuarios.

Para crear una nueva cuenta de usuario limitada en un equipo de grupo de trabajo:

1. Inicie sesión como administrador del Toolkit.
2. Si la herramienta Introducción no se abre automáticamente, haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Introducción**.
3. En el paso 3 de la herramienta Introducción, haga clic en el vínculo **Abrir Cuentas de usuario** al final del tema. También se incluye un acceso directo a las Cuentas de usuario en la sección **Acceso rápido**, cerca de la parte superior de la ventana Introducción.
4. En la ventana **Cuentas de usuario**, haga clic en **Crear una nueva cuenta**.
5. En la página **Dé un nombre a la cuenta nueva**, escriba el nombre de la nueva cuenta de usuario y, a continuación, haga clic en **Siguiente**.
6. En la página **Elija un tipo de cuenta**, haga clic en **Limitada** y, a continuación, haga clic en **Crear cuenta**.

Proporcionar acceso a las cuentas administrativas a los usuarios plantea una serie de problemas de seguridad. No obstante, puede que en algunas ocasiones los usuarios deseen ejecutar programas que requieren una cuenta administrativa para un funcionamiento correcto. Hay muchos juegos que entran en esta categoría. En estos casos, puede ser necesario crear cuentas de administrador para algunos usuarios y después restringirlas para limitar su acceso a herramientas de configuración potencialmente peligrosas. Puede obtener más información acerca de esta opción en la sección "Restringir una cuenta administrativa compartida" del capítulo 9, "Escenarios avanzados".

Configurar perfiles de usuario locales

Una vez creadas las cuentas de usuario locales, el paso siguiente es crear y configurar los perfiles de usuario de dichas cuentas. Para completar este proceso, se inicia sesión con las cuentas de usuario que ha creado, se ejecutan los programas por primera vez y se configuran las opciones de Windows. Al ejecutar los programas por primera vez en nombre de los usuarios, podrá aceptar los contratos de licencia y configurar las opciones que, de otro modo, los usuarios tendrían que volver a configurar cada vez que los utilizaran.

Nota
Puede usar la herramienta Administrador de perfiles para crear perfiles de usuario. De todos modos, debe realizar la primera configuración de cada perfil.

Para obtener más información acerca de los perfiles de usuario, consulte el apéndice A, "Conceptos técnicos elementales".

Para configurar un perfil de usuario local:

1. Inicie sesión usando una de las cuentas de usuario locales que acaba de crear. Si inicia sesión en una cuenta por primera vez, Windows creará automáticamente un nuevo perfil de usuario.
2. Lleve a cabo las tareas de primera configuración en programas como Microsoft Office. Configure los siguientes programas:
   - Microsoft Office
   - MSN Messenger
   - MSN Games Loader
   - Macromedia Flash
   - Adobe Reader
   - Otros programas o utilidades necesarios en el equipo compartido.
3. Configure las demás opciones importantes:
   - Instale y configure las impresoras que necesitará el usuario.
   - Instale la configuración de software y los controladores de dispositivo que pueda necesitar el usuario.
   - Configure las opciones de escritorio como el papel tapiz y el protector de pantalla.
   - Elimine los accesos directos de Windows Explorer del menú Inicio. En lugar de éstos, utilice los accesos directos de Mi PC.
4. Si el equipo utiliza un software de bloqueo de secuencias de comandos, ejecute todas las secuencias de comandos del Toolkit (enumeradas en la tabla siguiente) que se podrían ejecutar en un perfil de usuario restringido. Cuando el programa le pregunte si desea permitir o bloquear la secuencia de comandos, permítala permanentemente para evitar que se le vuelva a hacer la pregunta al usuario.

Nota
El temporizador de cierre de sesión inactiva de la herramienta Restricciones del usuario utiliza la configuración del protector de pantalla. Si tiene intención de configurar un temporizador de cierre de sesión inactiva para un usuario más adelante, no configure su protector de pantalla ahora.

Nota
Algunos programas de bloqueo no permiten la aprobación permanente de secuencias de comandos. Si no puede aprobar permanentemente las secuencias de comandos del Toolkit, desactive el bloqueo.

Archivo de secuencia de comandos	Ruta de acceso
Accessibility.wsf.	%ProgramFiles%\Microsoft Shared Computer Toolkit\
Accessibility.wsf	%ProgramFiles%\Microsoft Shared Computer Toolkit\scripts
AutoRestart.wsf.	%ProgramFiles%\Microsoft Shared Computer Toolkit\scripts
SCTLogoff.vbs	%ProgramFiles%\Microsoft Shared Computer Toolkit\scripts
Toast.hta	%ProgramFiles%\Microsoft Shared Computer Toolkit\scripts
Toast.vbs	%ProgramFiles%\Microsoft Shared Computer Toolkit\scripts

Además de las advertencias de bloqueo de secuencias de comandos, existen otros tipos de advertencias de software de seguridad o de aprobaciones que puede requerir el entorno. Si se producen estas advertencias, lleve a cabo los siguientes cambios antes de bloquear el perfil:

5. **Advertencia de cambio de la página principal de Internet Explorer**. Establezca la página principal de Internet Explorer desde el perfil (no desde la herramienta Restricciones del usuario) antes de bloquearlo.
6. **Advertencia de adición de claves de registro Run**.Las restricciones de usuario (en concreto el temporizador de cierre de sesión inactiva obligatorio) y la herramienta AutoRestart agregan claves de tipo **Run** al registro del usuario. Los programas de bloqueo de secuencias de comandos pueden advertir al usuario de la presencia de estas aplicaciones. Realice estos cambios y autorícelos iniciando sesión como usuario y respondiendo a las preguntas de bloqueo de secuencias de comandos antes de bloquear el perfil.
7. Repita los pasos 1 a 6 para cada cuenta de usuario local.

Actividad opcional: personalizar el menú Inicio de Todos los usuarios

Importante
Los cambios que se realicen en el menú Inicio de Todos los usuarios afectan a todos los usuarios del equipo. La mayoría de los programas instalan los accesos directos del menú Inicio en el perfil Todos los usuarios.

De manera predeterminada, la herramienta Restricciones del usuario habilita el menú Inicio clásico de Windows (parecido al de las versiones anteriores del sistema operativo). Con el menú Inicio clásico es más fácil personalizar los programas que aparecen en el menú Inicio de un perfil de usuario.

No es necesario activar el menú Inicio clásico manualmente, pero puede organizar los iconos del menú Inicio en ese momento para que aparezcan en la ubicación correcta después de ejecutar la herramienta Restricciones del usuario.

Windows XP crea el menú Inicio de un usuario basándose en los accesos directos de los programas que se almacenan de manera predeterminada en dos ubicaciones:

- **La carpeta \Documents and Settings\All Users\Menú Inicio**. Esta carpeta contiene los accesos directos de programas incluidos en el menú Inicio para todas las cuentas de usuario.
- **La carpeta \Documents and Settings*nombreDeUsuario*\Menú Inicio**. Esta carpeta contiene accesos directos de programas específicos de un perfil de usuario concreto.

Windows analiza el contenido de estas dos carpetas cuando genera los accesos directos de programa que aparecen en el menú Inicio. Para personalizar (y proteger) los menús Inicio de los usuarios, primero debe asegurarse de que la carpeta All Users\Menú Inicio contiene sólo los accesos directos de programa a los que desea que tengan acceso todos los usuarios. Más adelante, en esta sección, personalizará el menú Inicio para un perfil de usuario individual.

Algunos operadores de equipos compartidos prefieren asegurarse de que la carpeta All Users\Menú Inicio no contenga ningún programa y de que el menú Inicio de cada perfil incluya los accesos directos correspondientes. No obstante, tenga en cuenta que si quita un acceso directo del menú Inicio, no por ello el programa correspondiente dejará de estar disponible. Por ejemplo, los usuarios siguen teniendo la posibilidad de hacer doble

clic en un archivo .doc para abrir Microsoft Word, incluso si no hay ningún acceso directo para Word disponible en el menú Inicio.

Para personalizar los programas que aparecen en el menú Inicio de Todos los usuarios:

1. Inicie sesión con una cuenta de administrador.
2. Haga clic con el botón secundario en **Inicio** y, a continuación, haga clic en **Explorar todos los usuarios**. Los accesos directos ubicados en la carpeta Menú Inicio aparecen directamente en el menú Inicio. Los accesos directos de la carpeta Programas aparecen en el submenú Programas del Menú Inicio.
3. Use el Explorador de Windows para arrastrar accesos directos a la carpeta Menú Inicio y que aparezcan directamente en el Menú Inicio de todos los usuarios.
4. Arrastre los otros accesos directos hasta las carpetas de Todos los usuarios, o desde éstas, según sea necesario.

Importante
Cuando personalice el menú Inicio de Todos los usuarios, elimine el acceso a utilidades a las que no deben tener acceso los usuarios, como anvitirus, antispyware, Microsoft Update y las utilidades de discos.

Quite los siguientes iconos del menú Inicio de Todos los usuarios para que no estén disponibles en las cuentas compartidas que cree:

- Configurar acceso y programas predeterminados
- Catálogo de Windows
- Windows Update y Microsoft Update
- Símbolo del sistema
- Carpeta Herramientas del sistema

Actividad opcional: personalizar el menú Inicio de un usuario

Nota
Si desea restringir el acceso a la unidad C:, sustituya los accesos directos del Explorador de Windows por los de Mi PC en el menú Inicio del usuario para evitar mensajes de error. De manera predeterminada, el Explorador de Windows intenta mostrar carpetas de perfiles ubicadas en la unidad C:.

Al igual que resulta posible configurar los accesos directos que aparecen en el menú Inicio de Todos los usuarios, también se pueden configurar los que aparecen en el menú Inicio de un perfil de usuario individual.

Para personalizar los programas que aparecen en el menú Inicio de un usuario individual:

1. Inicie sesión con una cuenta de administrador.
2. Haga clic con el botón secundario en **Inicio** y, después, haga clic en **Explorar**.
3. En la carpeta Documents and Settings, verá una subcarpeta por cada perfil de usuario que haya en el equipo compartido. Si no ve las carpetas de las cuentas de usuario, es porque probablemente aún no ha creado los perfiles. A tal efecto, inicie sesión como usuario en el equipo siguiendo el procedimiento descrito en la sección "Configurar perfiles de usuario locales" de este capítulo.
4. Use el Explorador de Windows para copiar los accesos directos en las carpetas Menú Inicio de los usuarios y que aparezcan directamente en el Menú Inicio de cada uno de ellos.
5. Arrastre los demás accesos directos hasta las carpetas de cada usuario, o bien desde éstas, según sea necesario.

Capítulo 4: Restricciones del usuario

La herramienta Restricciones del usuario permite restringir las acciones del usuario. De manera predeterminada, los usuarios que tienen cuentas limitadas no pueden instalar software ni hardware, pero pueden ejecutar los programas que se descarguen o que traigan consigo almacenados en una unidad USB, lo cual puede causar problemas en el equipo. Con la herramienta Restricciones del usuario, puede definir restricciones para Microsoft® Internet Explorer, Microsoft Office, el sistema operativo Microsoft Windows® XP y el menú Inicio, así como especificar el software que se puede ejecutar.

Nota
Debe asegurarse de que la sesión de la cuenta de usuario que se va a restringir está cerrada antes de aplicar las restricciones. No se puede utilizar el cambio rápido de usuario para desplazarse entre la cuenta del administrador del Toolkit y la cuenta restringida.

En este capítulo se tratan los siguientes temas:

- Restringir un perfil de usuario local
- Configuración general
- Bloquear un perfil
- Restricciones recomendadas para cuentas compartidas
- Restricciones opcionales

Restringir un perfil de usuario local

Puede usar la herramienta Restricciones del usuario para restringir y bloquear los perfiles de los usuarios e impedir que éstos alteren la configuración del equipo. En esta sección, se describe un escenario típico de restricción de usuarios.

Nota
El cuadro de diálogo **Seleccione el perfil que desea restringir** muestra todas las cuentas de usuario configuradas en el equipo compartido, incluso las que están deshabilitadas. Sólo podrá seleccionar cuentas para las que existan perfiles de usuario.

Para restringir un perfil de usuario local:

1. Inicie sesión como administrador del Toolkit.
2. Haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Restricciones del usuario**. Otra opción es hacer clic en el vínculo **Abrir Restricciones del usuario** en el paso 5 de la herramienta Introducción. También se incluye un acceso directo a las Cuentas de usuario en la sección **Acceso rápido**, cerca de la parte superior de la ventana Introducción.
3. Haga clic en **Seleccionar un perfil**.
4. En el cuadro de diálogo **Seleccione el perfil que desea restringir**, haga clic en el perfil de usuario que desee restringir.
5. Seleccione la casilla de verificación **Bloquear este perfil** para evitar que los usuarios puedan cambiar la configuración durante una sesión que hayan iniciado con la cuenta de usuario. Puede obtener más información sobre el bloqueo de perfiles en la sección “Bloquear un perfil” de este capítulo.
6. Seleccione la casilla de verificación **Restricciones recomendadas para cuentas compartidas**. Con ello, se habilitan las restricciones más importantes. Puede obtener una restricción completa de la configuración en la sección “Restricciones recomendadas para cuentas compartidas” de este capítulo.
7. En la sección **Configuración general**, escriba la página principal predeterminada, un servidor proxy (si es necesario) y las excepciones aplicables a dicho servidor.

Importante
Debe emplear todas las restricciones recomendadas para cuentas compartidas a fin de impedir que el usuario altere la configuración del equipo.Las restricciones individuales no son suficientes.

8. En la sección **Temporizadores de la sesión**, establezca los límites del número de minutos que el usuario puede usar el equipo o que éste puede permanecer inactivo antes de forzar el cierre de la sesión. También puede dejar estas opciones en blanco.
9. Haga clic en **Seleccionar unidades** y, a continuación, restrinja todas las letras de unidades a las que el usuario no debe tener acceso. Microsoft recomienda restringir el acceso a la partición de Windows, donde se instalan el sistema operativo y los programas (suele ser la unidad C:).
10. Haga clic en **Aplicar** para aplicar las restricciones seleccionadas al perfil de usuario y seguir usando la herramienta Restricciones del usuario, o bien haga clic en **Aceptar** para aplicar las restricciones seleccionadas al perfil de usuario y cerrar la herramienta.

Nota

Si desea restringir el acceso a la unidad C:, sustituya los accesos directos del Explorador de Windows por los de Mi PC en el menú Inicio del usuario para evitar mensajes de error. De manera predeterminada, el Explorador de Windows intenta mostrar carpetas de perfiles ubicadas en la unidad C:.

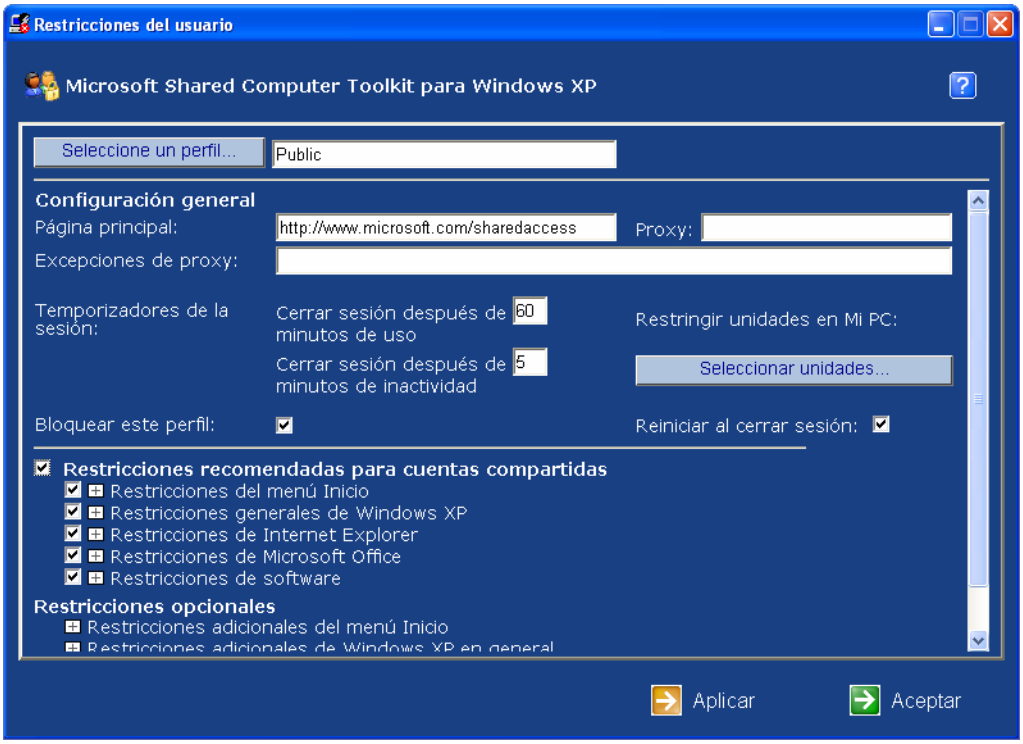

Figura 4.1 *Pantalla principal de la herramienta Restricciones del usuario*

Nota

En algunos entornos, se permite que los clientes usen cuentas administrativas. No es una práctica recomendada, pero se puede mejorar. Para obtener más información acerca de este tema, consulte la sección "Restringir una cuenta administrativa compartida" del capítulo 9, “Escenarios avanzados”.

Configuración general

Importante

El nombre de las carpetas de perfil de usuario bloqueado se cambia de \Documents and Settings*nombreDeUsuario* a \Documents and Settings*nombreDeUsuario*.Orig. Use esta nueva carpeta para ubicar los iconos del menú Inicio después de bloquear el perfil de usuario.

Para empezar, haga clic en **Seleccionar un perfil** y, a continuación, en el cuadro de diálogo **Seleccione el perfil que desea restringir**, haga clic en el perfil de usuario que desee restringir.

En la sección **Configuración general** de la herramienta Restricciones del usuario, puede definir las siguientes opciones:

- **Página principal**. Esta opción configura Internet Explorer para que use una página principal determinada.
- **Proxy**. Puede especificar la dirección de un servidor proxy, es decir, un servidor que proporciona acceso a Internet (y a menudo servicios de filtrado de contenido) al equipo.

- **Excepciones de proxy**. Puede especificar sitios o dominios que no utilicen el servidor proxy configurado. Utilice esta opción para permitir que se puedan visitar determinados sitios, incluso cuando las restricciones no permitan acceso general a Internet. Este tema se trata más detalladamente en la sección “Usar el filtrado de sitios simple para controlar el acceso a Internet” del capítulo 9, "Escenarios avanzados".
- **Temporizadores de la sesión**. Puede configurar restricciones para aplicarlas al usuario en dos momentos:
  - **Cerrar sesión después de __ minutos de uso.** Esta opción especifica el tiempo que los usuarios pueden utilizar el equipo antes de que se cierre su sesión automáticamente tras recibir una advertencia emergente.
  - **Cerrar sesión después de __ minutos de inactividad**. Esta opción especifica el tiempo que los usuarios pueden permanecer inactivos antes de que se cierre su sesión automáticamente tras recibir una advertencia de 15 segundos.
- **Restringir unidades en Mi PC**. Al hacer clic en el botón **Seleccionar unidades**, se abre un cuadro de diálogo en el que se pueden especificar una o más unidades a las que el usuario no puede tener acceso.
- **Bloquear este perfil**. Esta opción impide que los usuarios realice cambios permanentes en el perfil de usuario cuando han iniciado sesión.
- **Reiniciar al cerrar sesión**. Esta opción fuerza el reinicio de Windows cuando un usuario cierra una sesión del perfil seleccionado. Debe utilizarse junto con la herramienta Protección de discos Windows.

Bloquear un perfil

La opción **Bloquear este perfil** impide que se puedan realizar cambios permanentes en un perfil de usuario durante la sesión. Es muy útil para los perfiles de usuario que comparten varias personas. Si selecciona esta casilla de verificación, el cambio no tendrá efecto hasta que haga clic en **Aceptar** o **Aplicar**.

Si un perfil está bloqueado, los archivos que generalmente almacena Windows de forma automática para el usuario (normalmente en la carpeta Documents and Settings*nombreDeUsuario*) no estarán disponibles cuando el siguiente usuario inicie sesión. Los perfiles de usuario mejoran la privacidad de los usuarios y facilitan el mantenimiento de un escritorio limpio y estandarizado a los operadores de equipos compartidos.

Si se bloquea el perfil, no se conservan lo siguientes elementos entre sesiones:

- Cookies e historial de Internet
- Favoritos
- Archivos almacenados en el escritorio
- Papel tapiz del escritorio
- Cambios en la configuración de los programas
- Cambios de accesibilidad
- Cambios del menú Inicio

Importante

La eliminación de las restricciones recomendadas puede tener efectos adversos y no deseados, y sólo debe llevarse a cabo realizando previamente pruebas exhaustivas para asegurarse de que no supone un riesgo considerable para el entorno.

Restricciones recomendadas para cuentas compartidas

Puesto que la mayoría de estas restricciones operan de un modo coordinado para proporcionar un entorno más seguro para las cuentas compartidas, es mejor habilitar todas las restricciones recomendadas a la vez. Por ejemplo, Windows XP Home Edition permite a los usuarios cambiar las contraseñas si tienen acceso al Panel de control. Esto significa que debe usar la restricciones **Impedir cambios de contraseña** y **Quitar el icono Panel de control** para restringir eficazmente los cambios de contraseña. Asimismo, las restricciones de software constituyen una importante medida de seguridad que impide que los usuarios ejecuten programas no autorizados que puedan utilizarse para evitar otras restricciones.

Restricciones del menú Inicio

En la herramienta Restricciones del usuario, haga clic en el encabezado **Restricciones del menú Inicio** para expandir la lista completa de restricciones que puede configurar para el menú Inicio. En la lista siguiente, se describen las restricciones del menú Inicio:

- **Impedir hacer clic con el botón secundario en el menú Inicio**. Impide que el usuario obtenga acceso a menús contextuales al hacer clic con el botón secundario en elementos del menú Inicio.
- **Forzar el uso del menú Inicio clásico (recomendado para cuentas compartidas)**. El menú Inicio clásico simplifica la configuración de programas disponibles para un usuario en el menú Inicio.
- **Quitar la configuración del Panel de control, Impresoras y Redes del menú Inicio clásico**. Quita estos iconos del menú Inicio para ocultar las herramientas de configuración de los usuarios restringidos.
- **Quitar el icono Mis documentos**. Impide que los usuarios obtengan acceso a la carpeta Mis documentos con el icono del menú Inicio para aumentar la privacidad entre varios usuarios.
- **Quitar el icono Mis documentos recientes**. Impide que los usuarios obtengan acceso a los programas abiertos recientemente con el icono del menú Inicio. Ayuda a garantizar que los usuarios no puedan tener acceso a los programas a los que se les niega acceso y protege la privacidad de los usuarios anteriores.
- **Quitar el icono Mis imágenes**. Impide que los usuarios obtengan acceso a la carpeta Mis imágenes con el icono del menú Inicio.
- **Quitar el icono Mi música.** Evita que los usuarios obtengan acceso a la carpeta Mi música con el icono del menú Inicio.
- **Quitar el icono Favoritos**. Evita que los usuarios obtengan acceso a la carpeta Favoritos con el icono del menú Inicio. Ayuda a impedir el acceso no deseado a Internet.
- **Quitar el icono Mis sitios de red**. Impide a los usuarios obtener acceso a Mis sitios de red a través el icono del menú Inicio, evitando que puedan ver los accesos directos a otros equipos, impresoras y recursos de red que aparecen en Mis sitios de red.
- **Quitar el icono Panel de control**. Evita que los usuarios obtengan acceso a las herramientas del Panel de control con el icono del menú Inicio.
- **Quitar el icono Configurar acceso y programas predeterminados**. Quita el icono Configurar acceso y programas predeterminados.

Importante

Muchas de estas restricciones quitan el icono de una carpeta o programa del menú Inicio, pero en ningún caso impiden que se pueda obtener acceso a la carpeta o al programa. Por este motivo, es importante utilizar todas las restricciones recomendadas en la herramienta Restricciones del usuario para conseguir la mejor combinación de restricciones posible.

- **Quitar el icono Conectar a**. Impide que los usuarios se conecten a recursos de red con el icono del menú Inicio.
- **Quitar el icono Impresoras y faxes**. Evita que los usuarios obtengan acceso a la ventana Impresoras y faxes con el icono del menú Inicio.
- **Quitar el icono Buscar**. Impide que los usuarios utilicen la herramienta Buscar con el icono del menú Inicio para buscar carpetas, archivos y recursos de red a los que no deben tener acceso.
- **Quitar el icono Ejecutar**. Impide que los usuarios utilicen el cuadro de diálogo Ejecutar para emitir comandos o iniciar programas.
- **Quitar la lista de Programas usados con frecuencia**. Impide que el menú Inicio muestre los programas utilizados con frecuencia.
- **Quitar el botón Apagar**. Impide que los usuarios desactiven o reinicien el equipo a través del icono del menú Inicio.

Restricciones generales de Windows XP

En la lista siguiente, se describen las restricciones generales de Windows XP:

- **Impedir hacer clic con el botón secundario en el Explorador de Windows**. Deshabilita el menú contextual que aparece cuando un usuario hace clic con el botón secundario en un objeto del entorno Windows.
- **Impedir la reproducción automática en unidades de CD, DVD y USB**. Evita que Windows muestre opciones (o realice una acción determinada) automáticamente cuando un usuario inserta un medio extraíble. Los medios de entretenimiento digital como las canciones y las películas se seguirán reproduciendo automáticamente con esta opción habilitada.
- **Quitar la Papelera de reciclaje (para ayudar a asegurar la privacidad entre usuarios)**. Ayuda a garantizar que cuando un usuario elimine un archivo, los usuarios siguientes no puedan obtener acceso al mismo.
- **Impedir el acceso a algunas características del Explorador de Windows (como Buscar).** Deshabilita la búsqueda y evita que el usuario personalice barras de herramientas y Opciones de carpeta. Además, la carpeta Mis documentos queda oculta en el panel izquierdo.
- **Impedir el acceso a la barra de tareas**. Evita el acceso a la barra de tareas de Windows.
- **Impedir el acceso al símbolo del sistema**. Evita que los usuarios obtengan acceso a archivos, carpetas y programas desde el símbolo del sistema de Windows.
- **Impedir el acceso al Editor del Registro.** Evita que los usuarios obtengan acceso a las herramientas integradas que permiten modificar el Registro.
- **Impedir el acceso al Administrador de tareas**. Impide que los usuarios tengan acceso al Administrador de tareas, utilidad que se puede utilizar para detener e iniciar programas y procesos, y para apagar o reiniciar el equipo.
- **Impedir el acceso a las utilidades de Microsoft Management Console**. Evita que los usuarios utilicen la consola MMC para cargar complementos que se pueden utilizar para modificar el entorno Windows.
- **Impedir que los usuarios agreguen o quiten impresoras**. Evita que los usuarios agreguen o quiten impresoras para conservar la configuración del sistema.

- **Impedir que los usuarios bloqueen el equipo**. Evita que los usuarios puedan bloquear el equipo para denegar el acceso a otros usuarios.
- **Impedir cambios de contraseña (requiere también que el Panel de control se quite)**. Impide que los usuarios cambien la contraseña asociada a la cuenta de usuario con la que inician sesión.

