Guía de administración de computadora de escritorio

Computadoras de escritorio empresariales

Número de parte del documento: 312947-162

Septiembre de 2003

Esta guía proporciona definiciones e instrucciones para el uso de los recursos de seguridad y de Intelligent Manageability que vienen preinstaladas en modelos seleccionados.

ADVERTENCIA: El texto presentado de esta manera indica que si no se siguen las instrucciones se pueden producir lesiones corporales o pérdida de la vida.

PRECAUCIÓN: El texto presentado de esta manera indica que si no se siguen las instrucciones se pueden producir daños a los equipos o pérdida de información.

Guía de administración de computadora de escritorio
Computadoras de escritorio empresariales

Segunda Edición: Septiembre de 2003
Número de parte del documento: 312947-162

Contenido

Guía de administración de computadora de escritorio

Indice

Guía de administración de computadora de escritorio

Intelligent Manageability de HP ofrece soluciones basadas en estándares para administrar y controlar computadoras de escritorio, estaciones de trabajo y notebook en un entorno de red. HP fue pionero en la administrabilidad de computadoras de escritorio en 1995 con la introducción de las primeras computadoras personales de escritorio completamente administrables de la industria. HP posee una patente sobre tecnología de administrabilidad. Desde entonces, HP lideró un amplio esfuerzo en la industria para desarrollar las normas y la infraestructura necesarias para implantar, configurar y administrar eficientemente computadoras de escritorio, estaciones de trabajo y notebook. HP trabaja en estrecha colaboración con proveedores líderes de soluciones de software de administración para asegurar la compatibilidad entre Intelligent Manageability y esos productos. Intelligent Manageability es un aspecto importante de nuestro amplio compromiso de proporcionarle soluciones para el ciclo de vida de la computadora que lo ayuden durante las cuatro fases del ciclo de vida de las computadoras de escritorio: planificación, implantación, administración y transiciones.

Las capacidades y recursos clave de la administración de computadoras de escritorio son:

- Configuración e implantación iniciales
- Instalación remota del sistema
- Actualización y administración de software
- Flash ROM
- Seguimiento y seguridad de activos
- Notificación y recuperación de fallas

El soporte de los recursos específicos descritos en esta guía puede variar según el modelo o la versión del software.

Configuración e implantación iniciales

La computadora viene con una imagen preinstalada del software del sistema. Luego de un breve "desempaquetamiento" del software, la computadora queda lista para ser usada.

Puede ser que prefiera reemplazar la imagen de software preinstalada por un conjunto personalizado de software de sistema y de aplicación. Hay varios métodos para implantar una imagen de software personalizada. Estos incluyen:

- Instalación de aplicaciones de software adicionales, luego de desempaquetar la imagen de software preinstalada.
- Uso de las herramientas de implantación de software, como Altiris Deployment Solution™, para reemplazar al software preinstalado con una imagen de software personalizada.
- Uso de un proceso de clonación de disco para copiar el contenido de un disco duro a otro.

El mejor método de implantación depende de los procesos y del entorno de tecnología de la información. La sección Implantación de PC, del sitio Web HP Lifecycle Solutions (http://h18000.www1.hp.com/solutions/pcsolutions) provee informaciones para ayudarlo a seleccionar el mejor método de implantación.

El *CD Restore Plus!*, configuración basada en ROM y hardware ACPI brindan más ayuda con recuperación del software del sistema, administración y resolución de problemas de configuración y administración de la energía.

Instalación remota del sistema

La Instalación remota del sistema permite iniciar y configurar el sistema usando la información de software y de configuración ubicada en un servidor de red iniciando el Preboot Execution Environment (PXE). El recurso de instalación remota del sistema se usa generalmente como una herramienta de instalación y configuración del sistema y se puede utilizar para las siguientes tareas:

- Formateo de un disco duro.
- Implementación de una imagen de software en una o más computadoras nuevas.
- Actualización a distancia de la BIOS del sistema en ROM flash ("Remote ROM Flash" en la página 8)
- Configuración de los parámetros de la BIOS del sistema

Para iniciar la instalación remota del sistema, presione **F12** cuando aparezca el mensaje F12 = Network Service Boot en la esquina inferior derecha de la pantalla del logotipo HP. Siga las instrucciones en pantalla para continuar con el proceso. El orden de arranque predeterminado es un parámetro de configuración que puede ser alterado para que siempre intente el arranque PXE.

HP y Altiris, Inc. se asociaron para proporcionar herramientas diseñadas para hacer que la tarea de implantación y administración de las computadoras empresariales sea más fácil y rápida, lo que finalmente reduce el costo total de propiedad y hace que las computadoras HP sean las computadoras cliente más administrables en el medio empresarial.

Actualización y administración de software

HP proporciona diversas herramientas para administrar y actualizar el software en las computadoras de escritorio y estaciones de trabajo: Altiris; Altiris PC Transplant Pro; HP Client Manager Software, una solución Altiris; System Software Manager; Proactive Change Notification y Active Update.