Restricciones de Internet Explorer

En la lista siguiente, se describen las restricciones de Internet Explorer:

- **Impedir hacer clic con el botón secundario en Internet Explorer**. Evita que los usuarios puedan realizar actividades avanzadas de contenido Web en Internet Explorer al hacer clic con el botón secundario en los elementos. De todos modos, todavía es posible hacer clic con el botón secundario en algunos tipos de contenido, como objetos de Macromedia Flash.
- **Impedir el acceso a algunas opciones del menú de Internet Explorer (como Opciones de Internet)**. Evita que los usuarios obtengan acceso a determinados comandos de menú de Internet Explorer, como Opciones de Internet, que pueden utilizarse para modificar la configuración de Internet Explorer.
- **Impedir el acceso a algunos botones de la barra de herramientas de Internet Explorer (como Búsqueda)**. Evita que los usuarios obtengan acceso a determinados botones de barra de herramientas, como Historial, Búsqueda y Noticias. De este modo, se impide que los usuarios pasen por alto los controles de acceso.

Restricciones de Microsoft Office

Puede usar la herramienta Restricciones del usuario para establecer restricciones aplicables a Microsoft Office XP y 2003. Algunas de estas restricciones también se aplican a Microsoft Office 2000. En la siguiente lista, se describen las restricciones de Microsoft Office:

- **Impedir el uso de Visual Basic para aplicaciones (VBA) en Office XP/2003**. Impide que los usuarios tengan acceso a las herramientas de VBA en los programas de Office XP y Office 2003 (no funciona en Office 2000).
- **Deshabilitar teclas de acceso directo a macros**.
- Evita que los usuarios ejecuten macros mediante teclas de acceso directo en programas de Office.
- **Deshabilitar elementos del menú Herramientas | Macro**. Evita que los usuarios obtengan acceso a comandos de macro en programas de Office.
- **Deshabilitar elementos del menú Herramientas | Complementos**. Evita que los usuarios habiliten y deshabiliten complementos en programas de Office.
- **Deshabilitar la barra de herramientas Web**. Evita que los usuarios habiliten la barra de herramientas Web en programas de Office y puedan ver archivos y carpetas de unidades restringidas.
- **Deshabilitar Detectar y reparar en el menú de Ayuda**. Evita que los usuarios ejecuten el comando Detectar y reparar en programas de Office.
- **Impedir cambios al contenido de la Galería multimedia en Office XP/2003**. Impide que los usuarios importen o eliminen clips en la Galería multimedia de los programas de Office XP y Office 2003 (no funciona en Office 2000).

Restricciones de software

Importante
Algunos juegos (como Microsoft Halo® y Activision Call of Duty) y otros programas que utilizan la protección contra copia no funcionan correctamente cuando se seleccionan las restricciones de software. Si es usuario de estos juegos, no podrá utilizar las restricciones de software al mismo tiempo. Tenga presente que al desactivar las restricciones de software debilitará considerablemente la seguridad del equipo.

Las restricciones de software proporcionan una configuración de seguridad que puede ayudarle a restringir la ejecución de herramientas de sistema y software descargable. Para mayor seguridad, asegúrese de que ambas restricciones están seleccionadas. Si no lo están, es posible que los usuarios encuentren formas de evitar las restricciones configuradas mediante el Toolkit. Por ejemplo, un usuario limitado podría descargar un programa que omita las restricciones, lo que le permitiría editar el registro, obtener acceso a las unidades restringidas e incluso usar el símbolo del sistema aunque haya restricciones que se lo impidan.

En la lista siguiente, se describen las restricciones de software:

- **Únicamente permitir que se ejecute software en las carpetas Archivos de programa y Windows**. Impide que los usuarios puedan ejecutar programas que no se encuentren en la carpeta Archivos de programa o la ruta de acceso de Windows, como programas descargados o programas incluidos en unidades USB. Los accesos directos desde cualquier ubicación funcionarán si apuntan al software de las carpetas Archivos de programa y Windows. Los ejecutables no se pueden ubicar en un escritorio o en un menú Inicio restringido; desde estas ubicaciones, sólo f uncionarán los accesos directos a programas permitidos.
- **Impedir la ejecución de Herramientas del sistema y algunas herramientas administrativas**. Bloquea la ejecución de herramientas del sistema como Desfragmentador de disco.

Restricciones opcionales

En la lista siguiente, se describen las restricciones opcionales:

Nota
Si se impide que se muestren los elementos de menú de Todos los usuarios, se bloquearán todos los iconos que el Toolkit u otros programas de Windows coloquen en Todos los usuarios y no se mostrarán en el menú Inicio de los usuarios limitados. Asegúrese de que los iconos que van a necesitar los usuarios se copien de la carpeta del menú Inicio de Todos los usuarios a la carpeta de menú Inicio del usuario restringido.

Restricciones adicionales del menú Inicio

- **Impedir que los programas de la carpeta Todos los usuarios aparezcan en el menú Inicio**. Esta opción evita que los iconos que se encuentran en la carpeta Todos los usuarios del menú Inicio se muestren en el menú Inicio del usuario.
- **Quitar el icono Ayuda y soporte técnico**. Evita que los usuarios obtengan acceso a la ventana Ayuda y soporte técnico con el icono del menú Inicio. Muchas páginas de ayuda ofrecen acceso directo a herramientas y ubicaciones del sistema.

Restricciones adicionales de Windows XP en general

- **Quitar Documentos compartidos de Mi PC**. Esta opción evita el uso compartido de documentos entre usuarios y protege la privacidad del usuario.
- **Quitar características de copiado en CD y DVD.** Evita que los usuarios utilicen las características integradas de Windows XP para copiar información en un CD o un DVD grabable.
- **Deshabilitar cualquier acceso directo de teclado que use la tecla con el logotipo de Windows.** Impide que los usuarios usen métodos abreviados de teclado para obtener acceso a menús o programas no autorizados (como la tecla del logotipo de Windows + E para iniciar el Explorador de Windows).

Restricciones adicionales de Internet Explorer

- **Impedir el acceso a Internet desde Internet Explorer**. Esta opción evita que el usuario obtenga acceso a Internet con un programa que utilice la configuración proxy de Internet Explorer.Al habilitar esta restricción, la opción Proxy se configura automáticamente en *NoInternetAcces*s.
- **Impedir la impresión desde Internet Explorer**. Esta opción evita que los usuarios impriman desde Internet Explorer.

Restricciones adicionales de software

- **Impedir que se ejecuten Windows Messenger y MSN Messenger**. Esta opción evita que el usuario pueda utilizar Windows Messenger o MSN Messenger. Tenga en cuenta que esta opción impide que los usuarios ejecuten Windows Messenger directamente desde su icono, pero no que ejecuten Messenger desde una interfaz basada en Web, como MSN Web Messenger. Para evitar el acceso a un servicio basado en Web, será necesario agregar la dirección URL del servicio a la lista direcciones URL bloqueadas de Internet Explorer.
- **Restringir Notepad y WordPad (recomendado para Administradores restringidos)**. Esta opción restringe el uso de las dos principales herramientas de edición de texto que utilizan los administradores para editar archivos y secuencias de comandos por lotes en Windows XP. Puede utilizarse para evitar que desde una cuenta de administrador restringida se modifiquen las secuencias de comandos, incluidas las que proceden de Shared Computer Toolkit.
- **Impedir que se ejecuten los programas de Microsoft Office**. Esta opción evita que el usuario ejecute los programas de Microsoft Office. Para que funcione correctamente, es preciso que Microsoft Office se instale en la ubicación predeterminada (%ProgramFiles%), es decir, C:\Archivos de programa\Microsoft Office.

Capítulo 5: Experiencia de usuario restringida

Aunque son los operadores de equipos compartidos los que utilizan principalmente las herramientas de Microsoft® Shared Computer Toolkit para Windows® XP, la función más importante de dichas herramientas es mejorar y simplificar la experiencia del usuario.

En este capítulo se tratan los siguientes temas:

- Un escritorio restringido típico
- Cómo probar los perfiles de usuario restringidos
- Recursos en línea para el uso de equipos públicos
- La herramienta Accesibilidad

Un escritorio restringido típico

Si crea, configura y restringe perfiles de usuario, puede proporcionar a los usuarios una experiencia controlada y coherente. La siguiente ilustración muestra el menú Inicio de un perfil de usuario que se ha restringido para mostrar sólo los accesos directos de programa seleccionados.

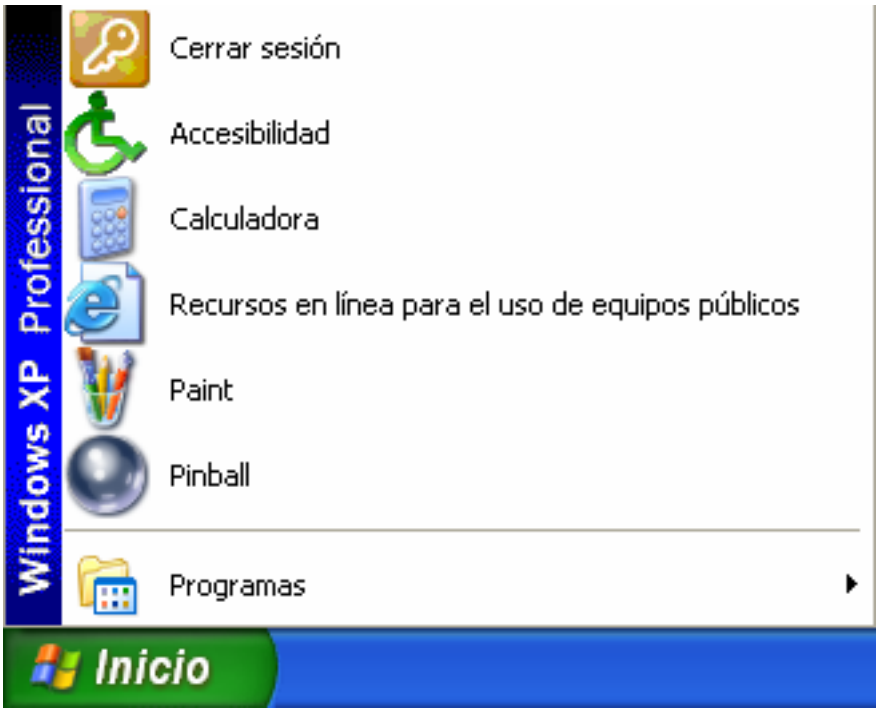

Figura 5.1 *Menú Inicio restringido*

Cómo probar los perfiles de usuario restringidos

Antes de activar Protección de discos de Windows, dedique un tiempo a probar los perfiles y las cuentas de usuario para asegurarse de que las configuraciones y las restricciones funcionan correctamente. Para probar una cuenta de usuario, inicie una sesión en el equipo con la cuenta de usuario y compruebe que:

- Los menús Inicio se muestran correctamente.
- Los accesos directos del menú Inicio y el Escritorio funcionan correctamente.
- No se ofrecen contratos de licencia ni pantallas de configuración inicial.
- Los programas a los que los usuarios no tienen acceso no aparecen en el menú Inicio.
- Las restricciones de usuario que ha configurado para el escritorio, el menú Inicio e Internet Explorer funcionan correctamente.
- Todos los temporizadores de sesión que ha aplicado funcionan correctamente.
- La herramienta Accesibilidad está ubicada directamente en el menú Inicio, a disposición de los usuarios que la necesiten.
- El vínculo Recursos en línea para el uso de equipos públicos está ubicado directamente en el menú Inicio, a disposición de todos los usuarios.
- No aparece ninguna advertencia de bloqueo de secuencias de comandos o de seguridad de terceros.

Normalmente, los problemas que se detecten al probar las cuentas de usuario pueden resolverse recurriendo a uno de los métodos siguientes:

- Seleccione restricciones adicionales en la herramienta Restricciones del usuario para impedir el acceso no deseado a los recursos del sistema. Esta tarea puede realizarla el administrador del Toolkit en un perfil de usuario que esté restringido y bloqueado.
- Borre las restricciones de la herramienta Restricciones del usuario si algunos programas no pueden ejecutarse a causa de las restricciones. Esta tarea puede realizarla el administrador del Toolkit en un perfil de usuario que esté restringido y bloqueado.
- Agregue o elimine iconos de programa del menú Inicio del usuario y el menú Inicio de Todos los usuarios si no aparecen los iconos que corresponden.Esta tarea puede llevarse a cabo utilizando el Explorador de Windows desde una cuenta administrativa, aunque el perfil esté restringido y bloqueado.
- Cambie la configuración de un perfil de usuario durante una sesión que haya iniciado como usuario. Esto sólo puede hacerse en un perfil de usuario que no esté restringido ni bloqueado.

Algunas opciones sólo se pueden configurar si se inicia sesión como usuario. El procedimiento siguiente describe cómo modificar esta configuración después de restringir y bloquear un perfil de usuario.

Para cambiar la configuración de perfil de usuario que requiere iniciar sesión como usuario:

1. Inicie sesión como *administrador del Toolkit*, la cuenta administrativa local con la que ha instalado el Toolkit.
2. Inicie la herramienta Restricciones del Usuario. Seleccione el perfil de usuario que desea cambiar.

3. Tome nota de las restricciones para volver a aplicarlas más tarde.
4. Haga clic en el botón **Seleccionar unidades**. En el cuadro de diálogo **Restringir unidades**, asegúrese de que todas las unidades aparecen en la columna **Mostradas** y de que la columna **Restringidas** está vacía.
5. Desactive las casilla de verificación, **Bloquear este perfil**, **Reiniciar al cerrar sesión** y **Restricciones recomendadas para cuentas compartidas**.
6. Haga clic en **Aceptar** para aplicar estos cambios y cerrar la herramienta Restricciones del usuario.
7. Cierre la sesión e inicie otra sesión con la cuenta de usuario. Configure las opciones necesarias.
8. Cierre la sesión y vuelva a iniciar otra sesión usando la cuenta de administrador del Toolkit.
9. Inicie la herramienta Restricciones del usuario para bloquear el perfil del usuario (si se ha bloqueado anteriormente) y configure las mismas restricciones que había antes.
10. Cierre la sesión y, a continuación, vuelva a iniciar una sesión como usuario y pruebe otra vez el perfil.
11. Repita los pasos 1 a 6 según sea necesario hasta que se corrija el problema.
12. Si la herramienta Protección de discos de Windows ha estado activada anteriormente (no debería ser éste el caso si es la primera vez que utiliza las herramientas), ábrala y seleccione la opción **Guardar cambios con el siguiente reinicio**, haga clic en **Aceptar** y, a continuación, haga clic en **Sí** para reiniciar el equipo.

Cuando haya comprobado que todas las cuentas de usuario funcionan correctamente con las restricciones configuradas, estará listo para activar Protección de discos de Windows siguiendo los pasos que se describen en el capítulo siguiente.

Recursos en línea para el uso de equipos públicos

Nota
En la carpeta menú Inicio del perfil Todos los usuarios, se instala un acceso directo a la página Recursos en línea para el uso de equipos públicos.

La página Web Recursos en línea para el uso de equipos públicos proporciona una lista de recursos en línea con información acerca de cómo usar Windows y mejorar la seguridad y la privacidad, dirigida a usuarios sin experiencia en equipos informáticos o Windows XP. La página también contiene recursos específicamente concebidos para niños y adolescentes.

Para obtener acceso a la página, los usuarios pueden hacer clic en el acceso directo **Recursos en línea para el uso de equipos públicos** del menú Inicio.

La herramienta Accesibilidad

Windows XP ofrece una serie de utilidades y opciones de accesibilidad para usuarios con necesidades especiales. Estas opciones facilitan la visión del escritorio y el uso de dispositivos de entrada como el teclado y el *mouse* (ratón).

El Toolkit proporciona un acceso fácil a algunas opciones de accesibilidad para que los usuarios de una cuenta restringida puedan seguir personalizando el entorno de Windows. Al iniciar una sesión, basta con hacer clic en **Inicio** y, a continuación, hacer clic en **Accesibilidad** para obtener acceso a la ventana de Accesibilidad que se muestra en la

ilustración siguiente. La configuración realizada en la ventana Accesibilidad, se guardará en el perfil del usuario, si no está bloqueado, para que vuelva a tener la misma experiencia la próxima vez que use el equipo.

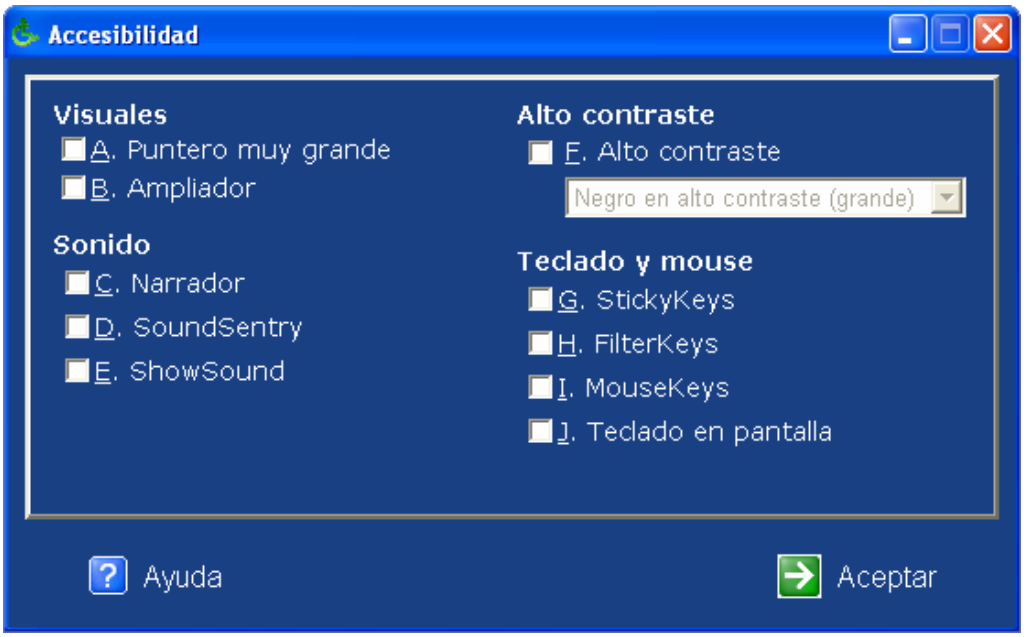

Figura 5.2 *Pantalla principal de la herramienta Accesibilidad*

Los usuarios pueden configurar las siguientes opciones en la ventana Accesibilidad:

- **Visuales**. Entre las opciones de esta sección se incluyen las siguientes:
  - **Puntero muy grande** aumenta el tamaño del puntero de Windows.
  - **Ampliador** reserva la parte superior de la pantalla para proporcionar una vista ampliada del área que rodea al puntero de Windows.
- **Sonido.** Entre las opciones de esta sección se incluyen las siguientes:
  - **Narrador** funciona con algunos programas; emplea una voz sintetizada para leer en voz alta el texto que aparece en pantalla.
  - **SoundSentry** hace que Windows genere advertencias visuales cuando el sistema emite un sonido, lo que resulta útil para usuarios con sordera o problemas auditivos. Puede establecer que Windows haga parpadear la barra de títulos situada en la parte superior de una ventana o un cuadro de diálogo, la propia ventana o todo el escritorio.
  - **ShowSound** hace que Windows muestre un icono o una nota de texto para indicar el sonido determinado que emite Windows.
- **Alto contraste**. Selección de opciones de contraste que pone a disposición de los usuarios combinaciones de colores de escritorio de alto contraste, lo que mejora la legibilidad para personas con deficiencias visuales.
- **Teclado y mouse.** Entre las opciones de esta sección se incluyen las siguientes:
  - **StickyKeys** permite al usuario utilizar combinaciones de teclas (como CTRL+ESC) presionando una tecla cada vez, en lugar de tener que presionarlas simultáneamente. StickyKeys funciona con las teclas CTRL, ALT y SUPR, así como con la tecla del logotipo de Windows. Cuando un usuario presiona una de estas teclas, Windows registra la tecla como “presionada” hasta que se complete la combinación de teclas.

- **FilterKeys** hace que Windows pase por alto las pulsaciones repetidas, lo que es de utilidad para personas con movimientos involuntarios de la mano que les hacen presionar las teclas varias veces consecutivas o mantenerlas presionadas más de lo que pretenden.
- **MouseKeys** permite al usuario utilizar el teclado numérico para controlar los movimientos del puntero en lugar de utilizar el mouse (o además de utilizarlo).
- **Teclado en pantalla** abre un teclado basado en software en una ventana en pantalla. Para presionar las teclas, los usuarios pueden hacer clic en ellas con el mouse u otro dispositivo señalador.

Para usar la herramienta Accesibilidad:

1. Haga clic en **Inicio** y, a continuación, haga clic en **Accesibilidad**.
2. En la herramienta **Accesibilidad**, seleccione una casilla de verificación o presione ALT junto con la tecla de la letra subrayada correspondiente a la opción deseada.
3. Seleccione tantas opciones como desee aplicar y, a continuación, haga clic en **Aceptar**.

Capítulo 6: Protección de discos de Windows

La herramienta Protección de discos de Windows protege el sistema operativo Windows y los archivos de programa contra los cambios permanentes realizados en la partición de Windows. Durante la sesión, el usuario puede realizar los cambios que sean necesarios dentro de los límites que imponen las restricciones que se le han aplicado. Al reiniciar el equipo, Protección de discos de Windows devuelve la partición de Windows a su estado original, descartando todos los cambios realizados durante la sesión.

Esta herramienta ayuda a proteger los equipos de los usuarios que intentan dañar el sistema operativo y también evita que códigos dañinos y spyware alteren el equipo.

Cada vez que se reinicia el equipo, la herramienta Protección de discos de Windows devuelve la partición que mantiene Windows y los archivos de programa (denominada *partición de Windows*) a su estado original. De este modo, se proporciona al siguiente usuario una experiencia estándar y confiable.

En este capítulo se tratan los siguientes temas:

- Activar la herramienta Protección de discos de Windows
- Guardar los cambios cuando está activada la herramienta Protección de discos de Windows
- Conservar los cambios cuando está activada la herramienta Protección de discos de Windows
- Conservar los cambios indefinidamente cuando está activada la herramienta Protección de discos de Windows
- Mejorar el rendimiento de la herramienta Protección de discos de Windows
- Administrar la partición de protección

código dañino
Software malintencionado. El concepto incluye virus, gusanos y caballos de Troya diseñados para dañar el sistema operativo del equipo.

spyware
Software potencialmente no deseado que puede obtener información personal y que resulta inadecuado para los equipos compartidos.

Importante
Antes de activar Protección de discos de Windows, asegúrese de que ha preparado correctamente el disco y ha creado, personalizado y restringido los perfiles de usuario necesarios de la forma descrita en los capítulos anteriores.

Activar la herramienta Protección de discos de Windows

El funcionamiento predeterminado de Partición de discos de Windows consiste en deshacer los cambios realizados en la partición de Windows con cada reinicio del equipo, protegiendo de este modo el disco de los cambios no deseados. Los operadores pueden optar por guardar los cambios realizados en el disco en cualquier momento. Los operadores también pueden programar la herramienta Protección de discos de Windows para descargar, instalar y guardar automáticamente actualizaciones críticas en el disco mientras no se esté utilizando el equipo.

Nota
Para obtener un mayor rendimiento del disco, desfragmente la partición de Windows antes de activar la herramienta Protección de discos de Windows. Mientras esté activada la herramienta Protección de discos de Windows, no desfragmente el disco.

Para activar la herramienta Protección de discos de Windows y programar actualizaciones críticas:

1. Haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Protección de discos de Windows**. Reinicie el equipo si se le pide y, a continuación, vuelva a iniciar Protección de discos de Windows.
2. En la sección **Acción de reinicio**, haga clic en **Conservar activada**. Si es la primera vez que usa Shared Computer Toolkit, la herramienta Protección de discos de Windows

creará la partición de protección. Es necesario reiniciar el equipo para completar el proceso de inicialización.

3. Después del reinicio, vuelva a Protección de discos de Windows para completar la configuración.
4. Si la herramienta Protección de discos de Windows identifica un programa antivirus que sabe cómo actualizar, mostrará un cuadro de diálogo al respecto. Si aparece este cuadro de diálogo, haga clic en **Aceptar**.
5. Si la herramienta Protección de discos de Windows no ha detectado el software antivirus, haga clic en **Establecer** para especificar una secuencia de comandos de antivirus que haya creado. Si es necesario, puede configurar otras secuencias de comandos de actualización para administrar las actualizaciones de programas de terceros.
6. En la sección **Actualizaciones críticas**, configure el día y la hora a la que Protección de discos de Windows debe descargar e instalar las actualizaciones críticas.
7. En Actualizaciones de Microsoft, haga clic en Habilitado para permitir que se lleven a cabo las actualizaciones críticas de Microsoft.
8. Haga clic en **Aceptar**.
9. La herramienta Protección de discos de Windows muestra un mensaje que indica que es necesario reiniciar el equipo para que los cambios surtan efecto. Haga clic en **Sí** para reiniciar el equipo.

Importante
No intente cambiar ninguna partición después de la activación Protección de discos de Windows, ya que esta herramienta realiza un seguimiento de los números de las particiones y el disco físico, y éstos no deben cambiar. Si debe cambiar las particiones, desactive Protección de discos de Windows y elimine la partición de protección antes de realizar los cambios.

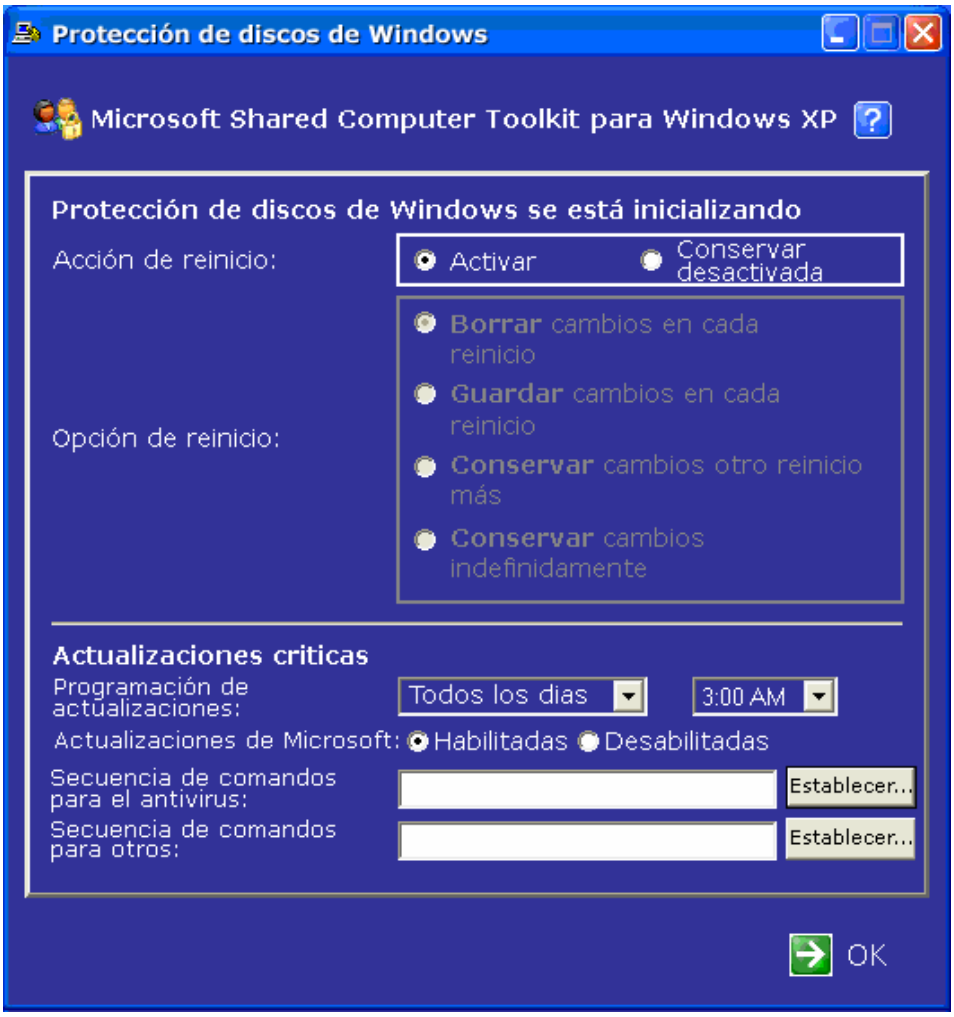

Figura 6.1 *Pantalla principal de la herramienta Protección de discos de Windows*

Nota
Los servicios que normalmente almacenan datos en la partición de Windows (como el registro de eventos) no podrán guardar entradas de registro permanentemente, porque las nuevas se perderán al borrar los cambios. Para conservar los registros de eventos, se recomienda moverlos a un volumen permanente. Este proceso se describe en la sección "Mejorar el rendimiento de la herramienta Protección de discos de Windows" de este capítulo.

La configuración predeterminada para Protección de discos de Windows es **Borrar cambios en cada reinicio**. Con esta opción, se garantiza que los usuarios que no son de confianza y el código dañino no puedan guardar cambios en la partición de Windows del equipo. Al reiniciar el equipo, se eliminan todos los cambios realizados en el disco, y el equipo vuelve a su estado anterior.

La **Opción de reinicio** no se podrá cambiar hasta después de reiniciar el equipo con la herramienta Protección de discos de Windows activada. Con ello se garantiza que Protección de discos de Windows se inicie con la configuración predeterminada.

Protección de discos de Windows e hibernación.

Si la hibernación está habilitada en el sistema, al activar la herramienta Protección de discos de Windows, recibirá un mensaje indicándole que la hibernación no es compatible con esta herramienta.

Cuando un equipo hiberna, el contenido de la memoria RAM del sistema se guarda en un archivo en el disco. Puesto que las modificaciones de la partición de Windows se borran cuando la herramienta Protección de discos de Windows está activada con la opción **Borrar cambios en cada reinicio** seleccionada, no se puede realizar la hibernación.

Para deshabilitar la hibernación, abra el Panel de Control, haga doble clic en **Opciones de energía**, haga clic en la ficha **Hibernación** y, a continuación, desactive la casilla de verificación **Habilitar hibernación**.

Estado de Protección de discos de Windows

Si la herramienta Protección de discos de Windows está activada y la herramienta Introducción no está configurada para ejecutarse automáticamente, aparecerá un elemento emergente denominado **Protección de discos está activada** cada vez que inicie una sesión como administrador del Toolkit. Este elemento emergente ofrece un modo muy práctico de abrir la herramienta Protección de discos de Windows cuando hay que guardar cambios en el disco.

Figura 6.2 *Ventana emergente Protección de discos está activada*

Si no desea que esta ventana emergente siga apareciendo, elimine el acceso directo **Comprobar Protección de discos de Windows** de la carpeta Inicio del administrador del Toolkit.

Actualizaciones críticas

Si activa la herramienta Protección de discos de Windows, las actualizaciones críticas de Microsoft se seguirán instalando según la programación de Actualizaciones automáticas que se haya configurado anteriormente. Según el servicio que esté usando Windows actualmente, la herramienta utilizará Microsoft Update (http://go.microsoft.com/fwlink/?LinkId=17289), Windows Update (http://go.microsoft.com/fwlink/?LinkId=17289) o Windows Server Update Services (http://go.microsoft.com/fwlink/?LinkId=12524); puede que las páginas estén en inglés. El servicio Software Update Services no es compatible. Al activar la herramienta Protección de discos de Windows, podrá habilitar o deshabilitar Microsoft Updates y elegir la programación que mejor se adapte a sus necesidades.

Cada vez que Protección de discos de Windows descargue e instale actualizaciones críticas, cerrará la sesión del usuario activo, reiniciará el equipo para borrar los cambios del disco y deshabilitará temporalmente las cuentas de usuario locales para impedir que al mismo tiempo se guarden cambios no aprobados en el disco. Una vez descargadas e instaladas las actualizaciones, la herramienta Protección de discos de Windows se establecerá en la opción **Guardar cambios con el siguiente reinicio** y, a continuación, reiniciará el equipo.

Además de guardar las actualizaciones críticas de Microsoft automáticamente, Protección de discos de Windows permite seleccionar una secuencia de comandos para guardar actualizaciones de programas antivirus y de otro tipo.

Nota

Para obtener más información acerca del proceso de actualizaciones críticas de la herramienta Protección de discos de Windows, consulte el apéndice A, “Conceptos técnicos elementales”.

Otra posibilidad es programar actualizaciones de antivirus mediante la interfaz gráfica que ofrece el producto antivirus. Programe las actualizaciones para que se produzcan exactamente a las mismas horas y días que la programación seleccionada para las actualizaciones críticas en la herramienta Protección de discos de Windows.El proceso de actualizaciones críticas de Protección de discos de Windows esperará por lo menos 10 minutos a que otras actualizaciones finalicen simultáneamente antes de reiniciar el equipo y guardar los cambios efectuados en el disco.

La herramienta Protección de discos de Windows se ofrecerá para realizar las actualizaciones del antivirus automáticamente como parte del proceso de actualizaciones críticas si detecta un producto que sea capaz de actualizar. Actualmente, el Toolkit detecta e incluye secuencias de comandos para actualizar los siguientes productos antivirus (puede que las páginas estén en inglés):

- Computer Associates Etrust 7.0 (http://www3.ca.com/Solutions/Product.asp?ID=156)
- McAfee VirusScan 2005 (http://us.mcafee.com/root/package.asp?pkgid=100)
- McAfee VirusScan Enterprise 8.0 (http://www.mcafee.com)

Si tiene otro programa antivirus, podría interesarle preparar una secuencia de comandos de actualización de firma para el mismo siguiendo las instrucciones del manual de software de dicho producto. Busque las secciones que describen las herramientas de línea de comandos que realizan actualizaciones de firma.

Consulte el grupo de noticias de Microsoft Windows Shared Access para averiguar si hay algún otro usuario que haya creado ya una secuencia de comandos de actualización de firma para su programa antivirus.

Otras actualizaciones de Microsoft

La herramienta Protección de discos de Windows sólo automatiza las actualizaciones críticas de Microsoft; no instala automáticamente actualizaciones recomendadas, opcionales, especiales ni de controladores que puedan tener sus propios contratos de licencia. Consulte la lista de actualizaciones disponibles en el sito Web de Microsoft Update (http://go.microsoft.com/fwlink/?LinkId=17289; puede que la página esté inglés) periódicamente, descargue e instale las que desee y, a continuación, utilice la herramienta Protección de discos de Windows para guardar los cambios en el disco.

Guardar los cambios cuando está activada la herramienta Protección de discos de Windows

Importante

Antes de cambiar la opción de reinicio de la herramienta Protección de discos de Windows para borrar todos los cambios anteriores que no desee conservar, reinicie el equipo una vez.

Si la herramienta Protección de discos de Windows está activada, debe tomar una serie de medidas especiales para que los cambios realizados en el disco sean permanentes. Estos cambios pueden incluir la instalación de un programa, la modificación del registro, agregar una cuenta de usuario o configurar las opciones del sistema para los usuarios.

Para instalar un programa con la herramienta Protección de discos de Windows desactivada, inicie una sesión en el equipo como administrador del Toolkit, instale el programa y, a continuación, asegúrese de que el acceso directo del mismo aparece en los menús Inicio correspondientes. Si la herramienta Protección de discos de Windows está activada, los cambios realizados en el disco deben guardarse dentro de la propia herramienta.

A veces, es necesario realizar un cambio permanente en el disco. Aunque esto se puede lograr desactivando Protección de discos de Windows durante el tiempo necesario para

instalar el programa, con este método corre el riesgo de olvidarse de volver a activar la herramienta una vez finalizada la instalación. El método más rápido es usar la opción **Guardar cambios con el siguiente reinicio** como se describe en el siguiente procedimiento:

Para realizar cambios cuando está activada la herramienta Protección de discos de Windows:

1. Reinicie el equipo compartido para asegurarse de que se borran los cambios más recientes realizados en el disco.
2. Inicie sesión como administrador del Toolkit.
3. Haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Protección de discos de Windows**. Otra opción es hacer clic en el vínculo **Abrir Protección de discos de Windows** en el paso 7 de la herramienta Introducción. También se incluye un acceso directo en la sección **Acceso rápido**, cerca de la parte superior de la ventana Introducción.
4. Haga clic en **Guardar cambios con el siguiente reinicio** y, a continuación, haga clic en **Aceptar**.
5. En este momento no se producirá el reinicio.
6. Realice los cambios necesarios (como instalar el software o modificar un perfil de usuario) en el equipo compartido y, a continuación, reinicie el equipo.
7. Cuando el equipo se reinicie, el sistema operativo guardará los cambios en la partición de Windows y volverá automáticamente a **Borrar cambios en cada reinicio**.

Conservar los cambios cuando está activada la herramienta Protección de discos de Windows

Puede que en algunas ocasiones los usuarios necesiten instalar un programa o realizar cambios en el sistema que desee poner a prueba o que no desee conservar permanentemente en el equipo; sin embargo, es necesario un reinicio.

Importante
La opción **Conservar cambios por un reinicio** sólo se mantiene en funcionamiento hasta el siguiente reinicio. Cuando el equipo completa el reinicio, la herramienta vuelve a la opción predeterminada: **Borrar cambios en cada reinicio**

Para conservar temporalmente los cambios cuando está activada la herramienta Protección de discos de Windows:

1. Reinicie el equipo compartido para borrar los cambios realizados anteriormente en el disco.
2. Inicie sesión como administrador del Toolkit.
3. Haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Protección de discos de Windows**.
4. Haga clic en **Conservar cambios por un reinicio** y, a continuación, haga clic en **Aceptar** para salir de la herramienta.
5. Realice los cambios que desee y, a continuación, reinicie el equipo.
6. Deje que el usuario inicie una sesión y use el equipo.
7. Después de la sesión del usuario, puede volver a reiniciar el equipo para deshacer los cambios de la partición de Windows y volver automáticamente a **Borrar cambios en cada reinicio**. Otra posibilidad es elegir la opción **Guardar cambios con el siguiente reinicio**.

El método anterior también se puede emplear para ejecutar CHKDSK en la partición de Windows, para lo cual es necesario reiniciar el equipo.

Importante
Si va a usar la opción **Conservar cambios indefinidamente** durante períodos prolongados, la herramienta Protección de discos de Windows necesitará más espacio no asignado. Para ejecutarse de este modo indefinidamente, el tamaño de la partición de protección debe coincidir con el de la partición de Windows.

Conservar los cambios indefinidamente cuando está activada la herramienta Protección de discos de Windows

Esta opción permite a los operadores realizar tareas que pueden implicar la instalación y la comprobación de varios programas nuevos. Después de hacer clic en la opción **Conservar cambios indefinidamente**, los cambios seguirán acumulándose en el equipo hasta que haga clic en **Guardar cambios con el siguiente reinicio** o **Borrar cambios en cada reinicio**.

La opción **Conservar cambios indefinidamente** puede resultar especialmente útil si necesita instalar varios programas nuevos. Por ejemplo, si esta opción está habilitada, puede instalar un nuevo programa, probarlo para detectar posibles problemas de compatibilidad con otros programas del equipo y después seguir instalando otros programas antes de borrar o guardar todos los cambios del disco.

Mejorar el rendimiento de la herramienta Protección de discos de Windows

Para mejorar el rendimiento de la herramienta Protección de discos de Windows, puede desfragmentar el disco cuando esté desactivada y eliminar los datos innecesarios moviendo los registros de eventos y los archivos de paginación de memoria virtual.

Estas actividades son totalmente opcionales y se han concebido para operadores expertos en la administración de Windows XP.

Desfragmentar la partición de Windows.

Puede optimizar el rendimiento del disco en la partición de Windows si la desfragmenta antes de activar la herramienta Protección de discos de Windows.

Una vez hecho esto, no es necesario volver a repetir el proceso muy a menudo.

Aunque la instalación de actualizaciones críticas y correcciones de programas produce un volumen de fragmentación insignificante, no debería ser necesario volver a desfragmentar el disco en lo sucesivo.

Mientras esté activada la herramienta Protección de discos de Windows, no desfragmente la partición de Windows. Para desfragmentar el disco, desactive la herramienta.

Para desfragmentar la partición de Windows:

1. Desactive la herramienta Protección de discos de Windows.
2. Reinicie el equipo para completar la desactivación de Protección de discos de Windows.
3. Use el Desfragmentador de disco de Windows o una herramienta de terceros para desfragmentar la partición de Windows.
4. Active la herramienta Protección de discos de Windows y vuelva a reiniciar el equipo.

Mover el archivo de paginación de memoria virtual

El archivo de paginación de memoria virtual es el archivo en el que se colocan las partes de los programas y archivos de datos que no caben en la memoria. Windows XP guarda este archivo de paginación en la partición de Windows de manera predeterminada. La escritura de datos en un archivo de paginación ubicado en la partición de Windows puede reducir el rendimiento del sistema considerablemente.

El traslado del archivo de paginación de la partición de Windows a un disco persistente permite que el sistema optimice el uso de la partición de protección.

Para mover el archivo de paginación a un disco persistente:

1. Configure la herramienta Protección de discos de Windows con la opción **Guardar cambios con el siguiente reinicio**.
2. Haga clic en **Inicio**, haga clic con el botón secundario en **Mi PC** y, después, haga clic en **Propiedades**. Se abrirá el cuadro de diálogo **Propiedades del sistema**.
3. En la ficha **Opciones avanzadas**, en **Rendimiento**, haga clic en **Configuración**.
4. En el cuadro de diálogo Opciones de rendimiento, haga clic en la ficha **Opciones avanzadas**.
5. En la sección **Memoria virtual**, haga clic en **Cambiar**.
6. En el cuadro de diálogo **Memoria virtual** (véase la ilustración siguiente), en la lista **Unidad**, haga clic en el disco de la partición de Windows y después seleccione la opción **Sin archivo de paginación** para quitar el archivo de paginación de ese disco.
7. Haga clic en **Establecer** para aplicar esta configuración.
8. En la lista **Unidad**, haga clic en un disco de una partición persistente y, a continuación, haga clic en **Tamaño administrado por el sistema** para hacer que Windows asigne espacio de ese disco a un archivo de paginación.
9. Haga clic en **Establecer** para aplicar esta configuración.
10. Haga clic en **Aceptar** para guardar la configuración del archivo de paginación. Recibirá un mensaje indicándole que la configuración no cambiará hasta que se reinicie el equipo. Haga clic en **Aceptar** para cerrar el cuadro de diálogo y, a continuación, haga clic en **Aceptar** para cerrar los cuadros de diálogo **Opciones de rendimiento** y **Propiedades del sistema**.
11. Haga clic en **Sí** cuando se le pida que reinicie el equipo y guarde el cambio de configuración.

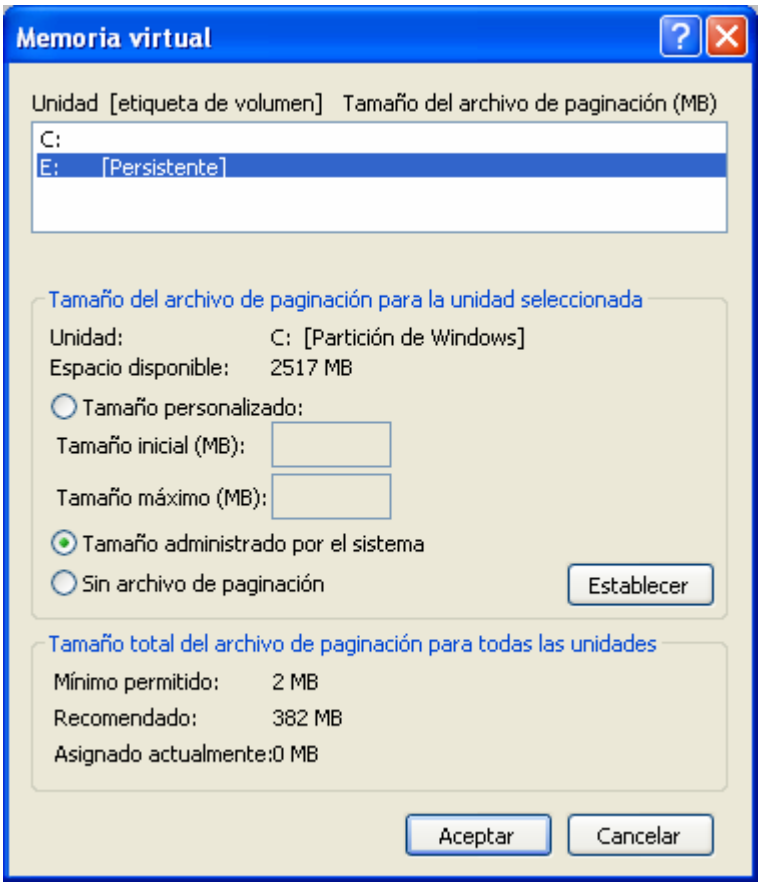

Figura 6.3 *Colocar el archivo de paginación en una partición persistente puede optimizar el rendimiento*

Colocar registros de eventos en una partición persistente

Las entradas efectuadas en los registros de eventos de aplicaciones y del sistema almacenados en la partición de Windows se perderán cada vez que el sistema se reinicie cuando la herramienta Protección de discos de Windows esté activada. Por este motivo, puede que en su entorno merezca la pena mover los registros de eventos a una partición persistente. Puede lograr este objetivo realizando una modificación en el registro del modo descrito en el siguiente procedimiento.

Para cambiar la ubicación en la que se almacenan los registros de eventos:

1. Reinicie el equipo para borrar todos los cambios pendientes de la partición de Windows.
2. Abra la herramienta Protección de discos de Windows y configúrela con la opción **Guardar cambios con el siguiente reinicio**.
3. Abra el Editor del Registro y modifique las rutas de acceso guardadas en las siguientes claves:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System
4. Cambie las rutas de acceso enumeradas en la clave **File** a una ubicación de la partición persistente del equipo.

5. Cierre el Editor del Registro y reinicie el equipo para guardar los cambios de configuración.

Administrar la partición de protección

La herramienta Protección de discos de Windows cumple muy bien su función cuando se configura siguiendo las instrucciones del capítulo 2, "Preparar el disco para Protección de discos de Windows". No obstante, en algunas ocasiones puede ser necesario realizar un control más riguroso de la herramienta Protección de discos de Windows. En esta sección, se explica cómo usar un segundo disco para crear en él la partición de protección (una opción útil para los equipos en los que el disco principal está casi lleno) y se describe un procedimiento para administrar el tamaño de dicha partición.

Estas actividades son totalmente opcionales y se han concebido para operadores expertos en la administración de Windows XP.

Colocar la partición de protección en otro disco

El proceso de preparación de Protección de discos de Windows descrito en los capítulos anteriores da por hecho que sólo se está utilizando una unidad de disco. En ocasiones, no es posible utilizar una unidad de disco existente, por motivos de espacio (la unidad está casi llena) o porque no se cumple algún otro requisito previo. En estos casos, puede utilizar una segunda unidad de disco para almacenar la partición de protección y seguir usando la herramienta Protección de discos de Windows.

Para ello, deben cumplirse las siguientes condiciones previas:

- Que el primer disco no disponga de espacio suficiente para admitir una partición de protección.
- Que el segundo disco tenga una partición primaria.
- Que el segundo disco disponga de suficiente espacio en disco no asignado, después de la partición primaria, para contener la partición de protección.

El proceso de creación de la partición de protección en un segundo disco consiste en instalar dicho disco, dar formato a la partición primaria (recuerde que la partición de protección debe realizarse después de una partición primaria) y configurar el Registro de Windows para permitir el uso del segundo disco como partición de protección.

Nota
El segundo disco de este escenario deber reunir los demás requisitos previos de la herramienta Protección de discos de Windows. No puede tener más de tres particiones primarias y debe disponer de espacio libre suficiente en una partición extendida.

Para usar un segundo disco físico con la herramienta Protección de discos de Windows:

1. Instale un segundo disco físico en el equipo.
2. En Administración de discos, cree una partición primaria al principio del nuevo disco.
3. Inicie el Editor del Registro. Busque la siguiente clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Computer Toolkit
4. Cambie el valor de SCTForceOverlay a un tamaño en bytes inferior al espacio en disco no asignado del segundo disco.

   Por ejemplo, para crear una partición de 3 GB, escriba el valor 3145728 para SCTForceOverlay (3 * 1024 * 1024 = 3145728).
5. Abra la herramienta Protección de discos de Windows. La herramienta Protección de discos de Windows detectará el espacio disponible en el segundo disco y configurará la partición de protección cuando esté activada.

Si más tarde desea cambiar la ubicación de la partición de protección, desinstale el Toolkit, vuelva a instalarlo y repita el proceso de creación de la partición de protección.

Especificar el tamaño de la partición de protección

Puede crear una partición de protección del tamaño especificado mediante la opción de registro **SCTForceOverlay** mencionada en el procedimiento anterior. Esto es aplicable al primer disco y al segundo. Resulta útil para controlar el tamaño de la partición de protección.

Para que la herramienta Protección de discos de Windows cree la partición de protección de tamaño fijo en el disco, deben cumplirse las dos siguientes condiciones previas:

- El disco debe tener una partición primaria.
- Debe disponer además de suficiente espacio no asignado para contener la partición de protección de tamaño fijo.

Para crear una partición de protección de tamaño fijo:

1. Inicie el Editor del Registro. Busque la siguiente clave: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Computer Toolkit**
2. Cambie el valor de **SCTForceOverlay** al tamaño que desea utilizar para la partición de protección.

   Por ejemplo, para crear una partición de 2 GB, escriba el valor 2097152 para **SCTForceOverlay** (2 * 1024 * 1024 = 2097152).
3. Abra la herramienta Protección de discos de Windows. La herramienta Protección de discos de Windows detectará el espacio disponible en el segundo disco y configurará automáticamente la partición de protección.

Si el disco vuelve alguna vez a un estado no protegido, puede deshacer esta configuración cambiando el valor de **SCTForceOverlay** a **0** o desinstalando y volviendo a instalar el Toolkit.

Capítulo 7: Lista de comprobación de seguridad

La seguridad de los equipos y las conexiones constituye una creciente preocupación para todos los usuarios de PC, especialmente si se proporciona un acceso público a equipos compartidos. A menudo, los problemas de seguridad parecen complicados y abrumadores, pero afortunadamente se pueden tomar una serie de medidas relativamente sencillas para mejorar la seguridad de un entorno de equipos compartidos.

Lista de comprobación de instalación

Realice las siguientes comprobaciones y operaciones durante la instalación y la configuración de Microsoft® Shared Computer Toolkit para Windows® XP para dotar a los sistemas de la mayor seguridad posible:

- ☐ Establezca una contraseña o una frase administrativa segura.
- ☐ Distinga visualmente las cuentas de administrador de las de usuario limitado.
- ☐ Quite la cuenta de administrador del Toolkit de la pantalla de bienvenida.
- ☐ Proteja físicamente los equipos manteniéndolos a la vista, marcándolos y cerrando las cubiertas con llave.
- ☐ Bloquee la BIOS del sistema
- ☐ Descargue e instale todas las actualizaciones críticas
- ☐ Lleve a cabo una auditoría de la seguridad de la red física
- ☐ Utilice un servidor de seguridad
- ☐ Instale un software antivirus
- ☐ Instale un programa antispyware
- ☐ Instale y configure un software de filtrado de Web

Lista de comprobación de mantenimiento (mensual)

Compruebe una vez al mes los siguientes elementos para garantizar un nivel de protección constante:

- ☐ Cambie las contraseñas de administrador
- ☐ Inspeccione visualmente los equipos para buscar indicios de alteraciones
- ☐ Lleve a cabo una auditoría de la seguridad de la red física
- ☐ Compruebe si hay actualizaciones disponibles para Windows y otros programas instalados
- ☐ Actualice el programa antivirus (si éste no se actualiza automáticamente)
- ☐ Actualice el programa antispyware (si éste no se actualiza automáticamente)

En las secciones siguientes, se describen más detalladamente cada uno de estos elementos de la lista de comprobación.

Seguridad del administrador del Toolkit

- **Use una contraseña segura**. Todas las cuentas administrativas de un equipo compartido, incluida la cuenta de administrador del Toolkit, deben tener una contraseña segura. No emplee palabras del diccionario, no base la contraseña en su nombre ni utilice contraseñas comunes como “contraseña” o “permiso”. No emplee una contraseña en blanco para la cuenta del administrador del Toolkit. Las contraseñas seguras son:
    - **Largas**. Las contraseñas deberían tener como mínimo ocho caracteres; cuanto más largas, mejor. Para la contraseña del administrador del Toolkit, se recomienda reforzar aún más la seguridad usando una contraseña de 15 caracteres como mínimo.
    - **Complejas**. Las contraseñas deberían componerse de una combinación de letras minúsculas y mayúsculas, números y símbolos (por ejemplo, ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . / o un espacio).
- **Use una frase en lugar de una palabra**. En Windows XP, es posible usar una frase en lugar de una sola palabra para la contraseña. Las frases tienen la ventaja de ser largas, complejas y fáciles de recordar. Asegúrese de utilizar las mismas reglas para la creación de contraseñas seguras que se han mencionado anteriormente. Un ejemplo de frase de contraseña puede ser “¡Les he enseñado a mis 3 perros viejos 6 nuevos trucos!”
- **Cambie la contraseña con frecuencia**. Cambie las contraseñas con regularidad y utilice siempre contraseñas totalmente diferentes a las anteriores. No basta con agregar un número al final de la contraseña habitual. Cambie las contraseñas administrativas cada trimestre o con mayor frecuencia.
- **Distinga visualmente la cuenta de administrador del Toolkit de las demás cuentas**. Facilite la identificación a simple vista de un usuario que haya iniciado una sesión con la cuenta de administrador del Toolkit. Use un fondo de escritorio distinto e incluso una combinación de colores diferente para los menús y las ventanas. Si las cuentas de usuario compartidas emplean el menú Inicio Clásico (práctica recomendada), puede hacer que la cuenta de administrador del Toolkit use el menú Inicio de Windows XP.
- **Quite la cuenta de administrador del Toolkit de la pantalla de bienvenida**. Utilice la herramienta Introducción o la herramienta Welcome.wsf para eliminar la cuenta del administrador del Toolkit de la pantalla de bienvenida de Windows. En la pantalla de bienvenida, presione CTRL+ALT+SUPR para obtener acceso al cuadro de diálogo de inicio de sesión tradicional, en el que puede escribir el nombre y la contraseña de la cuenta.

Seguridad de la red física

- **Lleve a cabo una auditoría de la seguridad de la red física**. Asegúrese de que no hay equipos o dispositivos no identificados conectados a la red o que se puedan conectar fácilmente a la misma. Alguien podría utilizar rastreadores de paquetes o servidores

Rogue para entrar en la red, poniendo en peligro la seguridad de los datos y los equipos.

Seguridad física

- **Mantenga los equipos a la vista**. Si se trata de equipos compartidos de acceso público, asegúrese de que puede ver lo que están haciendo los usuarios. Aunque normalmente no sea correcto vigilar al usuario durante la sesión, por lo menos debería poder ver si está intentando abrir la cubierta del equipo.
- **Cerrar los equipos con llave**. Utilice candados para cerrar con llave las cubiertas de los equipos y asegúrese de que los usuarios no pueden abrirlas. Con ello impedirá que los usuarios puedan abrir la cubierta para agregar o quitar componentes, o instalar dispositivos de seguimiento. Utilice cierres para mantener los equipos y otros dispositivos sujetos a las mesas o escritorios. Use un *mouse* óptico para que los usuarios no puedan retirar la bola. Asimismo, si proporciona auriculares a los usuarios, fije los cables de los mismos a las cubiertas de los equipos para evitar robos y actos de vandalismo.
- **Lleve a cabo inspecciones frecuentes**. Cada vez que un usuario termine de usar un equipo, inspeccione dicho equipo y los periféricos para comprobar si hay indicios de alteraciones. Algunos equipos de seguimiento se conectan a un puerto paralelo o USB, o se insertan en el cable del teclado.
- **Marque los equipos**. Utilice una herramienta de grabado para marcar el interior de las cubiertas con información que identifique a los equipos y a la organización. Asimismo, registre los números de serie y el modelo de los equipos y dispositivos periféricos.

Protección de la BIOS

- **Actualice la BIOS**. Asegúrese de que el equipo compartido esté ejecutando la última versión de la BIOS que ofrece el fabricante del equipo antes de instalar Windows XP.
- **Proteja la configuración de la BIOS mediante contraseña**. Esta protección requiere que el usuario escriba una contraseña válida para obtener acceso a las pantallas de configuración de la BIOS del equipo.

Importante

Si un usuario que no es de confianza puede iniciar el equipo desde un medio extraíble, cualquiera puede modificar la configuración y, por tanto, el equipo no es seguro. Las protecciones de la BIOS son medidas de seguridad críticas.

- **Impida el inicio desde medios extraíbles**. En las pantallas de configuración de la BIOS, deshabilite las opciones que permiten que el equipo se inicie desde un CD-ROM, un disquete o una unidad USB extraíble. Ello impedirá que los usuarios inicien el equipo con otro sistema operativo y realicen cambios en el mismo.
- **Use contraseñas de inicio si están disponibles**. En algunos equipos, la BIOS ofrece la posibilidad de proteger mediante contraseña el inicio del equipo desde alguna unidades (en la mayoría de las BIOS se denomina “contraseña de inicio”). Por ejemplo, podría exigir una contraseña para poder iniciar el equipo utilizando la unidad de disquete, la unidad de CD-ROM o incluso el disco duro. Si no desea deshabilitar el inicio desde dispositivos extraíbles, pruebe a usar una contraseña de inicio. Si se permite que el usuario inicie el equipo usando su propio disco, podrá burlar todas las medidas de seguridad que se tomen.

Actualizaciones de software

- **Habilite las actualizaciones críticas en la herramienta Protección de discos de Windows**. Use la herramienta Protección de discos de Windows para habilitar las actualizaciones críticas y programar actualizaciones periódicas. Para obtener más información, consulte la sección "Actualizaciones críticas" del capítulo 6, "Protección de discos de Windows".
- **Compruebe si hay actualizaciones de CLUF.** Compruebe rutinariamente (al menos una vez al mes) si hay actualizaciones críticas que requieren que los usuarios acepten un CLUF. Acepte el CLUF manualmente y, a continuación, guarde los cambios en el disco usando la herramienta Protección de discos de Windows.
- **Compruebe si hay actualizaciones recomendadas**. Visite el sitio Web de Microsoft Update (http://go.microsoft.com/fwlink/?LinkId=17289; puede que la página esté en inglés) mensualmente para buscar las actualizaciones de software recomendadas de Microsoft.
- **Actualice el resto del software**. Compruebe manualmente si hay actualizaciones disponibles para el software de terceros. Lleve a cabo esta comprobación al menos una vez al mes.

Servidores de seguridad

- **Utilice un servidor de seguridad perimetral**. Los servidores de seguridad perimetrales protegen toda la red bloqueando el tráfico que no esté explícitamente permitido entre Internet y una red local.También es posible ocultar las direcciones de los equipos de una red local detrás de un servidor de seguridad, haciendo que éstos sean invisibles al exterior. Un servidor de seguridad perimetral puede ser un elemento de hardware conectado a la red o un programa como Microsoft Internet Security and Acceleration (ISA) Server.
- **Utilice un servidor de seguridad local**. Un servidor de seguridad local es un programa que se instala en un equipo para bloquear el tráfico no solicitado que llega al equipo y sale del mismo. Windows XP con Service Pack 2 (SP2) incluye un servidor de seguridad local denominado *Firewall de Windows* que se habilita de forma predeterminada al instalar SP2.

Software antivirus

- **Instale un software antivirus de confianza**. El software antivirus analiza el contenido de los mensajes de correo electrónico entrante, las descargas y los archivos que ya están en el equipo para detectar firmas de virus. Si el software encuentra un virus, lo elimina o lo pone en cuarentena.
- **Actualice el software antivirus con regularidad**. Puesto que cada mes se ponen en circulación cientos de virus, es necesario actualizar frecuentemente el software antivirus para obtener los análisis y definiciones de firma que permitan al programa detectar los virus más recientes. Si utiliza la herramienta Protección de discos de Windows, puede emplear una secuencia de comandos para descargar e instalar las actualizaciones del software antivirus y guardar automáticamente esos cambios en el disco como parte del proceso de actualizaciones críticas.

Antispyware

Nota
Algunos programas antispyware le advertirán del funcionamiento de algunos aspectos de Shared Computer Toolkit. Se trata de mensajes esperados, que se tratan en el capítulo 8, "Solución de problemas".

- **Instale un software antispyware que sea de confianza**. Este tipo de software analiza regularmente el equipo compartido en busca de spyware que pueda haberse instalado. En algunos casos, estos programas disponen de componentes que se ejecutan en segundo plano para detectar spyware antes de que se instale o realice cambios en el equipo.
- **Actualice el software antispyware con regularidad**. Al igual que ocurre con el software antivirus, debe mantener actualizado el software antispyware para que pueda detectar las últimas amenazas. Aunque el Toolkit no incluye secuencias de comandos para actualizar el software antispyware, puede emplear las técnicas que se describen en el capítulo 6, “Protección de discos de Windows”, para actualizarlo y guardar las actualizaciones en el disco.

Filtrado Web

- **Considere la posibilidad de instalar un software de filtrado de Web**. Muchas compañías ofrecen productos para filtrar el uso de Internet basándose en diversos criterios. Normalmente, estos servicios son mucho más eficaces que el Asesor de contenido integrado en Internet Explorer. Puede obtener más información sobre fabricantes de software buscando en la categoría de filtrado de contenido en el sitio Web de Windows Marketplace (http://go.microsoft.com/fwlink/?LinkId=54027; puede que la página esté en inglés).

Capítulo 8: Solución de problemas

Si tiene algún problema al instalar el Toolkit o usar cualquiera de sus herramientas, las siguientes sugerencias y soluciones pueden servir de ayuda. En este capítulo se tratan los siguientes temas:

- Instalar y desinstalar
- Software de seguridad de bloqueo de secuencias de comandos
- Administración de perfiles
- Restricciones del usuario
- Protección de discos de Windows
- Errores generales

Instalar y desinstalar

A continuación, se ofrecen una serie de soluciones para los problemas que pueden surgir al instalar y desinstalar el Toolkit.

Windows le pide que valide su copia de Windows cuando intenta abrir una herramienta del Toolkit.

Shared Computer Toolkit requiere una copia validada de Windows XP. Windows comprueba la validación antes de permitir el acceso a cualquiera de las herramientas del Toolkit. Después de la validación no volverá a ver este mensaje.

Ha intentado validar su copia de Windows en el sitio Web de Ventajas de Windows Original, pero no lo ha conseguido.

Puede obtener más información acerca del software de Microsoft original y del proceso de validación (que incluye detalles sobre la solución de problemas) en el sitio Web de software de Microsoft original (http://go.microsoft.com/fwlink/?LinkId=54028; puede que el sitio esté en inglés).

No puede validar su copia de Windows porque no tiene acceso a Internet en el equipo compartido.

Para validar su copia de Windows en Ventajas de Windows Original necesita una conexión a Internet (la operación no se puede realizar de ningún otro modo). Sólo necesitará acceso a Internet temporalmente para realizar la validación; cuando haya terminado de validar su copia, puede quitar la conexión.

Se produce un error del instalador que indica que UPHClean no está instalado o no está en ejecución, aunque sí está instalado.

El instalador comprueba que el Servicio de limpieza del subárbol de perfiles de usuario (UPHClean) está instalado y en ejecución. Utilice la herramienta Servicios de la carpeta Herramientas administrativas para asegurarse de que el servicio UPHClean está ejecutándose realmente. Si no se puede iniciar, desinstale y vuelva a instalar UPHClean usando el paquete Windows Installer (MSI).

Ha instalado el Toolkit, pero no encuentra los accesos directos de ninguna de las herramientas en el menú Inicio (sólo aparecen los de la herramienta Accesibilidad y la página Recursos en línea para el uso de equipos públicos).

Los iconos del menú Inicio para el Toolkit sólo se instalan para el administrador (en la cuenta administrativa que se ha utilizado para instalar el Toolkit). Debe iniciar la sesión como el usuario que ha instalado el Toolkit para usar las herramientas.

Después de desinstalar el Toolkit, Windows muestra, para algunos usuarios, el error que indica que no se ha encontrado la secuencia de comandos.

Para utilizar muchas funciones, por ejemplo, los temporizadores de sesión, es necesario que el Toolkit esté instalado. Para evitar este problema, quite las restricciones y desactive la herramienta Protección de discos de Windows antes de desinstalar el Toolkit. Para resolverlo, vuelva a instalar el Toolkit, elimine las restricciones y desactive Protección de discos de Windows, y después desinstálelo. Para obtener más información, consulte el capítulo 1, “Instalación”.

Después de desinstalar el Toolkit, la herramienta Protección de discos de Windows deja de impedir los cambios en el disco.

Para utilizar muchas funciones, incluida la herramienta Protección de discos de Windows, es necesario que el Toolkit esté instalado.

Después de desinstalar el Toolkit, la herramienta AutoRestart deja de funcionar.

Para utilizar muchas funciones, incluida la herramienta AutoRestart, es necesario que el Toolkit esté instalado.

Software de seguridad de bloqueo de secuencias de comandos

A continuación, se ofrecen una serie de soluciones para los problemas que pueden surgir al ejecutar software de bloqueo de secuencias de comandos.

Durante la instalación del Toolkit, el software de seguridad genera un error indicando que ha bloqueado una secuencia de comandos sospechosa o malintencionada.

Algunos programas de seguridad informan acerca de la ejecución de las secuencias de comandos del Toolkit. Si ve estas advertencias durante la instalación y el software de seguridad lo admite, debería permitir que la secuencia de comandos se ejecute.

Su software de seguridad o antispyware no le permite autorizar de forma permanente la ejecución de secuencias de comandos.

Para ejecutarse, las secuencias de comandos del Toolkit deben autorizarse permanentemente; de lo contrario, el Toolkit no funcionará. Desactive la funcionalidad de bloqueo de secuencias de comandos del software antivirus o de seguridad.

Al ejecutar muchas de las herramientas del Toolkit, el software de bloqueo de secuencias de comandos muestra mensajes emergentes que indican que se ha detectado una secuencia de comandos malintencionada.

Puesto que muchas de las herramientas del Toolkit son secuencias de comandos, cuando las utiliza, el software de bloqueo las detecta y le advierte de la posibilidad de que sean malintencionadas. Las secuencias de comandos del Toolkit no son malintencionadas. Existen dos formas de resolver este problema:

- Deshabilitar el bloqueo de secuencias de comandos en el software de seguridad mientras se usan las herramientas del Toolkit.

- Si el software de bloqueo de secuencias de comandos lo admite, configúrelo para que autorice la secuencia de comandos y no vuelva a preguntarle si desea autorizarla. Si se elige esta opción, los mensajes emergentes sólo deben aparecer la primera vez que se usa cada secuencia de comandos.
- Si es posible, autorice las secuencias de comandos antes de utilizarlas. Busque la carpeta de instalación de Shared Computer Toolkit y ejecute las secuencias de comandos individualmente para autorizarlas en el software antispyware. El capítulo 3, “Configurar perfiles de usuario locales”, incluye una lista de estas secuencias de comandos.

El software antispyware le pide su aprobación para permitir que “GetStarted.hta” se agregue al inicio de Windows.

Para que la herramienta Introducción se ejecute al iniciar, debe configurar el software antispyware para que permita agregar GetStarted.hta a la clave Run del registro.

Administración de perfiles

A continuación, se ofrecen una serie de soluciones para los problemas que pueden surgir al configurar los perfiles y las cuentas de usuario.

Windows inicia sesión automáticamente como un usuario determinado, aunque no lo ha configurado para ello.

Si sólo hay una cuenta en la pantalla de bienvenida y dicha cuenta está configurada con una contraseña en blanco, Windows inicia sesión automáticamente con esa cuenta. Se trata de una característica de Windows, no del Toolkit.

Cierre la sesión de la cuenta para iniciar una sesión con otra cuenta mostrada en la pantalla de bienvenida. Para impedir que se aplique la función **Reiniciar al cerrar sesión**, mantenga presionada la tecla MAYÚS mientras hace clic en **Cerrar sesión** y en **Aceptar** para cerrar la sesión de la cuenta restringida.

Para impedir que la pantalla de bienvenida inicie la sesión automáticamente, asigne una contraseña a la cuenta o cree otra cuenta. Para obtener más información acerca de cómo impedir que la pantalla de bienvenida inicie sesión automáticamente, consulte el artículo 305281 de Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=54464; puede que la página esté en inglés). Para obtener más información acerca de cómo iniciar una sesión en una cuenta de usuario de Windows XP, consulte el artículo 282866 de Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=54465; puede que la página esté en inglés). Los dos artículos se encuentran en el sitio Web de Ayuda y soporte técnico de Microsoft.

Otra opción es desactivar las opciones **Usar la Pantalla de bienvenida para simplificar el proceso de inicio de sesión para los usuarios** e **Impedir que los nombres de cuenta se guarden en el diálogo de inicio de sesión CTRL+ALT+SUPR**, en el paso 2 de la herramienta Introducción.

La pantalla de bienvenida aparece, pero no puede iniciar la sesión como administrador del Toolkit presionando CTRL+ALT+SUPR dos veces.

Esto ocurre cuando se ha iniciado sesión como administrador del Toolkit, el equipo ha permanecido inactivo durante demasiado tiempo y, por tanto, el administrador del Toolkit ha desaparecido de la pantalla de bienvenida.

Para obtener más información sobre el estado de la pantalla de bienvenida después de que el equipo haya permanecido inactivo, consulte el artículo 810607 del sitio Web de Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=54469; puede que la página esté en inglés).

Uno de los usuarios no aparece en la herramienta Cuentas de usuario.

Esto ocurre cuando se ha deshabilitado la cuenta con la herramienta de la línea de comandos Accounts.wsf. Habilite la cuenta y volverá a aparecer en la herramienta Cuentas de usuario.

Para obtener más información acerca de qué hacer si una cuenta no aparece en la herramienta Cuentas de usuario, consulte el artículo 297221 del sitio Web de Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=54469; puede que la página esté en inglés).

Todas o algunas de las imágenes de los usuarios que aparecen en la pantalla de bienvenida son iguales.

Para obtener más información acerca de cómo agregar o cambiar la imagen de un usuario en Windows XP, consulte el artículo 292434 de Microsoft Knowledge Base en el sitio Web de Ayuda y soporte técnico (http://go.microsoft.com/fwlink/?LinkId=54471; puede que la página esté en inglés).

Los usuarios del equipo compartido le informan de que cada vez que ejecutan un programa deben aceptar un contrato de licencia, incluso si ya lo han hecho en la sesión anterior.

Este problema puede tener dos causas: puede que el perfil esté bloqueado o que la herramienta Protección de discos de Windows esté borrando los cambios realizados por el usuario al reiniciar el equipo.

- Para prevenir este problema, ejecute los programas al menos una vez para cada cuenta de usuario antes de bloquear los perfiles o activar la herramienta Protección de discos de Windows.

- Para resolver este problema si se produce, reinicie el equipo, seleccione la opción **Guardar cambios con el siguiente reinicio** en la herramienta Protección de discos de Windows, desactive la casilla de verificación **Bloquear este perfil**, inicie una sesión como usuario, ejecute el programa y vuelva a reiniciar el equipo.

Los usuarios reciben el siguiente error: "Esta operación ha sido cancelada debido a las restricciones especificadas para este equipo. Póngase en contacto con el administrador del sistema".

Este mensaje de error aparece porque la herramienta Restricciones del usuario está configurada para bloquear el acceso a la unidad C:, y el perfil del usuario está almacenado endicha unidad. El error aparece cuando el Explorador de Windows intenta obtener acceso a carpetas especiales (como Mis documentos y Mi música) que están ubicadas en esa unidad. Para resolver este problema, quite el acceso

directo al Explorador de Windows del menú Inicio y sustitúyalo por un acceso directo a Mi PC.

El botón Crear perfil no aparece en la herramienta Administrador de perfiles.

El perfil de usuario ya existe. Elimínelo si desea crear un nuevo perfil de usuario.

El botón Eliminar perfil no aparece en la herramienta Administrador de perfiles.

El perfil de usuario no existe; primero debe crearlo.

Los iconos que faltan en la carpeta del menú Inicio del perfil de un usuario aparecen en el menú Inicio de dicho usuario.

Windows XP crea el menú Inicio de los usuarios combinando los iconos de las carpetas de menú Inicio del perfil Todos los usuarios con el perfil individual de cada usuario. Lo más probable es que los iconos del menú Inicio del usuario se encuentren en la carpeta del menú Inicio de Todos los usuarios.

Ha instalado un nuevo programa y, durante la instalación, ha seleccionado la opción para que el programa esté disponible para todos los usuarios. Sin embargo, el acceso directo no aparece en el menú Inicio de algunos usuarios.

Los programas de instalación suelen instalar accesos directos a la carpeta del menú Inicio del perfil Todos los usuarios. Es probable que las cuentas en las que no aparecen los accesos directos estén restringidas por haber activado la casilla de verificación **Impedir que los programas de la carpeta Todos los usuarios aparezcan en el menú Inicio** en Restricciones del usuario.

Cuando crea un nuevo perfil de usuario, éste desaparece al reiniciar el equipo.

La herramienta Protección de discos de Windows borra los cambios realizados en el disco duro cuando el equipo se reinicia. Debe usar Protección de discos de Windows y seleccionar la opción **Guardar cambios con el siguiente reinicio**.

Algunos programas del equipo compartido no se pueden ejecutar con una cuenta de usuario limitada, ya que requieren una cuenta administrativa.

Aunque no es un escenario recomendado, es posible restringir una cuenta administrativa para que los usuarios puedan ejecutar dichos programas. Para obtener más información acerca de este tema, consulte la sección “Restringir una cuenta administrativa compartida” del capítulo 9, “Escenarios avanzados”.

Restricciones del usuario

A continuación, se ofrecen una serie de soluciones para los problemas que pueden surgir al utilizar la herramienta Restricciones del usuario.

Ha usado la herramienta Restricciones del usuario para cambiar la configuración, pero después de reiniciar el equipo, los cambios desaparecen.

La herramienta Protección de discos de Windows borra los cambios realizados en el disco duro cuando el equipo se reinicia. Debe usar Protección de discos de Windows para seleccionar la opción **Guardar cambios con el siguiente reinicio** o crear un perfil de usuario en una partición persistente.

Después de configurar las restricciones de usuario, la herramienta Accesibilidad y algunos iconos de programa no aparecen en el menú Inicio.

Si se selecciona la opción **Impedir que los programas de la carpeta Todos los usuarios aparezcan en el menú Inicio**, los iconos que se colocan en la carpeta del menú Inicio

de Todos los usuarios se bloquean en los menús Inicio de los usuarios restringidos. Para que estén disponibles, puede copiar los iconos en la carpeta del menú Inicio del usuario.

Una vez configuradas las restricciones de usuario, no puede ejecutar algunos accesos directos.

Si ha seleccionado la configuración de restricción de software **Únicamente permitir que se ejecute software en las carpetas Archivos de programa y Windows**, no se permitirá que los usuarios ejecuten accesos directos a programas que no se encuentren en la carpeta Archivos de programa o en la carpeta Windows. Mueva el programa a una de estas carpetas para permitir que se ejecute.

Los usuarios no pueden cambiar la configuración en Windows aunque la herramienta Protección de discos de Windows está desactivada.

Lo más probable es que haya utilizado la Restricciones del usuario para bloquear el perfil de usuario.

Establece la restricción para impedir que se ejecuten los programas de Microsoft Office, pero los usuarios siguen ejecutándolos.

Lo más probable es que Microsoft Office no esté instalado en la ubicación predeterminada. Esta restricción impide que se ejecuten los programas de la carpeta C:\Archivos de programa\Microsoft Office. Si Microsoft Office está instalado en otra carpeta, la restricción no funcionará.

Algunos juegos (como Microsoft Halo® y Activision Call of Duty) y otros programas que utilizan la protección contra copia no funcionan correctamente cuando se establecen restricciones de software.

Las restricciones de software pueden impedir que se ejecuten algunos juegos protegidos contra copia. Para usar estos juegos, desactive la casilla de verificación **Restricciones de software**. Tenga presente que al desactivar las restricciones de software debilitará considerablemente la seguridad del equipo compartido.

Los usuarios no ven la página Web que ha configurado desde Active Desktop para las cuentas restringidas.

Las restricciones recomendadas impiden que Active Desktop funcione; esto ocurre de forma intencionada.

Para mostrar una página Web que contenga información para todos los usuarios y que éstos la vean al iniciar sesión, agregue Internet Explorer a la carpeta Inicio de cada usuario y diríjalo a la página Web.

Si cambia la página principal de Internet Explorer para un perfil de usuario bloqueado, el usuario recibe un mensaje procedente del software antispyware relacionado con dicha página.

Algunos programas de seguridad emiten esta advertencia cuando la herramienta Restricciones del usuario modifica la página principal de Internet Explorer.

Para evitar este error, cambie la página principal desde Internet Explorer antes de bloquear el perfil.

Protección de discos de Windows

A continuación, se ofrecen una serie de soluciones para los problemas que pueden surgir al usar la herramienta Protección de discos de Windows.

No puede activar la herramienta Protección de discos de Windows.

Asegúrese de que el equipo está preparado para usar la herramienta Protección de discos de Windows. Para obtener más información, consulte el capítulo 2, “Preparar el disco para Protección de discos de Windows”.

Está usando un disco dinámico para el volumen de Windows y la herramienta Protección de discos de Windows le notifica el siguiente error: “Este equipo no es compatible con Protección de discos de Windows...”.

La herramienta Protección de discos de Windows sólo admite discos básicos. En los equipos cuyo volumen de Windows se encuentra en un disco dinámico no es posible utilizar dicha herramienta. Deberá reinstalar Windows usando un disco básico para la partición de Windows.

Windows muestra un mensaje indicándole que el filtro de escritura mejorado está confirmando cambios en el disco.

La aparición de este mensaje forma parte del funcionamiento esperado; se produce cuando se utiliza la opción **Guardar cambios con el siguiente reinicio** de la herramienta Protección de discos de Windows.

Al iniciar, Windows muestra un mensaje de advertencia indicando que ha terminado de instalar nuevos dispositivos.

Este mensaje vuelve a aparecer cada vez que se reinicia.

Este problema puede producirse cuando Windows realiza cambios en el sistema después de activar la herramienta Protección de discos de Windows. Debe abrir Protección de discos de Windows, seleccionar la opción **Guardar cambios con el siguiente reinicio** y después reiniciar el equipo.

Windows no se inicia y aparece una pantalla negra.

Este problema puede producirse si una utilidad de partición de terceros daña el registro de inicio maestro, las tablas de partición, el sector de inicio o el archivo NTLDR. Para obtener más información acerca de problemas relacionados con el inicio de Windows XP y la pantalla negra, consulte el artículo 314503 de Microsoft Knowledge Base en el sitio de Ayuda y soporte técnico de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54486; puede que la página esté en inglés).

Al iniciar una sesión en el equipo compartido, Windows muestra un mensaje en el que se le notifica que debe aceptar un contrato de licencia para realizar una actualización crítica. Incluso si lo acepta, vuelve a ver el mismo mensaje cada vez que reinicia el equipo e inicia una sesión.

La herramienta Protección de discos de Windows borra los cambios realizados en el disco duro cuando el equipo se reinicia, incluida la instalación de la actualización. La característica de actualizaciones programadas de Protección de discos de Windows no puede aceptar automáticamente el contrato de licencia. Debe reiniciar el equipo, iniciar una sesión como administrador, configurar la herramienta seleccionando la opción **Guardar cambios con el siguiente reinicio**, instalar la actualización y después reiniciar el equipo.

Cuando ejecuta la herramienta Protección de discos de Windows, Windows le pide que reinicie el equipo.

Para activar la herramienta Protección de discos de Windows es necesario reiniciar el equipo una vez tras finalizar la instalación; la herramienta se ha diseñado de esta forma.

Ha modificado las particiones o ha cambiado el tamaño de las mismas, o bien ha agregado un nuevo disco duro en el equipo. En consecuencia, la herramienta Protección de discos de Windows ha dejado de funcionar.

La herramienta Protección de discos de Windows realiza un seguimiento de la ubicación física del disco y la partición de Windows. Si se cambian estos parámetros, la herramienta deja de funcionar. Desactive la herramienta, elimine la partición de protección y vuelva a activarla.

La herramienta Protección de discos de Windows parece estar protegiendo correctamente los archivos del directorio de Windows, pero no protege la partición del sistema. En el equipo compartido, la partición de inicio y la partición del sistema están separadas.

En la mayoría de los equipos que ejecutan Windows XP, hay una única partición de disco para la partición de inicio y la partición del sistema. En estos casos, Protección de discos de Windows protege las particiones de inicio y del sistema. Si la partición del sistema y la de inicio no se encuentran en la misma partición de disco, la herramienta sólo protege la de inicio, ya que ésta contiene el directorio %Windir%.

Al activar la herramienta Protección de discos de Windows, recibe un mensaje de advertencia en el que se le notifica que la hibernación no funcionará si activa dicha herramienta.

La herramienta Protección de discos de Windows permite que se escriban o se modifiquen archivos en la partición de Windows y que éstos aparezcan como modificados. Cuando el sistema hiberna, el archivo Hiberfil.sys que almacena el contenido de la memoria RAM del sistema durante la hibernación no se escribe en la partición de Windows. Al reiniciar el equipo, el sistema no detecta el archivo de hibernación y se inicia de la manera habitual.

Cuando la herramienta Protección de discos de Windows está activada, recibe un error de escritura retrasada.

Estos errores de escritura se producen porque la partición de protección está llena. Esto puede ocurrir al grabar un CD o un DVD, ya que antes de empezar la grabación en el disco, se crea una imagen completa del mismo en el equipo.

Si los clientes necesitan grabar un CD o un DVD, o realizar cualquier otro tipo de operación que requiera una utilización intensiva del disco, elimine la partición de protección, aumente el volumen de espacio en disco no asignado y después vuelva a activar la herramienta Protección de discos de Windows. Para realizar estas operaciones, es necesario asegurarse de que hay suficiente espacio en el disco.

Si necesita grabar un CD o un DVD, basta con desactivar Protección de discos de Windows, realizar la grabación y volver a activar la herramienta.

También podría recibir un error de escritura retrasada si utiliza la opción **Conservar cambios indefinidamente**. Si el problema le impide iniciar sesión o tener acceso a la herramienta Protección de discos de Windows, presione F8 antes del inicio de Windows para obtener acceso a la pantalla **Opciones de inicio avanzadas**. Seleccione la opción **Modo de restauración del filtro de escritura mejorado (restaura un nivel)** para indicar a la herramienta Protección de discos de Windows que borre los cambios conservados en el disco.

Ha agregado un perfil para un nuevo usuario, pero después de reiniciar el equipo, el perfil desaparece.

En su configuración predeterminada, la herramienta Protección de discos de Windows descarta los cambios realizados en el disco del sistema cada vez que el equipo se reinicia. Para conservar el perfil de usuario, configure la herramienta Protección de discos de Windows con la opción **Guardar cambios con el siguiente reinicio**. Con esta configuración, el perfil de usuario se guardará en el disco y estará disponible después de reiniciar.

Ha instalado un nuevo programa en el equipo. Al reiniciarlo, los iconos se conservan, pero el nuevo programa ha desaparecido.

Si el perfil de usuario está almacenado en una partición persistente, se conservarán los iconos de los programas instalados incluso si éstos se eliminan mediante la opción **Borrar cambios en cada reinicio** de la herramienta Protección de discos de Windows. Para evitar este problema, seleccione la opción **Guardar cambios con el siguiente reinicio** antes de reiniciar el equipo.

Ha usado una herramienta de partición de discos para crear el espacio de la partición de protección y el sistema ya no se reinicia.

Desafortunadamente, Microsoft no puede ofrecer soporte técnico para las herramientas de partición de discos de terceros. Póngase en contacto con el fabricante de la herramienta de partición a fin de obtener ayuda para resolver este problema.

Cuando intenta ejecutar la herramienta Protección de discos de Windows o la herramienta Introducción, recibe un mensaje en el que se le notifica que su software de bloqueo de secuencias de comandos está bloqueando WDP.CMD.

Si el software de bloqueo de secuencias de comandos bloquea WDP.CMD, el Toolkit muestra un mensaje de advertencia en el que se pide al usuario que permita su ejecución. Autorice o permita la ejecución de WDP.CMD en su programa de bloqueo de secuencias de comandos para garantizar que la herramienta Protección de discos de Windows pueda proporcionar información precisa.

Cuando intenta administrar las particiones utilizando Norton PartitionMagic, el programa devuelve un error.

No intente cambiar ninguna partición mientras esté activada la herramienta Protección de discos de Windows. Desactive la herramienta, reinicie el equipo, elimine la partición de protección mediante Administración de discos de Windows y, a continuación, cambie las particiones con PartitionMagic. Si tiene intención de volver a utilizar la herramienta Protección de discos de Windows, asegúrese de mantener suficiente espacio no asignado en el disco para la creación de una partición de protección.

Recibe un mensaje de error en el registro de eventos del sistema en el que se le notifica que se ha producido un error en la configuración del archivo de paginación de un volcado (evento nº 49).

Se trata de un funcionamiento esperado que no afecta al uso normal del equipo. El sistema informa de este error porque no puede confirmar los cambios de un archivo de paginación en la partición de Windows y no puede iniciar las rutinas de volcado de memoria. Si desea corregir este problema, mueva el archivo de paginación a un disco persistente. Para obtener más información, consulte la sección "Mejorar el rendimiento de la herramienta Protección de discos de Windows" del capítulo 6, "Protección de discos de Windows".

No aparece el elemento emergente que indica que la protección de discos de Windows está activada

Este elemento emergente sólo aparecerá si la herramienta Protección de discos de Windows está activada y si la herramienta Introducción no está configurada para abrirse automáticamente. Desactive la casilla de verificación **Mostrar la Introducción al inicio** y asegúrese de que la herramienta Protección de discos de Windows esté activada.

Errores generales

A continuación, se ofrecen una serie de soluciones para los errores o problemas que pueden surgir al usar Shared Computer Toolkit.

A veces el desplazamiento automático es muy lento en la ventana de la herramienta Introducción.

Es probable que se deba a un problema del controlador de vídeo para el adaptador de gráficos del equipo compartido. Asegúrese de que está usando el controlador más reciente disponible para el dispositivo.

Cuando intenta ejecutar cualquiera de las herramientas del Toolkit, recibe un mensaje de error de Microsoft HTML Application Host en relación con el archivo LegitCheckControl.DLL.

El archivo LegitCheckControl.DLL está dañado y no puede validar su copia de Windows, así que no permite que se ejecute ninguna de las herramientas. Para corregir este problema, elimine el archivo LegitCheckControl.DLL de la carpeta Windows\System32. Elimine la herramienta de validación de Ventajas de Windows Original de la carpeta Windows\Downloaded Program Files. Vuelva a ejecutar la herramienta y lleve a cabo los pasos de validación de Windows necesarios para reactivar el Toolkit.

Una de las herramientas gráficas del Toolkit no se inicia.

Esto puede ocurrir si se fuerza el cierre de una de las herramientas mientras está procesando datos. Use el Administrador de tareas para terminar el proceso denominado mshte.exe.

La herramienta Introducción muestra un error que sugiere que las restricciones de software del equipo no se aplican a las cuentas administrativas.

Esta advertencia aparece sólo en los equipos cuyas directivas de restricción de software se han configurado previamente para no que no se apliquen a los administradores. La clave **PolicyScope** define si las restricciones de software se aplican sólo a los usuarios o también a los administradores. Si esta clave se ha establecido anteriormente en “sólo usuarios”, la instalación del Toolkit no aplicará las restricciones de software a los administradores. Esto permite garantizar que las restricciones de software anteriores no se apliquen involuntariamente a las cuentas administrativas.

Para obtener más información, consulte la página del sitio Web de Microsoft acerca del uso de directivas de restricción de software para proteger el equipo contra programas no autorizados (http://go.microsoft.com/fwlink/?LinkId=14508; puede que la página esté en inglés).

Capítulo 9: Escenarios avanzados

En esta sección del manual se describen una serie de escenarios avanzados que pueden adaptarse a sus necesidades de administración en un entorno de equipos compartidos. Estas técnicas están dirigidas a operadores expertos en la administración de Windows XP. En concreto, esta sección contiene información acerca de los siguientes temas:

- Almacenar datos de usuario persistentes
- Instalación rápida de software para un usuario limitado
- Configurar un menú Inicio de usuario para no utilizar el perfil Todos los usuarios.
- Restringir una cuenta administrativa compartida
- Bloquear los controles de Microsoft® ActiveX® en Internet Explorer
- Utilizar un filtrado de sitios sencillo para controlar el acceso a Internet
- Usar una secuencia de comandos centralizada para actualizaciones de cliente comunes
- Restringir el acceso de los niños al equipo familiar
- Automatizar las restricciones del usuario mediante Restrict.wsf
- Crear un perfil obligatorio para varios usuarios
- Clonar o crear una imagen de un equipo protegido mediante el Toolkit

Almacenar datos de usuario persistentes

Puede que desee permitir que los usuarios puedan personalizar su perfil o almacenar datos en algunos equipos compartidos y que la herramienta Protección de discos de Windows no descarte estos cambios al reiniciar. Existen dos formas de almacenar datos de usuario persistentes:

- Crear una partición separada de la partición de Windows que protege la herramienta Protección de discos de Windows. Usar esta partición separada para almacenar perfiles y otros datos de los usuarios. La ventaja de este método es que permite crear perfiles de usuario persistentes sin que ello impida seguir protegiendo el equipo compartido con la herramienta Protección de discos de Windows.
- Usar una unidad USB o una ubicación de red para almacenar datos de usuario persistentes. Este método permite a los usuarios guardar datos, pero no proporciona un método eficaz para almacenar perfiles de usuario persistentes.

Almacenar datos de usuario persistentes en una partición separada

Nota
La partición persistente puede ubicarse en el mismo disco físico que la partición de protección o en otro disco.

Puede crear una nueva partición para almacenar los datos persistentes utilizando la herramienta Administración de discos de Windows XP. Para crear una nueva partición de este modo, es necesario disponer de suficiente espacio no asignado en el disco y que dicha partición no ocupe el espacio sin asignar necesario para utilizar la herramienta Protección de discos de Windows.Una vez creada la nueva partición, puede utilizar la herramienta Administrador de perfiles para crear los perfiles de usuario en esa partición, en lugar de crearlos en la ubicación predeterminada de la partición de Windows.

Crear una nueva partición con la herramienta Administración de discos

Puede usar la herramienta Administración de discos de Windows XP para crear una nueva partición en el espacio no asignado.

Para usar la herramienta Administración de discos y crear una nueva partición:

1. En la ventana Administración de discos, haga clic con el botón secundario en el espacio sin asignar del disco que desea emplear para crear la partición y, a continuación, haga clic en **Nueva partición**.
2. En la página de bienvenida del Asistente para partición nueva, haga clic en **Siguiente**.
3. En la página Seleccionar el tipo de partición del asistente, acepte la opción predeterminada de la **partición primaria** y, a continuación, haga clic en **Siguiente**.
4. En la página Especificar el tamaño de la partición del asistente, especifique la cantidad de espacio no asignado que desea emplear para crear el nuevo volumen. Asegúrese de dejar suficiente espacio sin asignar para cubrir las necesidades mínimas de la herramienta Protección de discos de Windows (como mínimo el 10% del tamaño de la partición de Windows o 1 GB, el mayor de los dos valores).
5. En la página Asignar letra de unidad o ruta de acceso del asistente, acepte la recomendación predeterminada de asignar una letra de unidad y, a continuación, haga clic en **Siguiente**.
6. En la página Formatear la partición del asistente, acepte la configuración predeterminada para crear la nueva partición, haga clic en **Siguiente** y, a continuación, en la página final del asistente, haga clic en **Finalizar**.

Crear perfiles persistentes con la herramienta Administrador de perfiles

La herramienta Administrador de perfiles permite crear y eliminar perfiles en las cuentas de usuario existentes. También puede crear los perfiles en particiones alternativas.

Para usar la herramienta Administrador de perfiles y crear o eliminar perfiles de usuario persistentes:

1. Inicie sesión como administrador del Toolkit.
2. Haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Administrador de perfiles**.
3. En el Administrador de perfiles (véase la ilustración siguiente), haga clic en **Seleccionar una cuenta**.
4. En el cuadro de diálogo **Seleccione una cuenta**, haga clic en la cuenta de usuario que desea administrar.
5. En la casilla **Contraseña de usuario**, escriba la contraseña de la cuenta de usuario.
6. Lleve a cabo una de las siguientes operaciones:
   - Para crear un perfil para la cuenta de usuario, seleccione la unidad en la que ha creado la partición persistente desde el menú desplegable **Ubicación del perfil** y, a continuación, haga clic en **Crear perfil**. Si no ve este botón, es porque ya hay un perfil de usuario para esa cuenta.
   - Para eliminar un perfil de usuario de la cuenta, haga clic en **Eliminar perfil**. Si no ve este botón, es porque aún no existe ningún perfil de usuario para la cuenta.
   - Para abrir la ventana Cuentas de usuario a fin de crear y administrar cuentas de usuario locales, haga clic en **Administrar usuarios**.
7. Cuando haya terminado, haga clic en **Cerrar**.

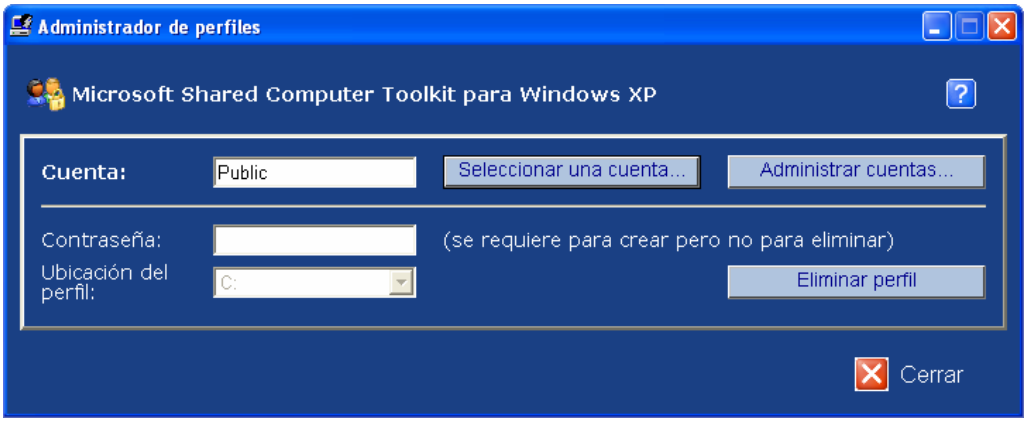

Figura 9.1 *Usar la herramienta Administrador de perfiles para crear o eliminar perfiles de usuario*

Usar unidades USB extraíbles o ubicaciones de red

Nota
Si los usuarios comparten una unidad USB o una ubicación de red, no hay forma de mantener la privacidad de los documentos. Todos los usuarios de la misma cuenta compartida podrán ver los archivos de los demás.

Windows XP ofrece la posibilidad de redirigir la carpeta Mis documentos (que normalmente se almacena dentro del perfil de un usuario) a otra ubicación. Si usa la herramienta Protección de discos de Windows, pero desea seguir ofreciendo a los usuarios la posibilidad de guardar documentos, puede redirigir las carpetas Mis documentos a una partición persistente, a una unidad extraíble (por ejemplo, una unidad USB) o a una ubicación de red.

Para redirigir la carpeta Mis documentos de un usuario a una unidad USB:

1. Reinicie el equipo para borrar los cambios más recientes realizados en el disco.
2. Inicie sesión como administrador del Toolkit.
3. Si la herramienta Protección de discos de Windows está activada, iníciela, haga clic en **Guardar cambios con el siguiente reinicio** y, a continuación, haga clic en **Aceptar**.
4. Inicie la herramienta **Restricciones del Usuario**.
5. Deshabilite las restricciones de la cuenta de usuario cuya carpeta Mis documentos desea redirigir. Este paso es necesario si las restricciones impiden que el usuario haga clic con el botón secundario.
6. Cierre la sesión y, a continuación, inicie sesión con la cuenta de usuario cuya carpeta Mis documentos desea redirigir.
7. Inserte una unidad USB y espere a que Windows la reconozca.
8. Haga clic en **Inicio**, haga clic con el botón secundario en **Mis documentos** y, después, haga clic en **Propiedades**.
9. En el cuadro de diálogo **Propiedades de Mis documentos**, haga clic en **Mover**.
10. En el cuadro de diálogo **Seleccione un destino**, haga clic en la unidad USB o la ubicación de red y, a continuación, en **Aceptar**.
11. En el cuadro de diálogo **Propiedades de Mis documentos**, haga clic en **Aceptar**.
12. Windows mostrará el cuadro de diálogo **Mover documentos**. Haga clic en **Sí** para mover los documentos o en **No** para dejar los documentos existentes en la ubicación anterior.
13. Cierre la sesión e inicie otra como administrador del Toolkit. Si ha deshabilitado alguna restricción en el paso 1, vuelva a habilitar esas restricciones ahora.

14. Reinicie el equipo para permitir que la herramienta Protección de discos de Windows guarde los cambios y vuelva a la opción predeterminada, **Borrar cambios en cada reinicio**.
15. Inicie sesión como usuario para probar la carpeta Mis documentos y las restricciones aplicadas.

Instalación rápida de software para un usuario restringido

A menudo, es necesario instalar software temporalmente para un usuario. Puede que este software sólo se utilice en una única sesión, o podría ser algo que desea agregar de modo permanente, pero debe instalarlo rápidamente y con el menor trastorno posible para el cliente.

Puede utilizar el cambio rápido de usuario para cambiar rápidamente a la cuenta de administrador del Toolkit e instalar el programa. Después podrá volver a la sesión del usuario restringido sin cerrar la sesión de usuario.

Nota
Si ha seleccionado la opción **Deshabilitar cualquier acceso directo de teclado que use la tecla con el logotipo de Windows** en Restricciones del usuario, la combinación de teclas logotipo de Windows + L no funcionará.

Para usar el cambio rápido de usuario e instalar software temporalmente para un usuario limitado:

1. Presione la tecla del logotipo de Windows + L para cambiar a la pantalla de bienvenida de Windows.
2. Inicie sesión como administrador del Toolkit.
3. Instale y configure el nuevo software. Asegúrese de que el icono se coloca en el menú Inicio del usuario o en el menú Inicio de Todos los usuarios.
4. Si el software requiere reiniciar, use la herramienta Protección de discos de Windows y establezca la opción de reinicio en **Conservar cambios por un reinicio**. Reinicie el equipo.
5. Cierre la sesión del administrador del Toolkit e inicie sesión como usuario limitado para reanudar la sesión inicial.

A menos que el software requiera reiniciar para completar la instalación, ya deberá estar disponible en la sesión del usuario limitado.

Configurar un menú Inicio de usuario para no utilizar el perfil Todos los usuarios.

Una de las restricciones opcionales disponibles en la herramienta Restricciones del usuario permite impedir que Windows muestre los accesos directos del menú Inicio del perfil Todos los usuarios en el menú Inicio de los perfiles de usuario individuales. Esta restricción proporciona un control óptimo sobre los elementos que aparecen en los menús Inicio, pero también requiere algo más de trabajo para su correcta configuración. Concretamente, deberá realizar dos operaciones adicionales:

- Si configura un perfil de usuario con esta restricción, en el menú Inicio del mismo no aparecerá ningún acceso directo de manera predeterminada. Debe usar el Explorador de Windows para copiar los accesos directos que desee del menú Inicio del perfil Todos los usuarios.En el capítulo 3, “Administración de perfiles”, se describen los pasos para obtener acceso a estas carpetas en el Explorador de Windows.

- Si instala nuevos programas en el equipo compartido, el programa de instalación creará accesos directos en el menú Inicio del perfil Todos los usuarios.Para que dichos accesos directos aparezcan en los menús Inicio de los usuarios individuales, debe copiar en éstos los accesos directos del menú Inicio de Todos los usuarios. Asimismo, si la herramienta Protección de discos de Windows está activada, necesitará configurarla para conservar los cambios cuando copie los accesos directos. Para obtener más información, consulte el capítulo 6, “Protección de discos de Windows”.

Restringir una cuenta administrativa compartida

Nota
Para obtener más información acerca de los programas de terceros que no funcionan con cuentas de usuario limitadas, consulte el artículo 307091 de Microsoft Knowledge Base en el sitio Web de Ayuda y soporte técnico de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54487; puede que la página esté en inglés).

Importante
Aunque el Toolkit puede ayudar a restringir una cuenta administrativa, no puede eliminar todos los riesgos para la seguridad asociados al uso de dicha cuenta.

Microsoft recomienda encarecidamente que a los usuarios del equipo compartido sólo se les permita iniciar sesión con cuentas de usuario limitadas. Con ello se garantiza un acceso limitado a los recursos del equipo y un entorno más seguro. Al utilizar cuentas limitadas, los usuarios no pueden obtener acceso a las herramientas administrativas y privilegios que les permitirían insertar cambios no deseados en los programas y el sistema operativo.

No obstante, existen algunos programas de terceros que no se han diseñado para ejecutarse correctamente con una cuenta de usuario limitada y que no cumplen los requisitos del logotipo "Diseñado para Windows XP". En estos casos, el usuario debe iniciar sesión con una cuenta administrativa compartida para poder ejecutar los programas. Aunque lo mejor es evitar este tipo de programas y utilizar sólo cuentas de usuario limitadas, no siempre es posible, y puede que en algunos casos sea necesario permitir que los usuarios inicien sesiones con cuentas administrativas. Este escenario es muy frecuente en entornos como los cibercafés donde se usan juegos de Internet, ya que existen muchos juegos que se han concebido para que varios usuarios jueguen conectados a una red, o a través de Internet, y para ello se necesitan cuentas administrativas.Algunos programas educativos más antiguos presentan problemas similares.

Si tiene programas con esta limitación de cuentas administrativas, tome las siguientes medidas:

- Averigüe si el software se puede actualizar a una versión que funcione correctamente con privilegios de cuenta de usuario limitada en Windows XP.
- Averigüe si el software se puede sustituir por otro producto que funcione correctamente con privilegios de cuenta de usuario limitada en Windows XP.
- Investigue la posibilidad de eliminar el software del entorno con un impacto limitado en las necesidades del negocio.

Si no es posible tomar ninguna de estas medidas, puede ser necesario permitir que algunos usuarios utilicen cuentas administrativas para usar determinados programas.

Si el entorno requiere cuentas administrativas compartidas, puede utilizar la herramienta Protección de discos de Windows en combinación con la herramienta Restricciones del usuario para restringir las actividades de dichas cuentas y mejorar la seguridad del equipo. Sin embargo, ninguna solución le ofrecerá un 100% de protección contra el uso indebido de las cuentas administrativas.

Para restringir una cuenta administrativa compartida:

1. Inicie sesión como administrador del Toolkit.
2. Haga clic en **Inicio**, seleccione **Todos los programas**, **Microsoft Shared Computer Toolkit** y, a continuación, haga clic en **Restricciones del usuario**.
3. En la ventana **Restricciones del usuario**, haga clic en **Seleccionar un perfil**.
4. En la ventana **Seleccione el perfil que desea restringir**, haga clic en la cuenta de administrador compartida que desea restringir.
5. Active la casilla de verificación **Bloquear este perfil**.
6. En la ventana **Restricciones del usuario**, en la sección **Configuración general**, haga clic en **Seleccionar unidades.**
7. En la ventana **Seleccione las unidades que desea restringir**, haga clic en **Restringir todas**. Haga clic en **Aceptar**.
8. En la ventana Restricciones del usuario, seleccione la casilla de verificación **Restricciones recomendadas para cuentas compartidas**. Asegúrese de seleccionar todas las restricciones, ya que si deja alguna restricción inactiva, abrirá una puerta que podrá explotar cualquier usuario malintencionado de la cuenta administrativa.
9. En Restricciones adicionales del menú Inicio, active las casillas de verificación **Impedir que los programas de la carpeta Todos los usuarios aparezcan en el menú Inicio** y **Quitar el icono Ayuda y soporte técnico**.
10. En Restricciones adicionales de software, seleccione las casillas de verificación **Restringir Notepad y WordPad** e **Impedir que se ejecuten los programas de Microsoft Office**.Con ello, se evitará que el administrador restringido modifique archivos de procesamiento por lotes y secuencias de comandos críticas para burlar las medidas de seguridad.
11. Haga clic en **Aceptar** para aplicar las restricciones y cerrar la herramienta Restricciones del usuario.

Bloquear los controles ActiveX en Internet Explorer

Internet Explorer ofrece un método de control basado en zonas de seguridad que incluye la posibilidad de bloquear los controles ActiveX.Las zonas de seguridad contienen listas de sitios Web que requieren una configuración de seguridad similar. Hay cuatro zonas de seguridad:

- **Internet**. Contiene todos los sitios Web que no se han asignado a otras zonas.
- **Intranet local**. Contiene todos los sitios Web que se encuentran dentro de la red local. De manera predeterminada, esta zona incluye todos los sitios que traspasan el servidor proxy (si se está utilizando).
- **Sitios de confianza**. Contiene los sitios Web que se consideran seguros. De manera predeterminada no hay ningún sitio en esta zona.
- **Sitios restringidos**. Contiene los sitios Web que podrían ser dañinos. De manera predeterminada no hay ningún sitio en esta zona.

Importante
Si bloquea los controles ActiveX, tendrá problemas para ver algunas páginas Web.

Aunque por regla general es aconsejable mantener la configuración de zonas de seguridad predeterminada, puede personalizar el nivel de seguridad de cada sitio si ésta no es adecuada para un usuario.De manera predeterminada, en la zona de seguridad de Internet, se impide la descarga e instalación de controles ActiveX no firmados. Para mejorar esta configuración de seguridad, puede personalizar la zona de seguridad de Internet.

Para bloquear los controles ActiveX en Internet Explorer:

1. Inicie sesión como administrador del Toolkit.
2. Si es necesario, quite las restricciones de la cuenta de usuario en la que desea bloquear los controles ActiveX y configure la herramienta Protección de discos de Windows con la opción **Guardar cambios con el siguiente reinicio**.
3. Inicie una sesión como el usuario para el que desea bloquear los controles ActiveX.
4. Inicie Internet Explorer
5. En Internet Explorer, en el menú **Herramientas**, haga clic en **Opciones de Internet**.
6. En el cuadro de diálogo **Opciones de Internet**, haga clic en la ficha **Seguridad**.
7. Haga clic en la zona de seguridad Internet y, a continuación, haga clic en **Nivel personalizado**.
8. En el cuadro de diálogo Configuración de seguridad, deshabilite todas las opciones de la sección **Controles y complementos de ActiveX** de la lista.
9. Vuelva a iniciar sesión como administrador del Toolkit, habilite las restricciones del usuario y vuelva a reiniciar el equipo.

Utilizar un filtrado de sitios sencillo para controlar el acceso a Internet

La herramienta Restricciones del usuario ofrece una manera de deshabilitar el acceso a Internet. Aunque en algunos equipos compartidos sea necesario habilitar el acceso a Internet, pueden limitarse los sitios a los que un usuario puede conectarse.

Utilice el siguiente procedimiento para limitar el acceso a Internet de unos cuantos sitios seleccionados. Este procedimiento sólo funciona en entornos que no utilizan un servidor proxy.

Para usar un filtrado de sitios sencillo en Internet Explorer:

1. Inicie sesión como administrador del Toolkit.
2. Abra la herramienta Restricciones del usuario y seleccione el perfil de usuario que desea limitar.
3. En **Restricciones opcionales**, expanda **Restricciones adicionales de Internet Explorer** y active la casilla de verificación **Impedir el acceso a Internet desde Internet Explorer**.
4. La opción Proxy cambiará a NoInternetAccess, lo que deshabilita el acceso de todos los sitios, excepto los enumerados en el cuadro **Excepciones de proxy**.
5. En el cuadro **Excepciones de proxy**, indique los sitios que va a permitir que examine el usuario. En la lista de sitios permitidos, puede utilizar caracteres comodín, como *.microsoft.com. Use un signo de punto y coma (;) como delimitador entre sitios.

6. Haga clic en **Aceptar**.
7. Inicie sesión como el usuario restringido y use Internet Explorer para confirmar que los sitios elegidos son los únicos disponibles.
8. Inicie sesión como administrador del Toolkit.
9. Configure la herramienta Protección de discos de Windows en **Guardar cambios con el siguiente reinicio** y reinicie el equipo para guardar los cambios.

Si se necesita un sitio más avanzado o servicios de filtrado de contenido, busque en Windows Marketplace un producto de terceros que cumpla sus requisitos (http://go.microsoft.com/fwlink/?LinkId=374; puede que la página esté en inglés).

Usar una secuencia de comandos centralizada para actualizaciones de cliente comunes

Si cuenta con varios equipos compartidos en red, puede que en ocasiones sea necesario aplicar una actualización o realizar una instalación en todos los equipos compartidos aunque la herramienta Protección de discos de Windows esté activada. Para resolver este problema, puede utilizar la opción **Secuencia de comandos para otros** de Protección de discos de Windows para llamar a una secuencia de comandos común desde una ubicación de red.

Por ejemplo, podría mantener una secuencia de comandos denominada Sharedupdate.bat en una carpeta compartida en la red. Por lo general, esta secuencia de comandos se conservaría vacía (un documento en blanco). Todos los días durante el proceso de actualización normal, los equipos compartidos ejecutarían esta secuencia de comandos vacía sin consecuencias. Cuando desee que los equipos compartidos ejecuten una secuencia de comandos (por ejemplo, instalar un nuevo programa), podría simplemente agregar la secuencia de comandos correspondiente al archivo Sharedupdate.bat. Tras el ciclo de actualización normal, cuando todos los equipos compartidos hayan ejecutado la secuencia de comandos, se podría devolver el archivo Sharedupdate.bat a su estado vacío.

Restringir el acceso de los niños al equipo familiar

Aunque no es el propósito planteado del Toolkit, una interesante posibilidad que éste ofrece es la de restringir las acciones de otros tipos de usuario en otros entornos. Uno de esos entornos es un equipo doméstico utilizado por niños.

En un equipo doméstico, la herramienta Restricciones del usuario simplifica el control de las características y los programas de Windows a los que un niño tiene acceso. Por ejemplo, podría restringir el acceso de un niño de las siguientes maneras:

- Impedir que el niño utilice Internet Explorer o Windows Messenger.
- Impedir que el niño cambie el perfil utilizado para iniciar sesión en Windows.
- Aplicar restricciones de tiempo al uso del equipo del niño.
- Restringir el acceso a características de Windows que habilitarían al niño para modificar configuraciones o ejecutar programas inadecuados.
- Restringir las características y los programas que están disponibles en el menú Inicio.

Importante
Los ejemplos facilitados en este manual no se han diseñado como prescripciones para mantener el niño a salvo, sino como ejemplos de cómo se puede utilizar el Toolkit para ayudar a implementar un plan de seguridad y privacidad para el niño. La página Web Recursos en línea para el uso de equipos públicos proporciona vínculos a varios recursos que se pueden utilizar para obtener más información acerca de niños y equipos.

Puede utilizar la herramienta Protección de discos de Windows para garantizar que los niños no puedan realizar cambios permanentes en Windows. Tenga cuidado al utilizar Protección de discos de Windows en equipos en los que desea guardar datos de forma permanente. Sin un planeamiento meticuloso, podría borrar inadvertidamente documentos, imágenes y otros archivos importantes que usted y su familia desean conservar.

Ejemplo 1: Restringir el acceso de niños

En el caso de los niños, en especial los que aprenden a usar un equipo, el objetivo de los padres es tanto proteger al niño de los peligros asociados a la actividad en línea como proteger el equipo de las exploraciones temerarias del niño.

Se puede utilizar el Toolkit para restringir las actividades de los niños de las siguientes maneras:

- Restricciones del usuario
  - Bloquee el perfil de usuario para que no permita efectuar cambios de configuración permanentes. Si bloquea el perfil de usuario, puede redirigir la carpeta Mis documentos del perfil de usuario a una carpeta en una partición persistente para que el niño pueda seguir guardando documentos. También puede almacenar el perfil de usuario en la partición de Windows y activar la herramienta Protección de discos de Windows para obtener protección adicional.
  - Configure el menú Inicio de modo que sólo estén disponibles los juegos locales, no los juegos de Internet. Asimismo, puede hacer que los juegos de contenido inadecuado no estén disponibles para niños.
  - Deshabilite el acceso a Internet. Los expertos sugieren que a los niños sólo se les debe permitir el acceso a Internet cuando sus padres o profesores puedan ayudarlos, o por lo menos, que sólo utilicen Internet en un equipo que se encuentre en una zona familiar común.
  - Deshabilite Windows Messenger. La mayoría de los expertos coincide en que los programas de mensajería instantánea no son adecuados para niños.
  - Impida el acceso a todos los discos excepto aquél en que se permite al niño almacenar documentos.
  - Establezca restricciones de tiempo que impongan los límites que ha elegido para su familia.
  - Configure Restricciones del usuario para impedir el acceso a áreas del sistema operativo con las que el niño no debe relacionarse.
  - Configure las restricciones del menú Inicio para impedir el acceso a características y programas del sistema operativo.
- Protección de discos de Windows
  - Active la herramienta Protección de discos de Windows para que no se guarden los cambios que el niño efectúe. Esto es de especial importancia si permite que el niño tenga acceso a Internet, correo electrónico, Windows Messenger o a herramientas de configuración.

Ejemplo 2: Restringir el acceso de adolescentes

En el caso de los adolescentes, probablemente desee establecer menos restricciones que para un niño. En concreto, los adolescentes suelen necesitar acceso a Internet, correo

electrónico y Windows Messenger. También les parecerá más importante poder configurar su escritorio y puede incluso que disfruten al tener acceso a otras herramientas de configuración para obtener más información acerca del sistema operativo.

Se puede utilizar el Toolkit para restringir las actividades de los adolescentes de las siguientes maneras:

- Restricciones del usuario
  - No bloquee el perfil de usuario. Los adolescentes desearán poder configurar su entorno. Redirija la carpeta Mis documentos del perfil de usuario a una carpeta de una partición persistente y almacene también el perfil de usuario en una partición persistente, como la unidad D:.
  - Puede que desee configurar el menú Inicio para que algunos juegos de Internet estén disponibles para el adolescente. Si no, debe configurar el menú Inicio de modo que sólo estén disponibles los juegos locales.
  - Habilite el acceso a Internet y Windows Messenger. Puede que desee utilizar las opciones de privacidad de Internet Explorer o configurar controles paternos adicionales para el uso de Internet.
  - Establezca restricciones de tiempo que impongan los límites que ha elegido para su familia.
  - Establezca restricciones para impedir el acceso a algunas áreas del sistema operativo.
  - Configure las restricciones del menú Inicio para impedir el acceso a características y programas del sistema operativo.
- Protección de discos de Windows
  - Active la herramienta Protección de discos de Windows para que no se guarden los cambios efectuados en la partición de Windows.

Automatizar las restricciones del usuario mediante Restrict.wsf

La herramienta de línea de comandos Restrict.wsf permite configurar restricciones para un perfil de usuario mediante restricciones almacenadas en un archivo XML. Entre las maneras en que se puede utilizar esta herramienta con un archivo XML se incluyen las siguientes:

- Use un archivo XML preconfigurado para aplicar restricciones a usuarios. El Toolkit incluye varios archivos XML de ejemplo en la carpeta XML que se encuentra dentro de la carpeta del programa (C:\Archivos de programa\Microsoft Shared Computer Toolkit\xml). Por ejemplo, se puede utilizar el archivo Restrict.Office.XML para restringir programas de Microsoft y también personalizarlo para restringir programas de terceros.
- Use Restrict.wsf para crear un archivo XML para un usuario. A continuación, puede personalizar el archivo XML a fin de agregar restricciones para el usuario o para los usuarios adicionales.
- Use Restrict.wsf para aplicar un archivo XML a un usuario.
- Use Restrict.wsf para bloquear o desbloquear un perfil.

La sintaxis de Restrict.wsf es la siguiente:

Restrict.wsf [/User:nombreDeUsuario] [/Create] [/Apply] [/Accounts] [/XML:nombreDeArchivo.xml] [/Lock] [/Unlock]

- **/User** especifica el usuario que se va a configurar con esta herramienta.
- **/Create** indica a la herramienta que cree un archivo XML mediante la configuración del usuario especificado.
- **/Apply** aplica la configuración de un archivo XML al usuario especificado.
- **/Accounts** muestra las cuentas de usuario en que puede utilizarse la herramienta para configurar.
- **/XML** especifica el nombre del archivo que se va a utilizar para almacenar o aplicar la configuración del usuario especificado.
- **/Lock** bloquea el perfil del usuario especificado.
- **/Unlock** desbloquea el perfil del usuario especificado.

Si utiliza Restrict.wsf para copiar restricciones del usuario Jane en el archivo Cafe.xml, emitirá el siguiente comando:

Restrict.wsf /User:Jane /Create /XML:Cafe.xml

Para utilizar Restrict.wsf a fin de aplicar restricciones al usuario Joe del archivo Cafe.xml y bloquear también el perfil de Joe, emitirá el siguiente comando:

Restrict.wsf /User:Joe /Apply /XML:Cafe.xml /Lock

Además de guardar y aplicar la configuración de un solo usuario, se puede utilizar Restrict.wsf para automatizar la aplicación de la configuración a varios usuarios.

Crear un perfil obligatorio para varios usuarios

Los perfiles de usuario obligatorios son básicamente perfiles móviles en los que los usuarios no pueden efectuar cambios permanentes. Existen perfiles de usuario obligatorios disponibles en Windows XP Professional, pero no en Windows XP Home Edition. Los perfiles de usuario obligatorios se almacenan en un servidor de red y se descargan y se aplican cada vez que un usuario inicia sesión. El perfil no se actualiza cuando el usuario cierra la sesión.

La ventaja de utilizar un perfil de usuario obligatorio es que sólo se pueden efectuar cambios en el perfil obligatorio maestro y utilizar dicho perfil en cualquier equipo compartido. La posible desventaja de los perfiles obligatorios es que el equipo compartido debe tener acceso de red para que un usuario inicie sesión. Si no hay ningún perfil de usuario obligatorio disponible, el usuario no puede iniciar sesión.

Para crear un perfil obligatorio para varios usuarios:

1. Cree una carpeta compartida en el servidor de red que va a contener los perfiles.
2. Cree una subcarpeta en dicha carpeta compartida para cada perfil obligatorio que desee utilizar.
3. En cada carpeta compartida, inicie la herramienta Administración de equipos; haga clic con el botón secundario en **Mi PC** y luego haga clic en **Administrar**.
4. En la herramienta Administración de equipos, en **Usuarios y grupos locales**, expanda la carpeta **Usuarios**.
5. En cada cuenta de usuario que vaya a utilizar el perfil obligatorio, haga clic con el botón secundario en la cuenta y luego haga clic en **Propiedades**.

6. En el cuadro de diálogo **Propiedades**, en la ficha **Perfil**, en el cuadro **Ruta de acceso al perfil**, escriba la ruta de acceso de red al recurso compartido donde se guarda el perfil (por ejemplo, **\\server1\profiles\user1**).
7. Cree, configure y restrinja un perfil de usuario, y copie el perfil en el recurso compartido de red correspondiente.
8. En el recurso compartido de red, en la carpeta del perfil, cambie el nombre del archivo Ntuser.dat a Ntuser.man. De este modo, se cambia el perfil de un simple perfil móvil a un perfil obligatorio.

- Para obtener más información acerca del uso de perfiles móviles y obligatorios con Windows XP Professional, consulte el sitio sobre perfiles de usuario en el sitio Web de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54488; puede que la página esté en inglés).
- Para obtener más información acerca de cómo asignar un perfil obligatorio a una cuenta de usuario en Windows XP, consulte el artículo 307800 de Microsoft Knowledge Base en el sitio Web de ayuda y soporte técnico de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54489; puede que la página esté en inglés).

Clonar o crear una imagen de un equipo protegido mediante el Toolkit

Cuando se instala Windows XP Professional en varios equipos que tienen configuraciones de hardware idénticas, el método de instalación más eficaz es la creación de imágenes de disco, proceso que también se denomina *clonación*. Este método comprende las acciones siguientes:

- **Configurar un equipo de referencia.** Se trata de un equipo que se prepara según las instrucciones descritas en los capítulos 1 a 5 de este manual.
- **Usar la herramienta de preparación del sistema (Sysprep.exe) para preparar el equipo para crear imágenes (opcional).** Sysprep.exe se encuentra en el CD del sistema operativo Windows XP. Para obtener más información, consulte el sitio acerca del uso de Sysprep.exe en el sitio Web de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54491; puede que la página esté en inglés).
- **Crear una imagen exacta del disco duro del equipo de referencia y transferirla a los discos duros de otros equipos.** Para ello, puede utilizar un programa de creación de imágenes de discos como Symantec Norton Ghost o Acronis True Image.
- **Realizar algunas tareas finales en el equipo clonado.** Tras la creación de imágenes, el equipo clonado iniciará un programa de instalación mínima que valida y activa el uso de Windows XP en el nuevo sistema.

Configurar un equipo de referencia

Debe configurar en primer lugar el equipo de referencia que se va a clonar. La configuración de un equipo de referencia comprende las tareas siguientes:

- **Instalar el sistema operativo**. Instalar Windows XP Professional con SP2 o Windows XP Home Edition con SP2.
- **Preparar el disco duro para Protección de discos de Windows**. Para obtener más información, consulte el capítulo 2, “Preparar el disco para Protección de discos de Windows”.

- **Instalar Microsoft Shared Computer Toolkit para Windows XP**. Para obtener más información, consulte el capítulo 1, “Instalación”.
- **Crear cuentas de usuario locales limitadas**. En el equipo de referencia, cree un superconjunto con todas las cuentas de usuario que va a necesitar en todos los equipos compartidos. Siempre puede quitar las cuentas que no va a necesitar de los equipos específicos.
- **Crear y personalizar los perfiles de usuario para cada cuenta**. Para obtener más información, consulte el capítulo 3, “Administración de perfiles”.
- **Configurar restricciones del usuario en el equipo**. Para obtener más información, consulte el capítulo 4,“Restricciones del usuario”.

Importante

No active la herramienta Protección de discos de Windows antes de clonar un equipo. Esto podría traducirse en dificultades para obtener una imagen de disco limpia y problemas en los equipos de destino.

Usar la herramienta de preparación del sistema

Una vez configurado el equipo de referencia, el siguiente paso es preparar el equipo para la creación de imágenes. Muchas de las configuraciones de un equipo con Windows XP Professional deben ser exclusivas, como el nombre del equipo y el identificador de seguridad (SID), que es el número que se usa para realizar el seguimiento de un objeto a través del subsistema de seguridad de Windows. Para solucionar esta necesidad, Windows XP Professional proporciona una utilidad denominada herramienta de preparación del sistema (Sysprep.exe) que quita del equipo el SID y el resto de la información específica del usuario y del equipo. A continuación, apaga el equipo para que se pueda utilizar una utilidad de duplicación de disco y crear una imagen del disco. La imagen de disco es simplemente un archivo comprimido que incluye el contenido de todo el disco duro en el que está instalado el sistema operativo.

Nota

Cuando se crea una imagen de disco, toda la configuración de hardware del equipo de referencia pasa a formar parte de la imagen. Por tanto, el equipo de referencia debe tener la misma configuración de hardware (o similar) que los equipos de destino.

Normalmente, cuando un equipo cliente inicia Windows XP Professional por primera vez después de cargar una imagen de disco preparada con Sysprep, Windows genera automáticamente un SID único e inicia la detección Plug and Play y el asistente para la instalación mínima. El asistente para la instalación mínima pedirá información específica del usuario y del equipo, como el Contrato de licencia para el usuario final (CLUF), la configuración regional, el nombre del usuario y la empresa, la clave del producto, etc.

Puede automatizar aun más el proceso de creación de imágenes si incluye un archivo de respuesta denominado Sysprep.inf con la imagen maestra. Sysprep.inf es un archivo de respuesta que se utiliza para automatizar el proceso de instalación mínima. Utiliza la misma sintaxis del archivo INI y nombres de clave (para claves compatibles) como Unattend.txt. Coloque el archivo Sysprep.inf en la carpeta %unidadDeSistema%\Sysprep o en un disquete. Si utiliza un disquete, insértelo en la unidad de disquete cuando aparezca la pantalla de inicio de Windows. Observe que si no incluye Sysprep.inf al ejecutar Sysprep, el asistente para la instalación mínima requiere entrada del usuario en cada pantalla de personalización.

Para obtener más información acerca de cómo usar la herramienta de preparación del sistema, consulte los siguientes recursos (puede que las páginas estén en inglés):

- Para obtener información general acerca del proceso de creación de imágenes de clientes, incluido el uso de Sysprep para preparar un sistema para crear imágenes, consulte el sitio sobre creación de imágenes en el sitio Web de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54493).
- Para obtener más información, consulte el sitio acerca de la personalización de instalaciones de Sysprep en el sitio Web de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54494).

Crear y transferir una imagen de disco duro

Una vez ejecutada la herramienta de preparación del sistema para preparar el equipo de referencia para crear imágenes, la herramienta apaga el equipo de referencia. En este momento, se puede utilizar una herramienta de creación de imágenes de terceros para crear una imagen del disco duro del equipo. Puede encontrar recomendaciones acerca de herramientas de creación de imágenes si busca utilidades de copia de unidades en la Windows Marketplace (http://go.microsoft.com/fwlink/?LinkId=54495; puede que la página esté en inglés).

Entre las utilidades de creación de imágenes más utilizadas se incluyen (puede que las páginas estén en inglés):

- Symantec Norton Ghost 9.0 (http://www.symantec.com/sabu/ghost/ghost_personal/)
- Acronis True Image 8.0 (http://www.acronis.com/enterprise/products/ATICW/)

Actividades posteriores a la creación de imágenes

Nota
Los equipos que ejecutan Windows XP con licencias por volumen no requieren activación ni validación después de la clonación si la imagen original estaba activada y validada. Esta es una de las ventajas del programa de licencias por volumen.

Después de transferir una imagen a un nuevo equipo e iniciar dicho equipo, Windows genera un SID único e inicia la detección Plug and Play y el asistente para la instalación mínima. Una vez finalizada la instalación, hay varias tareas que es preciso llevar a cabo. Entre ellas se incluyen:

- **Activar Windows**. Para obtener más información acerca de la activación de productos de Microsoft, consulte el artículo 302806 de Microsoft Knowledge Base en el sitio Web de ayuda y soporte técnico de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54496; puede que la página esté en inglés).
- **Validar Windows XP**. Puede validar Windows en el sitio Web acerca de las Ventajas de Windows Original (http://go.microsoft.com/fwlink/?LinkId=53507; puede que la página esté en inglés). Si ha utilizado Sysprep para preparar el equipo para crear imágenes, se le pedirá que valide Windows de nuevo antes de utilizar las herramientas del Toolkit.
- **Activar la herramienta Protección de discos de Windows**. Puede activar Protección de discos de Windows si utiliza la herramienta directamente o con la herramienta de línea de comandos **DiskProtect**.

Capítulo 10: Shared Computer Toolkit en entornos de dominio

Este capítulo del manual se centra en el uso de Shared Computer Toolkit en equipos en entornos de dominio y el control de otros requisitos de ámbito empresarial. En concreto, en este capítulo se trata:

- Shared Computer Toolkit y Active Directory
- Protección de discos de Windows en equipos unidos por dominio
- Crear un perfil de usuario persistente para una cuenta de dominio
- Restricciones de directiva de grupo para cuentas de dominio
- Restricciones del usuario para cuentas de dominio no restringidas
- Perfiles de usuario en otros idiomas

Shared Computer Toolkit y Active Directory

El servicio de directorio Active Directory® ofrece importantes ventajas para equipos compartidos en red. Active Directory proporciona a los usuarios de red acceso controlado a los recursos de cualquier punto de la red mediante un solo conjunto de credenciales. Además, proporciona a los administradores de red una vista jerárquica e intuitiva de la red, así como un punto de administración único para todos los objetos de dicha red.

Active Directory ofrece un mejor entorno para administrar de forma centralizada cuentas de usuario que requieren acceso a recursos de red o necesitan iniciar sesión con las mismas credenciales en varios equipos, como en el caso de muchas instituciones educativas. Por ello, Shared Computer Toolkit se ha diseñado para funcionar correctamente tanto en entornos de dominio como en equipos de grupo de trabajo.

Nota
El Toolkit proporciona una plantilla de directiva de grupo (SCTSettings.adm) que incluye la mayoría de las configuraciones que se encuentran en la herramienta Restricciones del usuario. Puede utilizar esta plantilla para configurar usuarios en un objeto de directiva de grupo.

La herramienta Protección de discos de Windows funciona de forma óptima e inmediata en equipos unidos por dominio, simplificando en gran medida la carga administrativa de proteger y mantener quioscos de Internet, sistemas de autoservicio de empleados y equipos de acceso público de un dominio.

La mayoría de las configuraciones y restricciones de la herramienta Restricciones del usuario están disponibles a través de la plantilla de directiva de grupo (SCTSettings.adm) que se suministra con el Toolkit. La directiva de grupo es más eficaz que la herramienta Restricciones del usuario para restringir varias cuentas de usuario en gran cantidad de equipos a la vez.

Protección de discos de Windows en equipos unidos por dominio

Nota
La Herramienta Protección de discos de Windows deshabilita el inicio automático de cliente de cambios de contraseñas de cuentas de equipo del dominio. Para resolverlo, Protección de discos de Windows actualiza automáticamente la contraseña cada vez que se guardan cambios en el disco. Como mínimo, esto se produce durante el proceso de actualizaciones críticas programadas.

Cuando un equipo que ejecuta Windows XP Professional se une a un dominio Active Directory, el equipo utiliza una contraseña de cuenta de equipo para autenticarse en el dominio y obtener acceso a recursos del mismo. De manera predeterminada, el equipo unido por dominio inicia automáticamente un cambio de la contraseña de cuenta de equipo en cada 30 días. Un controlador de dominio acepta el cambio de contraseña y permite al equipo unido por dominio continuar con la autenticación. La nueva contraseña se almacena localmente en el equipo unido por dominio y puede confirmarse con Active Directory. Si un cambio de contraseña produce error o si un equipo unido por dominio intenta utilizar una contraseña incorrecta, el equipo no podrá obtener acceso al dominio.

Contraseñas de cuenta de equipo en un entorno de dominio

Cuando Protección de discos de Windows se activa, la herramienta deshabilita las actualizaciones automáticas de contraseña de cuenta de equipo iniciadas por el cliente del sistema. Protección de discos de Windows inicia automáticamente un cambio de contraseña cada vez que se guardan cambios en el disco. Esto sucede una vez al activar la herramienta Protección de discos de Windows. Después, la actualización se produce con cada reinicio en el que se guarden cambios en el disco. Como mínimo, esto se produce durante el proceso de actualizaciones críticas programadas.

La razón para este cambio de funcionalidad es que si un equipo compartido con Protección de discos de Windows activada inicia un cambio de contraseña de cuenta de equipo, se creará una nueva contraseña en Active Directory. Tras reiniciar el equipo, la herramienta Protección de discos de Windows volverá a la contraseña anterior; todo esto se traduce en la imposibilidad de tener acceso a todos los recursos del dominio.

Importante
Los clientes unidos por dominio que ejecuten la herramienta Protección de discos de Windows no se deben ejecutar durante 30 días con ninguna de las opciones de reinicio de **Conservar cambios**; de lo contrario, dejarán de estar unidos por el dominio debido a una contraseña de cuenta de equipo obsoleta.

Si se activa alguna de las opciones de **Conservar cambios** de la herramienta Protección de discos de Windows, no se guarda ningún cambio en la partición de Windows. Si se efectúa un cambio de contraseña de cuenta de equipo mientras alguna de estas opciones está activada y los cambios no se guardan en el número máximo de días permitido para un cambio de contraseña en el dominio (30 días de manera predeterminada), las contraseñas dejarán de estar sincronizadas. Por tanto, no debe ejecutar ninguna de las opciones de reinicio de **Conservar cambios** durante 30 días o más.

Otra cuestión que debe tener en cuenta es el efecto de cambiar **Opción de reinicio**. Si configura la herramienta Protección de discos de Windows en **Guardar cambios con el siguiente reinicio**, la herramienta cambia inmediatamente la contraseña del dominio antes de reiniciar. Si a continuación configura Protección de discos de Windows en **Borrar cambios en cada reinicio**, el equipo descarta la nueva contraseña y ya no puede iniciar sesión en el dominio.

Administración centralizada de software y Protección de discos de Windows

Cuando la herramienta Protección de discos de Windows se activa, las actualizaciones de software del equipo se realizan de forma idónea mediante el proceso de actualizaciones críticas que ofrece esta herramienta. Para mantener la condición de confianza del equipo, Protección de discos de Windows realiza en primer lugar un reinicio programado con regularidad para borrar todos los cambios en disco y, a continuación, descarga e instala las actualizaciones necesarias sobre esta base de confianza. Este modelo es algo menos flexible que algunos modelos de administración centralizada de software en los que las actualizaciones se pueden iniciar de forma centralizada y programar para que se produzcan en cualquier momento.

Un sistema de distribución de software administrado de forma centralizada, como Microsoft Systems Management Server, puede proporcionar la flexibilidad para programar actualizaciones de software que se produzcan en cualquier momento, pero la herramienta Protección de discos de Windows no puede igualar fácilmente esta flexibilidad.

Si la organización tiene una gran necesidad de cambiar con regularidad el programa de actualizaciones de software, en lugar de seguir un programa fijo establecido en Protección de discos de Windows, puede que convenga contemplar la posibilidad de que la herramienta no sea adecuada para su entorno.

Por el contrario, si puede integrar el proceso de actualización de software administrado de forma centralizada en el proceso de actualización de la herramienta Protección de discos de Windows controlado por el cliente, puede que encuentre un medio acertado en el que la distribución de software centralizada y la herramienta puedan coexistir.

Equipos portátiles y Protección de discos de Windows

Es importante recordar que puede que el modelo de administración de software que utiliza la herramienta Protección de discos de Windows no sea adecuado en entornos con equipos portátiles, como las tabletas, que se desconectan o se desactivan de forma rutinaria en el momento en el que se programa el proceso de actualizaciones críticas de Protección de discos de Windows.

Administrar Protección de discos de Windows mediante DiskProtect.wsf

Para automatizar la configuración de la herramienta Protección de discos de Windows en varios equipos, se puede utilizar la herramienta de línea de comandos DiskProtect.wsf que se incluye con Shared Computer Toolkit. Esta herramienta se puede utilizar en archivos por lotes y secuencias de comandos para configurar Protección de discos de Windows.

La sintaxis de esta herramienta es la siguiente:

DiskProtect.wsf [/Status] [/On] [/Off] [/Save] [/Clear] [/Retain] [/Once] [/Restart] [/MU] [/NoMU] [/AV] [/Other] [/Time] [/Day]

Nota
Si utiliza la herramienta DiskProtect.wsf con la opción **/?** obtendrá una descripción de cada opción de línea de comandos.

El siguiente ejemplo activa la herramienta Protección de discos de Windows, habilita Microsoft Updates e instala las actualizaciones de McAfee Antivirus, todo a las 02:00:

DiskProtect.wsf /On /MU /AV:"C:\Archivos de programa\Microsoft Shared Computer Toolkit\scripts\update\SCTMcAfeeVirusUpdate.vbs" /Time:2

DiskProtect.wsf se puede llamar desde archivos por lotes, secuencias de comandos de inicio de sesión y secuencias de comandos de instalación de software. Una posibilidad consiste en establecer la herramienta Protección de discos de Windows en **Guardar cambios con el siguiente reinicio** para permitir la instalación de un programa mediante secuencias de comandos. Tras el reinicio, el programa se guarda en la partición de Windows.

Crear un perfil de usuario persistente para una cuenta de dominio

Puede que, en algunas cuentas de dominio que inician sesión en equipos compartidos, sea necesario crear un perfil de usuario local persistente que no se vea afectado por el comportamiento de reinicio predeterminado de la herramienta Protección de discos de Windows cuando borra todos los cambios en disco efectuados en la partición de Windows. Puede ser necesario, por ejemplo, permitir que una profesora guarde sus documentos y su configuración de Windows en un equipo protegido con la herramienta Protección de discos de Windows.

Nota
Si se utiliza ProfileMgr.wsf para crear un perfil en una partición persistente, se creará una carpeta Documents and Settings para que contenga el nuevo perfil (si no existe aún).

Para crear perfiles de usuario locales persistentes para cuentas de dominio, use la herramienta de línea de comandos ProfileMgr.wsf que se encuentra en la subcarpeta denominada **Scripts** de la instalación del Toolkit. Para crear un perfil de usuario, utilice la siguiente sintaxis de comandos:

ProfileMgr.wsf /create *nombreDeUsuario contraseña /domain:<nombreDeDominio>*
**   */drive:<letraDeUnidad>***

Por ejemplo, para crear un perfil en la unidad D de un usuario denominado User1 en el dominio Contoso con la contraseña UserPass5, se utilizará el siguiente comando:

ProfileMgr.wsf /create User1 UserPass5 /domain:Contoso /drive:D:

Crear perfiles de usuario locales persistentes para todas las cuentas

Si desea garantizar que todos los perfiles de usuario locales creados para cualquier cuenta, incluidas las cuentas de dominio, se sitúen en una partición persistente en la que no se vean afectados por la herramienta Protección de discos de Windows, será necesario personalizar la instalación del equipo para que la ubicación predeterminada para perfiles de usuario no esté en la partición de Windows.

Es posible cambiar la ubicación predeterminada en la que se instalan los perfiles de usuario, pero este cambio sólo se admite durante la instalación de Windows XP y se debe efectuar mediante la automatización de la instalación de Windows con un archivo especial de respuesta. Este método cambia la ubicación en la que se almacenan *todos* los perfiles de usuario, incluidos los perfiles de usuario predeterminado y de todos los usuarios. Esto permite que Windows cree automáticamente perfiles en una partición persistente en lugar de tener que utilizar la herramienta Administrador de perfiles para especificar la ubicación de los perfiles al crearlos.

Los archivos de respuesta son archivos de texto que contienen respuestas a algunas o todas las preguntas que hace el programa de instalación durante el proceso de instalación. Después de crear un archivo de respuesta, denominado unattend.txt, puede aplicarlo a todos los equipos que sea necesario.

La manera más sencilla de crear un archivo de respuesta para una instalación desatendida de Windows XP es utilizar el Administrador de instalación de Windows, una herramienta de implementación que ofrece una interfaz de asistente para crear el archivo de respuesta. Para obtener más información acerca del uso del Administrador de instalación para automatizar instalaciones, consulte el sitio sobre cómo automatizar y personalizar instalaciones en el sitio Web de Microsoft (http://go.microsoft.com/fwlink/?LinkId=54497; puede que la página esté en inglés). El archivo de respuesta que cree mediante el Administrador de instalación puede incluir otra información, como la zona horaria, la configuración de red, etcétera.

Una vez creado un archivo de respuesta, puede cambiar la ubicación predeterminada en la que se almacenan los perfiles de usuario si agrega la siguiente entrada:

[GuiUNattended]
ProfilesDir = drive:\nombreDeCarpeta

Restricciones de directiva de grupo para cuentas de dominio

El Toolkit incluye una plantilla de directiva de grupo denominada SCTSettings.adm en la carpeta bin de la instalación. Esta plantilla reproduce la mayoría de las configuraciones incluidas en la herramienta Restricciones del usuario y se puede utilizar para implementar estas restricciones en usuarios que son miembros de un dominio de Active Directory.

La directiva de grupo se puede configurar para un dominio mediante la Consola de administración de directivas de grupo (GPMC), una herramienta complementaria disponible para descarga en Microsoft, o bien mediante el Editor de directivas de grupo integrado en Usuarios y equipos de Active Directory. Al agregar la plantilla SCTSettings.adm a estas herramientas, obtendrá acceso a restricciones y configuraciones de cuenta adecuadas para cuentas compartidas.

La plantilla de directiva de grupo SCTSettings.adm que se incluye con Shared Computer Toolkit ofrece la posibilidad de establecer temporizadores de cierre de sesión obligatorio y cierre de sesión inactiva, si el Toolkit se instala en los equipos.

Es importante que sólo se apliquen estas configuraciones a cuentas de usuario específicas, para no restringir actividades administrativas legitimas en ninguno de los equipos.

Nota
Microsoft recomienda crear una unidad organizativa que almacene las cuentas de usuario compartidas del entorno y aplicar la plantilla SCTSettings.adm a la parte de configuración de usuario de un objeto de directiva de grupo vinculado a esta unidad organizativa dedicada.

Para usar Usuarios y equipos de Active Directory y administrar restricciones del Toolkit:

1. Para iniciar Usuarios y equipos de Active Directory en un equipo con Windows Server 2003, desplácese hasta Herramientas administrativas, que se encuentra en el menú Inicio o en el Panel de control.
2. En la consola Usuarios y equipos de Active Directory, haga clic con el botón secundario en la unidad organizativa donde desea configurar la directiva y haga clic en **Propiedades**.
3. En la ficha **Directiva de grupo**, haga clic en la directiva que desee cambiar y en **Editar**.
4. Expanda **Configuración de usuario**, haga clic con el botón secundario en la carpeta **Plantillas administrativas** y, luego, haga clic en **Agregar o quitar plantillas**.
5. En el cuadro de diálogo **Agregar o quitar plantillas**, haga clic en **Agregar** y desplácese hasta la ubicación de la plantilla SCTSettings.adm (por lo general, la carpeta Archivos de programa\Microsoft Shared Computer Toolkit\bin).
6. Examine las opciones de la carpeta **Todas las restricciones de Shared Computer Toolkit** y observe su similitud con las opciones de Restricciones del usuario. Observe también las explicaciones facilitadas para cada opción.
7. Haga los cambios de restricciones que desee y salga del Editor de directivas de grupo.

Importante
La plantilla SCTSettings.adm sólo se ha diseñado para que se aplique a la configuración de usuario de un objeto directiva de grupo. No aplique la plantilla SCTSettings.adm a la configuración del equipo, ya que restringe a todos los usuarios de los equipos afectados por la directiva.

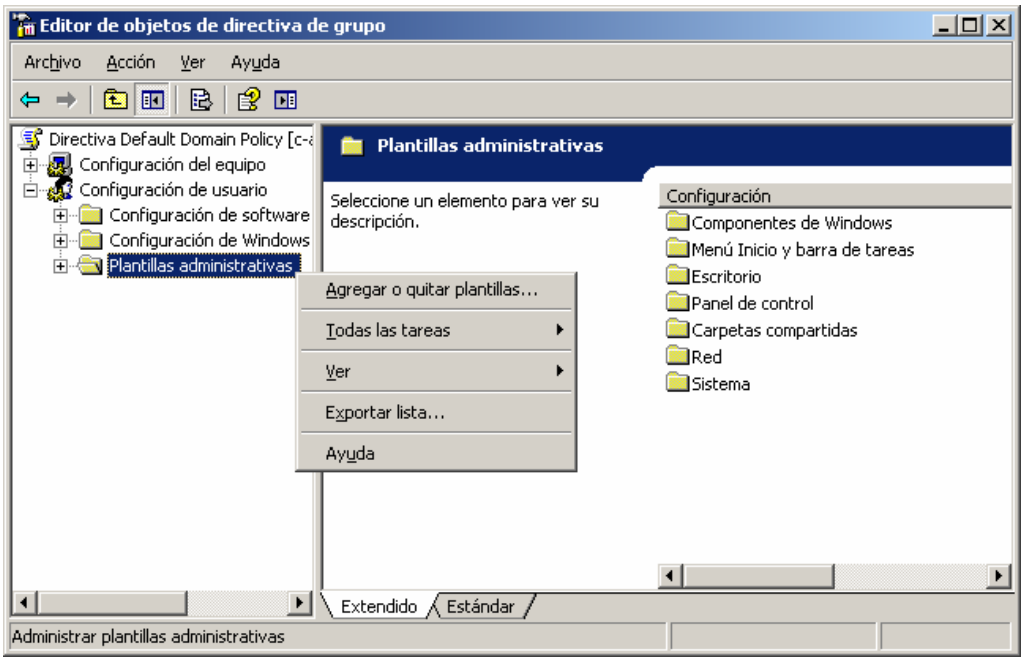

Figura 10.1 *Configurar plantillas de directiva de grupo en el Editor de directivas de grupo*

Nota
Para adaptar restricciones de software a usuarios o grupos de usuarios, cree más de una directiva y controle la directiva que se aplica a los distintos usuarios a través de la configuración de seguridad.

Usar una directiva de grupo para configurar directivas de restricción de software

Las directivas de restricción de software proporcionan control sobre los programas que se permiten ejecutar en un equipo. Shared Computer Toolkit ofrece algunas restricciones de software en la herramienta Restricciones del usuario. Esta herramienta funciona bien para pocos equipos, pero su administración no resulta eficaz cuando el número de equipos o ubicaciones aumenta. La configuración de directivas de restricción de software en la directiva de grupo es la mejor manera de administrar de forma centralizada restricciones de software entre varios equipos o usuarios.

Las restricciones de software idénticas a las aplicadas con la herramienta Restricciones del usuario se pueden configurar en Active Directory mediante las directivas de restricción de software, que se encuentran en la directiva de grupo, en Configuración de seguridad.

Nota
También pueden aplicarse restricciones de software en Configuración del equipo; tenga cuidado y asegúrese de que los administradores legítimos no se ven restringidos al establecer Obligatoriedad en Todos los usuarios excepto los administradores locales.

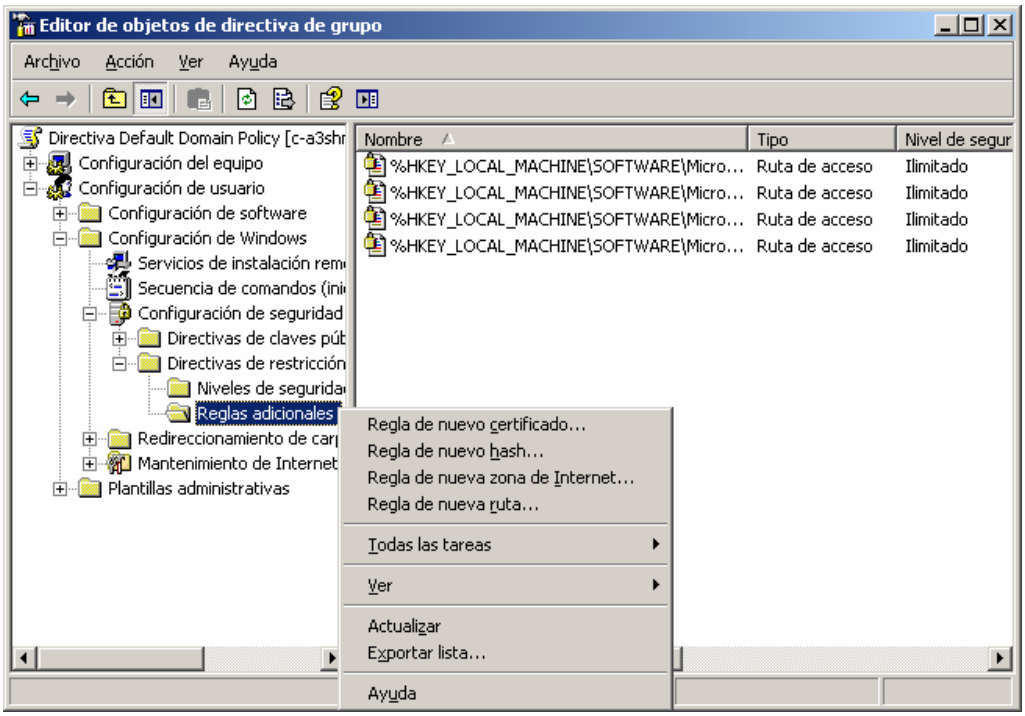

Figura 10.2 *Usar reglas de ruta de acceso para restringir software en función de su nombre o ubicación*

Nota
Para obtener más información, consulte la página del sitio Web de Microsoft acerca del uso de directivas de restricción de software para proteger el equipo contra programas no autorizados (http://go.microsoft.com/fwlink/?LinkId=14508; puede que la página esté en inglés).

Para configurar restricciones de software en Windows XP mediante una directiva de grupo:

1. Para iniciar Usuarios y equipos de Active Directory en un equipo con Windows Server 2003, desplácese hasta Herramientas administrativas, que se encuentra en el menú Inicio o en el Panel de control.
2. En la consola Usuarios y equipos de Active Directory, haga clic con el botón secundario en el dominio Active Directory o la unidad organizativa donde desea configurar la directiva y haga clic en **Propiedades**.
3. En la ficha **Directiva de grupo**, haga clic en la directiva que desee cambiar y en **Editar**.
4. Expanda **Configuración de usuario**, **Configuración de Windows**, **Configuración de seguridad** y haga clic en **Directivas de restricción de software**.
5. Si se han definido directivas de restricción de software, habrá una carpeta **Reglas adicionales** en **Directivas de restricción de software** que contiene reglas.
6. Puede editar una definición existente o hacer clic con el botón secundario en la carpeta **Reglas adicionales** y hacer clic en **Regla de nueva ruta** (como se muestra en la ilustración siguiente).
7. En el cuadro de diálogo **Regla de nueva ruta**, especifique la ruta de acceso y elija si la regla va a permitir o no el software en la ruta de acceso. La entrada de la ruta de acceso puede utilizar variables de entorno (como %ProgramFiles%) y caracteres comodín (* y ?) para definir la ruta.
8. Haga clic en **Aceptar** para guardar la nueva regla de ruta de acceso.

Para duplicar las restricciones de software establecidas mediante la herramienta Restricciones del usuario, cree las reglas de ruta de acceso que se definen en las dos secciones siguientes. De manera opcional, también puede restringir Notepad y WordPad, e impedir que se ejecuten los programas de Microsoft Office mediante directivas de restricción de software, tal como se describe a continuación.

Nota
Impedir que se ejecuten Windows Messenger y MSN Messenger se incluye en la plantilla de directiva de grupo SCTSettings.adm y no utiliza ninguna restricción de ruta de acceso.

Únicamente permitir que se ejecute software en las carpetas Archivos de programa y Windows

Para utilizar directivas de restricción de software y duplicar el efecto de la casilla de verificación **Únicamente permitir que se ejecute software en las carpetas Archivos de programa y Windows** de la herramienta Restricciones del usuario, establezca la opción del nivel de seguridad de la directiva de restricción de software en No permitido y cree reglas adicionales para permitir o no cada una de las siguientes rutas de acceso:

- %ProgramFiles% (permite que se ejecuten programas)
- %Windir% (permite que se ejecuten programas de Windows)
- *.lnk (permite que el menú Inicio y los accesos directos del escritorio funcionen)

Para mayor seguridad, también debe crear una regla de ruta de acceso adicional que no permita la ejecución de archivos de la carpeta Temp, porque todos los usuarios tienen acceso de escritura a los archivos de esta ubicación:

- %WinDir%\Temp

Impedir la ejecución de Herramientas del sistema y algunas herramientas administrativas

Nota
Tal vez tenga intención de investigar las rutas de acceso de programas adicionales que desee restringir. Puede restringir otros programas además de los listados aquí.

Para utilizar directivas de restricción de software y duplicar el efecto de la casilla de verificación **Impedir la ejecución de Herramientas del sistema y algunas herramientas administrativas** de la herramienta Restricciones del usuario, cree una regla de ruta de acceso adicional para no permitir los siguientes archivos:

> NTBackup.exe, Cleanmgr.exe, Migwiz.exe, MSInfo32.exe, Rstrui.exe, CACLS.exe, MMC.EXE, Diskpart.exe, Net.exe, Reg.exe, Regini.exe, GPEdit.exe, XCopy.exe, Rename.exe, Ren.exe, Control.exe, DiskMgmt.msc, NusrMgr.cpl, ConfigWizards.exe, DDEShare.exe, RegSvcs.exe, RegSvr32.exe, ShrPubw.exe, SPUninst.exe, FSquirt.exe y DxDiag.exe

Si se ha instalado Shared Computer Toolkit en los equipos, cree reglas de ruta de acceso adicionales para no permitir los siguientes archivos:

> ETPrep.exe, EWFMgr.exe, SrvAny.exe, NetDom.exe, UPHClean.exe, XPePM.exe, SchTasks.exe, CreateProfile.exe, DenyAccess.exe, WindowsUpdates.vbs, Banner.wsf, DiskProtect.hta, GetStarted.hta, CheckWDP.hta, ProfileMgr.hta y Restrict.hta

Restringir Notepad y WordPad (recomendado para Administradores restringidos)

Para utilizar directivas de restricción de software y duplicar el efecto de la casilla de verificación de restricción opcional **Restringir Notepad y WordPad** de la herramienta Restricciones del usuario, cree una regla de ruta de acceso adicional para no permitir los siguientes archivos:

- Notepad.exe
- Wordpad.exe

Impedir que se ejecuten los programas de Microsoft Office

Para utilizar directivas de restricción de software y duplicar el efecto de la casilla de verificación de restricción opcional **Impedir que se ejecuten los programas de Microsoft**

Office de la herramienta Restricciones del usuario, cree una regla de ruta de acceso adicional para no permitir los siguientes archivos:

- %ProgramFiles%/Microsoft Office

Reiniciar al cerrar sesión mediante una secuencia de comandos de cierre de sesión

Cuando un equipo con Windows XP se une a un dominio, puede ser más difícil garantizar que los cambios se borren entre inicios de sesión de distintos usuarios. Como la herramienta Restricciones del usuario no se utiliza en escenarios de dominio, pasa a ser necesario reproducir la función **Reiniciar al cerrar sesión** que suele proporcionar esta herramienta.

Nota
Puede utilizar el comando **shutdown** en un archivo de proceso por lotes para reiniciar el equipo. En la línea de comandos, emita el comando **shutdown -r -t 00**
El comando **shutdown** está restringido cuando se restringe el acceso al símbolo del sistema. También puede utilizar la herramienta **ForceLogoff.exe** que se incluye en el Toolkit para reiniciar el equipo.

Para utilizar una directiva de grupo para forzar el reinicio del equipo cuando un usuario cierra sesión:

1. Abra el objeto de directiva de grupo del dominio o la unidad organizativa a la que el usuario pertenece.
2. En **Configuración de usuario**, expanda **Configuración de Windows** y haga clic en **Secuencias de comandos (inicio de sesión/cierre de sesión)**.
3. Abra el objeto **Cerrar sesión** y agregue una secuencia de comandos de cierre de sesión. La secuencia de comandos de cierre de sesión puede estar escrita en cualquier lenguaje de secuencias de comandos compatible con Windows que incluya un comando para reiniciar el equipo.

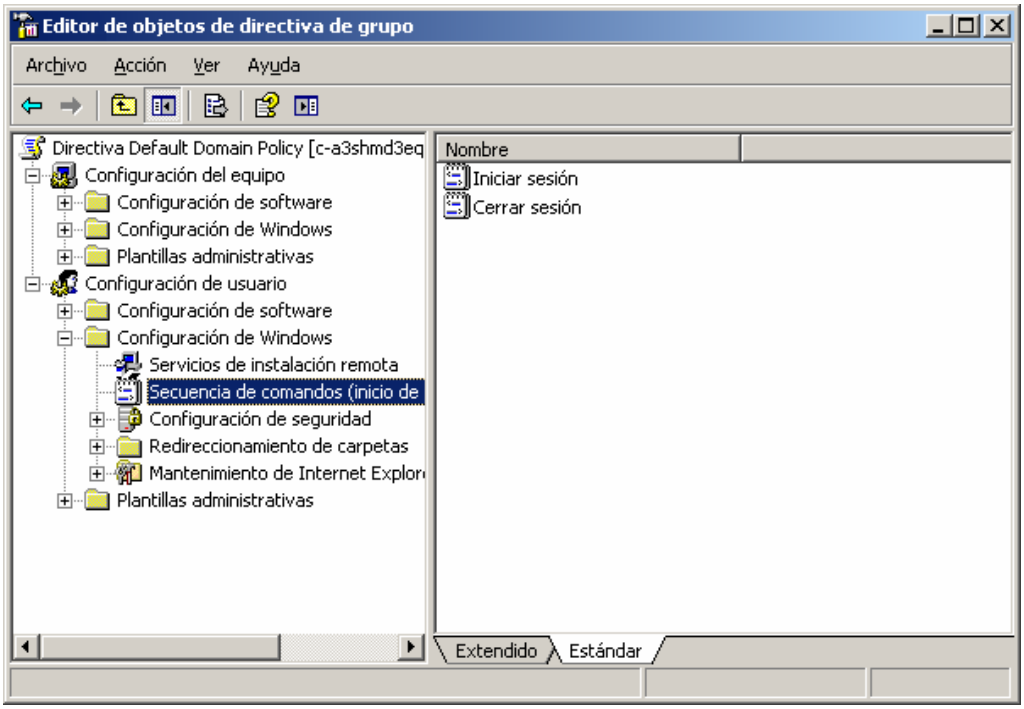

Figura 10.3 *La directiva de grupo permite la configuración de secuencias de comandos de inicio y cierre de sesión para usuarios*

Restricciones del usuario para cuentas de dominio no restringidas

Algunas organizaciones necesitan restringir cuentas de dominio en equipos específicos, pero la directiva de grupo elimina las restricciones para estas cuentas de dominio. Esto

suele suceder en servicios compartidos que los usuarios de dominio utilizan brevemente, como los laboratorios de copia de medios u otros tipos de quioscos de equipos dedicados.

De manera similar, puede que los operadores necesiten restringir cuentas de dominio en equipos específicos, pero carezcan de derechos de acceso para efectuar los cambios necesarios en la directiva de grupo.

Otros entornos preocupados por la seguridad desean garantizar la aplicación de restricciones predeterminadas a usuarios de dominio, aunque los problemas de red impidan que se apliquen restricciones de directiva de grupo en el primer inicio de sesión (por lo general provocado por alteraciones, como la eliminación oportuna de un cable de red).

Todos estos escenarios se pueden resolver con la herramienta Restricciones del usuario para aplicar restricciones al perfil de usuario predeterminado de un equipo. El perfil de usuario predeterminado se utiliza como plantilla al crear nuevos perfiles de usuario para cuentas de dominio y locales. Esta técnica en particular no funciona en cuentas de dominio que se han configurado con perfiles de usuario móviles.

Importante
Antes de personalizar el perfil de usuario predeterminado, cree una copia de seguridad por si se producen problemas. Para ello, haga una copia de la carpeta Default User que se encuentra en la carpeta Documents and Settings.

Para crear un perfil de usuario predeterminado:

1. Inicie sesión como administrador del Toolkit.
2. Cree una nueva cuenta de usuario local limitada.
3. Cierre la sesión e inicie otra sesión con la cuenta de usuario local que acaba de crear.
4. Personalice el perfil. Puede, por ejemplo:
   - Personalizar el menú Inicio.
   - Personalizar el escritorio y la barra de tareas.
   - Instalar y configurar impresoras.
5. Cierre la sesión e inicie otra como administrador del Toolkit.
6. Utilice la herramienta Restricciones del usuario para configurar y aplicar restricciones al perfil recién creado.
7. Haga clic en **Inicio** y en **Mi PC**.
8. Haga clic en el menú **Herramientas** y en **Opciones de carpeta**.
9. En el cuadro de diálogo **Opciones de carpeta**, en la ficha **Ver**, en **Configuración avanzada**, haga clic en **Mostrar todos los archivos y carpetas ocultos** y en **Aceptar**. De manera predeterminada, varios de los archivos del nuevo perfil están ocultos, por lo que deben mostrarse los archivos ocultos para copiarlos en el nuevo perfil de usuario predeterminado personalizado.
10. Haga clic en **Inicio**, haga clic con el botón secundario en **Mi PC** y, luego, haga clic en **Propiedades**.
11. En el cuadro de diálogo **Propiedades del sistema**, en la ficha **Opciones avanzadas**, en **Perfiles de usuario**, haga clic en **Configuración**.
12. En el cuadro de diálogo **Perfiles de usuario**, haga clic en el perfil de usuario que acaba de crear y personalizar, y haga clic en **Copiar a**.
13. En el cuadro de diálogo **Copiar a**, en **Copiar perfil en**, haga clic en **Examinar**, en la carpeta C:\Documents and Settings\Default User y en **Aceptar**.
14. En **Está permitido usar**, haga clic en **Cambiar**, en **Todos** y en **Aceptar**. Si **Todos** no está disponible, haga clic en **Opciones avanzadas**, en **Buscar ahora**, en **Todos** y en **Aceptar**.

Nota
Si copia la carpeta Default User en el recurso compartido NETLOGON de un controlador de dominio, todos los usuarios de dominio recibirán la configuración y las restricciones de este perfil la primera vez que inicien sesión.

Esta carpeta se replica en los demás controladores de dominio para proporcionar un perfil de usuario predeterminado a todas las cuentas de dominio nuevas.

Windows XP asigna ahora el perfil de usuario predeterminado junto con sus restricciones a cualquier nuevo usuario que inicie sesión en el equipo.

Esta técnica no se puede utilizar para bloquear nuevos perfiles de usuario cuando se crean. Sin embargo, puede utilizarla conjuntamente con la herramienta Protección de discos de Windows para borrar los nuevos perfiles de usuario que se crean en la partición de Windows cada vez que se reinicia el equipo.

Perfiles de usuario en otros idiomas

Multilingual User Interface Pack (MUI, Interfaz de usuario multilingüe) es un conjunto de archivos de recurso específicos para cada idioma que se puede agregar a la versión en inglés de Windows XP Professional. Con MUI, los usuarios podrán cambiar el idioma de interfaz del sistema operativo a cualquiera de los 33 idiomas admitidos. Una vez instalado el Toolkit, puede especificar el idioma de interfaz de usuario de los usuarios.

Requisitos de MUI

MUI se ejecuta en equipos con Windows XP Professional, pero no en equipos con Windows XP Home Edition.

La interfaz MUI de Windows XP sólo se comercializa a través de programas de licencias por volumen, como el Programa de licencias abiertas de Microsoft (MOLP/Open) y los contratos Select o Enterprise de Microsoft. Puede solicitar una versión OEM de MUI, aunque dicha interfaz no está disponible a través de canales comerciales. Esto tiene por objeto garantizar que los clientes ejecutan la versión en inglés del sistema operativo en sus equipos antes de instalar MUI.

Para obtener más información, consulte el sitio acerca de MUI y sus requisitos para Windows Server 2003, Windows XP y Windows 2000 en el sitio Web de Microsoft (http://go.microsoft.com/fwlink/?LinkId=3925; puede que la página esté en inglés).

Cómo instalar MUI

MUI incluye seis CDs: uno que contiene la versión en inglés de Windows XP Professional y los cinco restantes para los archivos de recursos de la interfaz MUI. Una vez utilizado el primer CD para instalar Windows XP Professional, puede ejecutar el programa MUISetup.exe desde uno de los cinco CDs de recursos para instalar los idiomas de interfaz de usuario. Puede instalar tantos idiomas como sea necesario. También puede quitar idiomas en cualquier momento.

Cómo cambiar el idioma de dispositivos de entrada

Una vez instalada la interfaz MUI, puede utilizar el cuadro de diálogo **Configuración regional y de idioma** del Panel de control para definir los estándares y formatos que el equipo usa, una ubicación de usuario y los idiomas de dispositivos de entrada que utiliza el perfil de usuario.

El idioma de dispositivo de entrada configurado para el equipo indica a Windows cómo reaccionar cuando se escribe texto con el teclado. Cuando se configuran varios idiomas, un usuario puede pasar de un idioma a otro cuando sea necesario. Puede agregar un idioma de dispositivo de entrada a un perfil de usuario siempre que haya instalado el idioma correspondiente de la interfaz MUI.

Para agregar un idioma de dispositivo de entrada en un perfil de usuario:

1. Inicie sesión como el usuario para el que desea agregar un idioma de dispositivo de entrada.
2. Haga clic en **Inicio** y en **Panel de control**.
3. En el Panel de control, haga doble clic en **Opciones regionales, de idioma, y de fecha y hora**.
4. En la ventana **Opciones regionales, de idioma, y de fecha y hora**, haga clic en **Configuración regional y de idioma**.
5. En la ventana **Configuración regional y de idioma**, en la ficha **Idiomas**, en la sección **Servicios de texto e idiomas del dispositivo de entrada**, haga clic en **Detalles**.
6. En el cuadro de diálogo **Servicios de texto e idiomas del dispositivo de entrada**, haga clic en **Agregar**.

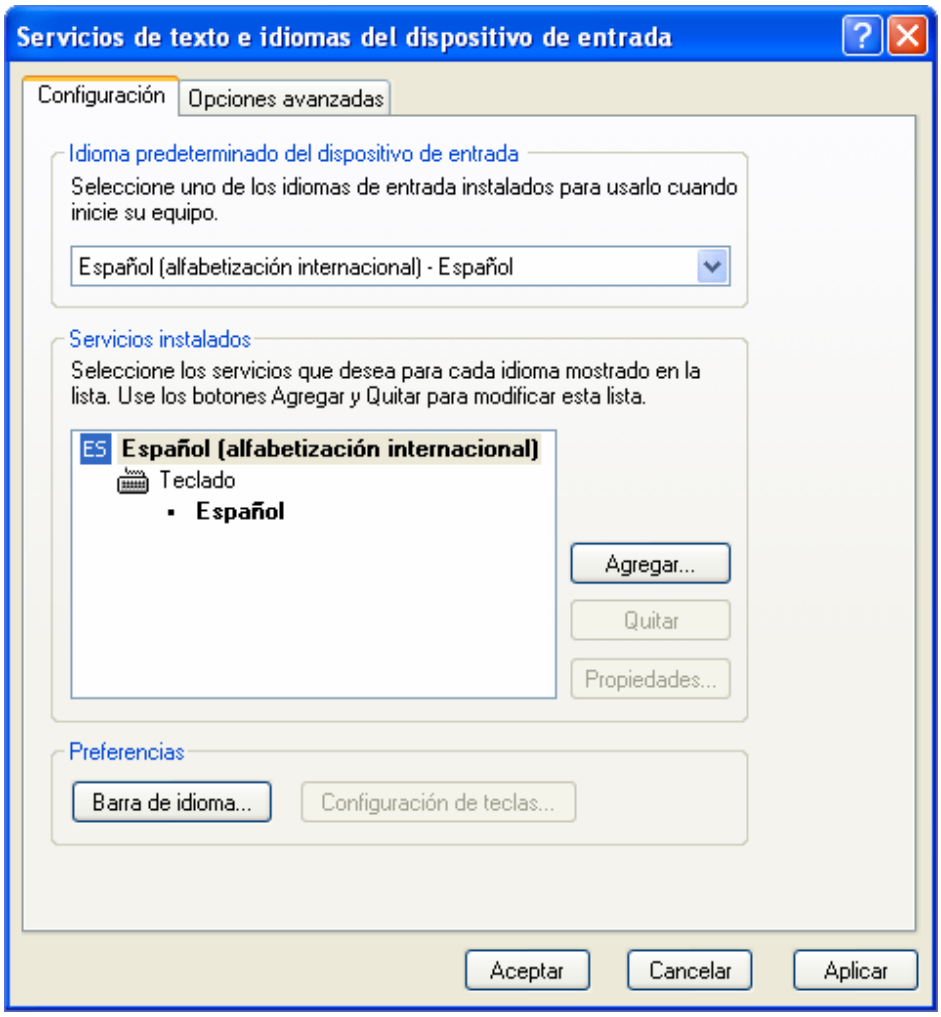

Figura 10.4 *Agregar un idioma de dispositivo de entrada para una cuenta de usuario*

7. En el cuadro de diálogo **Agregar idioma de entrada**, haga clic en el idioma que desee agregar. Para elegir una determinada distribución de teclado, active la casilla de verificación **Distribución del teclado/IME** y elija la distribución adecuada. Para agregar una distribución de teclado o un editor de métodos de entrada (IME), es necesario instalarlo primero en el equipo. Haga clic en **Aceptar**.
8. En el cuadro de diálogo **Servicios de texto e idiomas del dispositivo de entrada**, en la lista desplegable **Idioma predeterminado del dispositivo de entrada**, haga clic en el idioma que desee como predeterminado y haga clic en **Aceptar**.

Apéndice A: Conceptos técnicos elementales

Para configurar Microsoft® Shared Computer Toolkit para Windows® XP y administrar equipos compartidos se requiere estar familiarizado con varias tecnologías y características de Windows.

En este apéndice se tratan los siguientes temas:

- Cuentas y perfiles de usuario
- Cómo funciona la herramienta Administrador de perfiles
- Cómo funciona la herramienta Restricciones del usuario
- Discos y particiones
- Cómo funciona la herramienta Protección de discos de Windows

Cuentas y perfiles de usuario

Una cuenta de usuario es una colección de datos que definen al usuario. En esta información se incluye el nombre del usuario, la contraseña, los grupos a los que pertenece el usuario, la configuración básica del entorno que se aplica al usuario y otros detalles acerca de éste.

Un perfil de usuario es un grupo de valores y archivos que define el entorno que Windows XP carga al iniciar sesión un usuario. Este perfil incluye todos los valores de configuración específicos del usuario, como los elementos de programa, los colores de pantalla, las conexiones de red, las conexiones de impresora, la configuración del *mouse* y el tamaño y la posición de las ventanas. Un perfil de usuario permite especificar diferentes programas, idiomas y características de accesibilidad para cada cuenta de usuario.

Un perfil de usuario se compone de dos partes:

- Un conjunto de carpetas y archivos almacenado en el disco duro. De manera predeterminada, estas carpetas y archivos se almacenan en la carpeta Documents and Settings de la partición de Windows. Como refleja la ilustración siguiente , Windows crea una carpeta por perfil de usuario en la carpeta Documents and Settings. Una carpeta de usuario es un contenedor de programas y otros componentes del sistema operativo que se llenan con subcarpetas y la configuración específica del usuario, como vínculos de acceso directo, iconos de escritorio, programas de inicio, documentos, archivos de configuración, etc. El Explorador de Windows utiliza ampliamente las carpetas de perfil de usuario en carpetas especiales, como el escritorio del usuario, el menú Inicio y la carpeta Mis documentos.
- Un archivo de datos del Registro. El Registro es una base de datos que se utiliza para almacenar la configuración específica del equipo y la configuración específica del usuario en un equipo que ejecuta Windows XP. Parte del Registro se puede guardar en forma de archivos. Windows puede volver a cargar estos archivos para utilizarlos cuando sea necesario. Los perfiles de usuario aprovechan esta característica para proporcionar la funcionalidad del perfil de

usuario. El archivo de Registro del perfil de cada usuario se guarda como un archivo denominado Ntuser.dat en la carpeta del perfil. La información de este archivo se asigna a la parte **HKEY_CURRENT_USER** del Registro siempre que el usuario inicia sesión. Almacena los valores que mantienen las conexiones de red, las configuraciones del Panel de control exclusivas del usuario (como el color del escritorio y la configuración del *mouse*) y la configuración específica de programas.

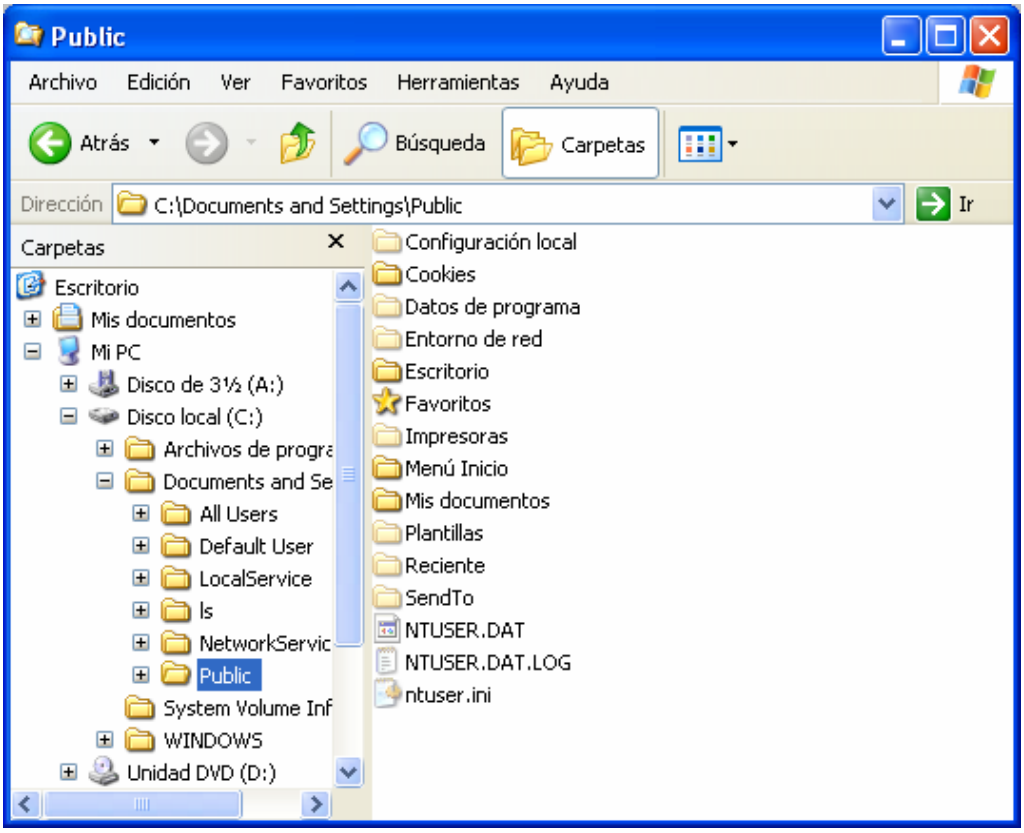

Figura A.1 *Un perfil de usuario es una colección de archivos y carpetas*

Los perfiles de usuario se pueden almacenar en la unidad de disco duro local o establecerse de manera que los datos se muevan con el usuario en el lugar donde inicie sesión. En Windows XP están disponibles los siguientes tipos de perfil de usuario:

- **Perfil de usuario local**. Creado la primera vez que un usuario inicia sesión en un equipo, el perfil de usuario local se almacena en un disco duro local del equipo. Todas las modificaciones efectuadas en un perfil de usuario local son específicas del equipo en el que se hayan realizado.
- **Perfil de usuario móvil**. El perfil local se copia (y almacena) en una ubicación de red de fácil acceso. Este perfil se carga cada vez que el usuario inicia sesión en algún equipo de la red y los cambios realizados en un perfil de usuario móvil se sincronizan con la copia del servidor tras el cierre de sesión.
- **Perfil de usuario obligatorio**. Tipo de perfil que los administradores pueden utilizar para especificar una configuración en particular para los usuarios, un perfil obligatorio es en esencia un perfil móvil en el que el usuario no puede efectuar cambios permanentes. Sólo los administradores de sistemas pueden realizar cambios en los perfiles de usuario obligatorios. Los cambios realizados por el usuario en la configuración de escritorio se pierden cuando el usuario cierra

sesión. Un perfil de usuario obligatorio suele conocerse como *sin estado*, lo que significa únicamente que los cambios efectuados en la sesión no se guardan en el perfil. Esto resulta de utilidad en cuentas de usuario compartidas en las que un usuario no debe poder cambiar la experiencia de otros usuarios. La opción **Bloquear este perfil** de la herramienta Restricciones del usuario funciona al convertir el perfil de usuario en un perfil de usuario obligatorio (y por tanto, un perfil móvil).

- **Perfil de usuario temporal**. Un perfil temporal se emite cada vez que un error impide que se cargue el perfil predeterminado del usuario. Los perfiles temporales se eliminan al final de cada sesión. Los cambios realizados por el usuario en la configuración de escritorio y los archivos se pierden cuando el usuario cierra la sesión.

Cómo funciona la herramienta Administrador de perfiles

Normalmente, un perfil de usuario no se crea hasta que el usuario inicia sesión por primera vez en el equipo con una nueva cuenta de usuario. Si se produce este inicio de sesión, Windows creará automáticamente un nuevo perfil de usuario para esa cuenta. La herramienta Administrador de perfiles permite crear perfiles de usuario sin iniciar sesión como usuario y, lo que es más importante aún, permite crear perfiles en particiones de disco duro alternativas. También se pueden eliminar perfiles de usuario de cuentas de usuario existentes. Esto incluye la posibilidad de eliminar perfiles bloqueados con Restricciones del usuario (que en realidad son perfiles de usuario obligatorios).

Cuando se crea un perfil con la herramienta Administrador de perfiles, ésta simula el inicio de sesión con la cuenta del usuario para que se pueda crear el perfil de usuario (aunque esta simulación es completamente transparente para el usuario). Una vez creado el perfil, si ha especificado que el perfil se cree en una participación alternativa, la herramienta mueve el perfil a dicha partición.

Cómo funciona la herramienta Restricciones del usuario

La mayoría de las restricciones disponibles en la herramienta Restricciones del usuario funcionan mediante la modificación de la configuración del Registro relacionada con un perfil de usuario. Al bloquear un perfil en Restricciones del usuario, el perfil se convierte en un perfil obligatorio que se almacena en /Documents and Settings/<*usuario*>.orig.

Puede ver la lista exacta de restricciones aplicadas a **HKEY_CURRENT_USER** para cada perfil de usuario restringido en el archivo Restrict.xml de la subcarpeta Xml de la carpeta de instalación del Toolkit.

Cuando la herramienta Restricciones del usuario restringe a un usuario, se crea una copia de Restrict.xml denominada User.<*usuario*>.xml que contiene la lista exacta de restricciones aplicadas a dicho perfil de usuario. Este archivo se puede personalizar manualmente (con gran cuidado) y aplicar de nuevo mediante la herramienta de línea de comandos Restrict.wsf en otros perfiles locales. Para ayudar a los operadores avanzados en el proceso de personalización, este apéndice muestra todos los valores de configuración del Registro incluidos en estos archivos .xml y describe lo que hacen.

Microsoft no puede admitir ninguna de las personalizaciones efectuadas en Restrict.xml, porque éste determina gran parte de la interfaz de usuario de la herramienta Restricciones del usuario. Es preferible, y se recomienda especialmente, personalizar un

archivo User.<*usuario*>.xml y procesarlo mediante la herramienta de línea de comandos Restrict.wsf. Sin embargo, si piensa modificar Restrict.xml a pesar de estas recomendaciones técnicas, asegúrese de hacer una copia de seguridad y no modificar las restricciones de la sección Configuración general, porque dicha sección está estrechamente vinculada a los campos codificados de forma rígida de la interfaz de usuario de la herramienta Restricciones del usuario (contenida en Restrict.hta).

Discos y particiones

Una partición es una sección lógica de un disco duro en la que Windows puede escribir datos. Todos los discos duros se deben dividir en particiones para poder utilizarlos. Un disco duro se suele configurar como una gran partición, pero puede dividirse en varias particiones. Cuando un disco duro se divide en particiones, se decide cuánto espacio se asigna a cada una de las particiones.

Por ejemplo, supongamos que el equipo tiene un disco duro de 80 GB. Si ha adquirido el equipo con Windows XP ya instalado o ha instalado Windows XP con las opciones predeterminadas durante la instalación, es probable que el disco duro tenga una sola partición que ocupa los 80 GB del disco. Sin embargo, se podría dividir el mismo disco en varias particiones; tal vez una partición de 40 GB para contener Windows y archivos de programa, una partición de 20 GB para los documentos del usuario y otra partición de 20 GB para un uso futuro.

Cuando se divide un disco duro en particiones, no hay que utilizar todo el espacio del disco duro a la vez. Por ejemplo, en el disco duro de 80 GB, se podría crear una sola partición de 40 GB y dejar el resto del espacio sin particiones. El espacio sin particiones de un disco duro se denomina *sin asignar*.

espacio en disco sin asignar
Espacio que no se utiliza en un disco duro y que no forma parte de ninguna partición.

Windows XP trata cada partición del disco duro como si fuera una unidad independiente, asignando a cada partición una letra de unidad. Normalmente, a la primera partición (y la que suele contener los archivos de sistema de Windows) se le asigna la letra C. En este manual, a la partición que incluye los archivos de Windows se le denomina *partición de Windows*. A las otras particiones se les asignan las letras de unidad a medida que se crean. Las letras de unidad exactas asignadas dependen del momento en que estas particiones se creen (durante la instalación o después) y de las otras unidades que haya en el equipo (como unidades de CD o DVD).

partición de Windows
Partición del disco duro que contiene los archivos de sistema y programas de Windows.

Windows puede reconocer un máximo de cuatro *particiones primarias*. Para sortear esta limitación, Windows permite crear una partición *extendida* (en lugar de una de las cuatro particiones primarias) que actúa como una estructura en la que se puede instalar cualquier cantidad de particiones *lógicas*. La herramienta Protección de discos de Windows reduce el límite de particiones primarias a tres, más el requisito de espacio sin asignar.

Windows XP admite dos tipos de almacenamiento en disco. El primero, denominado *almacenamiento básico*, utiliza particiones para asignar espacio de almacenamiento en Windows. Es el tipo de almacenamiento que se describe a lo largo de este manual. Otro tipo, denominado *almacenamiento dinámico*, ofrece mayor flexibilidad de almacenamiento. El almacenamiento dinámico supera los límites de cuatro particiones por disco y permite un uso más flexible del espacio en disco. Las versiones de servidor de Windows pueden incluso utilizar volúmenes de almacenamiento dinámico para crear conjuntos de discos tolerantes a errores a fin de obtener un almacenamiento confiable.

La herramienta Protección de discos de Windows se ha diseñado para que admita únicamente almacenamiento básico. Los equipos que utilicen almacenamiento dinámico

presentarán errores en el paso 1 de Introducción y no pueden activar Protección de discos de Windows.

Cómo funciona la herramienta Protección de discos de Windows

La herramienta Protección de discos de Windows se ha diseñado para proteger la partición de Windows mediante el rechazo de todos los cambios efectuados desde el último reinicio. Entre los ejemplos de cambios se incluyen las modificaciones de valores de configuración de Windows, la instalación de programas (virus y spyware incluidos) o incluso los cambios sencillos en el entorno de escritorio.

partición de protección
Partición que utiliza la herramienta Protección de discos de Windows para proteger el equipo contra cambios que no se hayan autorizado.

Partición de protección

Para obtener esta protección, la herramienta Protección de discos de Windows crea una partición especial en el espacio en disco sin asignar del disco duro. Esta partición especial se denomina *partición de protección*. La herramienta guarda los cambios realizados durante la sesión de usuario en esa partición especial, lo que hace que ante el usuario parezca como si todo funcionara normalmente. Según se configure la herramienta Protección de discos de Windows, ésta puede descartar los cambios realizados en la partición de protección al finalizar la sesión de usuario o guardarlos en la partición de Windows.

Proceso de actualizaciones críticas

Cuando Protección de discos de Windows está activada, deshabilita el cliente Actualizaciones automáticas de Windows XP, al que se suele obtener acceso a través del Panel de control. Cualquier programación establecida por medio de Actualizaciones automáticas no tendrá efecto en el equipo mientras la herramienta Protección de discos de Windows esté activada. Después de activar Protección de discos de Windows, los cambios de programación de las actualizaciones críticas se deben realizar en la sección **Actualizaciones críticas** de dicha herramienta.

Si desea cambiar la programación de actualizaciones críticas, establezca Protección de discos de Windows para que use la opción de reinicio **Guardar cambios con el siguiente reinicio**, realice los cambios correspondientes y reinicie el equipo.

Una vez activada la herramienta Protección de discos de Windows, encontrará tres tareas en la carpeta Tareas programadas del sistema. Estas tareas, por lo general denominadas At1, At2 y At3, se establecen de manera que se ejecuten una detrás de otra según la programación seleccionada en la herramienta Protección de discos de Windows.

- **At1** muestra un mensaje de encabezado cinco minutos antes de la hora programada para informar a los usuarios interactivos que en 60 segundos se cerrarán automáticamente todas las sesiones por tareas de mantenimiento, tras las cuales el equipo se reiniciará. Este reinicio borra los cambios que puedan no ser de confianza realizados en la partición de Windows a través del comportamiento predeterminado de la herramienta Protección de discos de Windows.
- **At2** muestra el mismo mensaje un minuto antes de la hora programada. Se cierra la sesión de los usuarios interactivos y se deshabilitan todas las cuentas locales excepto las cuentas de administrador del Toolkit y administrador de Windows XP Professional. Las cuentas de dominio no se deshabilitan.
- **At3** se produce a la hora programada y ejecuta la secuencia de comandos real de actualizaciones críticas. Esta secuencia de comandos descarga e instala las

actualizaciones críticas de Microsoft, inicia la secuencia de comandos de antivirus que se identifique y cualquier otra secuencia de comandos que se haya configurado con la herramienta Protección de discos de Windows. A continuación, habilita las cuentas anteriormente deshabilitadas, establece la opción de reinicio de Protección de discos de Windows en **Guardar cambios con el siguiente reinicio** y reinicia el equipo. Después del reinicio, la herramienta Protección de discos de Windows restablece la opción de reinicio a su valor predeterminado: **Borrar cambios en cada reinicio**.

Para permitir que se produzcan otras actualizaciones que se hayan podido programar a la misma hora que las actualizaciones críticas de la herramienta Protección de discos de Windows, la tarea At3 anteriormente descrita esperará un mínimo de 10 minutos antes de reiniciar el equipo. Para aumentar este retraso, cambie el número de minutos en la siguiente clave del Registro (establecida en 10 de manera predeterminada): **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Shared Computer Toolkit\ CriticalUpdatesMins**

Aunque el proceso de actualizaciones críticas de Protección de discos de Windows descarga e instala las actualizaciones, es importante que ni usted ni ninguna cuenta de dominio utilice el equipo para que los cambios en disco no deseados no se guarden junto con las actualizaciones críticas.

Por esta razón, programe el proceso de actualizaciones críticas para que se efectúe durante el período de menor demanda de usuarios del día en el entorno que se administra. Si administra equipos que funcionan 24 horas al día, considere la posibilidad de escalonar la programación de actualizaciones críticas entre los equipos, para que siempre haya algunos equipos disponibles para los usuarios.

Agradecimientos

Microsoft Solutions for Security and Compliance (MSSC) desea dar las gracias a las personas responsables de Microsoft Shared Computer Toolkit para Windows XP.

Programadores

José Maldonado, MSSC

Gareth Jones, MSSC

Rajendran Ganapathy, Infosys Technologies

Sivaraman Kothandaraman, Infosys Technologies

Pruebas de software

Gaurav Singh Bora, Infosys Technologies

Amol Choudhari, Infosys Technologies

Archita Dash, Infosys Technologies

Arjun Radhakrishanan, Infosys Technologies

Harsha Sanagaram, Infosys Technologies

Redacción y edición

John Cobb, Volt

Walter Glenn, Studio B

Walter Glenn, Studio B

Jennifer Kerns, Wadeware

Administración de programas y productos

Derick Campbell, MSSC

John Eversole, Windows Client Marketing

Vínculos

Páginas Web de Shared Computer Toolkit (puede que las páginas estén en inglés)

Página principal de Shared Computer Toolkit
http://go.microsoft.com/fwlink/?LinkId=46755

Página de descarga de Shared Computer Toolkit
http://go.microsoft.com/fwlink/?LinkId=47025

Página de descarga de actualizaciones de Shared Computer Toolkit
http://go.microsoft.com/fwlink/?LinkId=47035

Página de preguntas más frecuentes acerca de Shared Computer Toolkit
http://go.microsoft.com/fwlink/?LinkId=47836

Página de registro de Shared Computer Toolkit
http://go.microsoft.com/fwlink/?LinkId=40009

Página de comunidad y recursos en línea de acceso compartido
http://go.microsoft.com/fwlink/?LinkId=39998

Sitios Web de Microsoft (puede que las páginas estén en inglés)

Sitio de Active Directory de Windows Server 2003
http://go.microsoft.com/fwlink/?LinkId=8596

Sitio de Windows XP Service Pack 2 (SP2)
http://go.microsoft.com/fwlink/?LinkId=25086

Sitio de las Ventajas de Windows Original
http://go.microsoft.com/fwlink/?LinkId=53507

Página de descarga del Servicio de limpieza del subárbol de perfiles de usuario de Microsoft (UPHClean)
http://go.microsoft.com/fwlink/?LinkId=27031

Sitio Web de Microsoft acerca de la protección de equipos
http://go.microsoft.com/fwlink/?LinkId=13366

Sitio de Windows Update
http://go.microsoft.com/fwlink/?LinkId=17289

Sitio de Microsoft Update
http://go.microsoft.com/fwlink/?LinkId=17289

Sitio de Windows Server Update Services
http://go.microsoft.com/fwlink/?LinkId=12524

Sitio acerca del software de Microsoft original
http://go.microsoft.com/fwlink/?LinkId=54028

Sitio de Windows Marketplace (filtrado de contenido)
http://go.microsoft.com/fwlink/?LinkId=54027

Sitio de Windows Marketplace (copia de unidades)
http://go.microsoft.com/fwlink/?LinkId=54495

Sitio acerca de recursos en línea para el uso de equipos públicos
http://go.microsoft.com/fwlink/?LinkId=39997

Sitio del kit de recursos de Windows XP (automatización y personalización de instalaciones)
http://go.microsoft.com/fwlink/?LinkId=54497

Sitio del kit de recursos de Windows XP (uso de Sysprep para implementar Windows XP)
http://go.microsoft.com/fwlink/?LinkId=54491

Sitio de Multilingual User Interface Pack (MUI)
http://go.microsoft.com/fwlink/?LinkId=3925

Artículo acerca del uso de directivas de restricción de software para protegerse contra software no autorizado
http://go.microsoft.com/fwlink/?LinkId=14508

Herramientas y recursos de terceros (puede que las páginas estén en inglés)

Adobe Acrobat Reader
http://go.microsoft.com/fwlink/?LinkId=57398

Symantec Norton PartitionMagic 8.0
http://go.microsoft.com/fwlink/?LinkId=47542

TeraByte BootIt NG
http://go.microsoft.com/fwlink/?LinkId=46756

Computer Associates eTrust 7.0
http://www3.ca.com/Solutions/Product.asp?ID=156

McAfee
http://www.mcafee.com

Symantec Norton Ghost 9.0
http://www.symantec.com/sabu/ghost/ghost_personal/

Acronis TrueImage 8.0
http://www.acronis.com/enterprise/products/ATICW/

WebSense
http://www.websense.com/

Secure Computing
http://www.securecomputing.com/

Faronics
http://www.faronics.com

Fortres Grand
http://www.fortres.com

Artículos útiles (puede que las páginas estén en inglés)

Artículo 307881 de Microsoft Knowledge Base sobre cómo convertir un volumen FAT16 o un volumen FAT32 en un sistema de archivos NTFS en Windows XP
http://go.microsoft.com/fwlink/?LinkId=53509

Artículo acerca de las ventajas de utilizar NTFS en Windows XP
http://go.microsoft.com/fwlink/?LinkId=54026

Artículo acerca de cómo automatizar y personalizar instalaciones
http://go.microsoft.com/fwlink/?LinkId=54494

Artículo acerca de determinados programas que no funcionan correctamente si se inicia sesión mediante una cuenta de usuario limitada
http://go.microsoft.com/fwlink/?LinkId=54487

Sitio Web de creación de imágenes de TechNet
http://go.microsoft.com/fwlink/?LinkId=54493

Artículo acerca de cómo personalizar instalaciones de Sysprep
http://go.microsoft.com/fwlink/?LinkId=54494

Artículo acerca de la descripción de la activación de productos de Microsoft
http://go.microsoft.com/fwlink/?LinkId=54496

Artículo de información general acerca de perfiles de usuario
http://go.microsoft.com/fwlink/?LinkId=54488

Artículo acerca de cómo asignar un perfil de usuario obligatorio en Windows XP
http://go.microsoft.com/fwlink/?LinkId=54489

Artículo acerca del uso de directivas de restricción de software para protegerse contra software no autorizado
http://go.microsoft.com/fwlink/?LinkId=14508

Índice

—U—

—V—

—W—