Software HP Client Manager

El software Intelligent HP Client Manager (HP CMS) se integra completamente con la tecnología HP Intelligent Manageability dentro de Altiris para proporcionar una capacidad superior de administración de hardware para HP acceder a dispositivos, que incluye:

- Vistas detalladas de inventario de hardware para administración de activos.
- Monitoreo y diagnóstico del estado de la computadora.
- Notificación proactiva de cambios en el entorno de hardware.
- Información accesible a través de la Web de detalles fundamentales de la empresa, tales como máquinas con advertencias térmicas, alertas de memoria y otros.
- Actualización remota de software del sistema, como por ejemplo, controladores de dispositivos y BIOS de la ROM.
- Alteración a distancia del orden de arranque.

Para obtener más informaciones acerca del HP Client Manager, visite http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Solutions

HP Client Manager Solutions proporciona una administración de hardware centralizada de los dispositivos cliente HP para las siguientes áreas del ciclo de vida TI.

- Administración de inventario y activos
  - Conformidad con licencia de SW
  - Rastreo e información de la computadora
  - Contrato de leasing, rastreo de activo fijo
- Implantación y migración
  - Migración Microsoft Windows 2000 o Windows XP Professional o Home Edition
  - Implantación del sistema
  - Migración de personalidad
- Mesa de ayuda y solución de problemas
  - Administración de papeletas de la mesa de ayuda
  - Solución de problemas remota
  - Solución de problemas a distancia
  - Recuperación ante desastres de cliente
- Administración de software y operaciones
  - Administración continua de computadora de escritorio
  - Desarrollo del software del sistema HP
  - Autorreparación de aplicaciones

En algunos modelos de computadoras de escritorio y notebook, se incluye el agente de administración Altiris como parte del software precargado. Este agente activa la comunicación con el software Altiris Solution, que se puede usar para finalizar el desarrollo de nuevo hardware o la migración de personalidad a un nuevo sistema operativo utilizando asistentes fáciles de seguir. El software Altiris Solutions ofrece capacidades de distribución de software fáciles de usar. Cuando el software Altiris Solutions se utiliza en conjunto con System Software Manager o HP Client Manager, los administradores también pueden actualizar la BIOS de la ROM y el software controlador de los dispositivos desde una consola central.

Para obtener más informaciones, visite http://www.compaq.com/easydeploy.

Altiris PC Transplant Pro

Altiris PC Transplant Pro ofrece una migración de computadoras sin complicaciones al conservar la configuración, las preferencias y los datos antiguos y migrarlos al nuevo entorno rápida y fácilmente. Las actualizaciones llevan minutos y no horas o días y la computadora de escritorio y las aplicaciones se ven y funcionan tal como los usuarios lo esperan.

Para obtener más informaciones y detalles sobre cómo descargar una versión de evaluación plenamente funcional por 30 días, visite http://h18000.www1.hp.com/im/prodinfo.html#deploy.

System Software Manager

System Software Manager (SSM) es una utilidad que permite actualizar el software a nivel de sistema en varios sistemas simultáneamente. Cuando se ejecuta en un sistema de computadoras cliente, SSM detecta versiones de hardware y de software y luego actualiza el software correspondiente desde un repositorio central, también conocido como almacén de archivos. Las versiones de controladores admitidas por SSM se indican con un icono especial en el sitio Web de descarga de controladores y en el CD de Software de soporte. Para descargar la utilidad o para obtener más información sobre SSM, visite http://h18000.www1.hp.com/im/ssmwp.html.

Notificación proactiva de cambios (Proactive Change Notification)

El programa de Notificación proactiva de cambios utiliza el sitio Web Subscriber's Choice para proactivamente y automáticamente:

- Enviarle e-mails de Notificación proactiva de cambios (PCN) informando sobre cambios de hardware y software de la mayoría de las computadoras y los servidores comerciales, con anticipación de hasta 60 días.
- Enviarle e-mails que contenienen Boletines al Cliente, Avisos al Cliente, Notas al Cliente, Boletines de Seguridad y alertas de Controladores para la mayoría de las computadoras y los servidores comerciales.

Usted crea su propio perfil para asegurar que reciba sólo la información relevante para un entorno específico de TI. Para saber más acerca del programa de Notificación proactiva de cambios y crear un perfil personalizado, visite http://www.hp.com/go/pcn.

ActiveUpdate

ActiveUpdate es una aplicación basada en cliente de HP. El cliente ActiveUpdate se ejecuta en el sistema local y usa el perfil definido por el usuario para descargar en forma proactiva y automática actualizaciones de software para la mayoría de las computadoras y de los servidores comerciales de HP. Dichas actualizaciones de software descargadas pueden ser distribuidas inteligentemente entre las máquinas para las cuales se destinan, a través del Software HP Client Manager y System Software Manager.

Para saber más acerca de ActiveUpdate, descargar la aplicación y crear su perfil de cliente, visite http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html.

Flash ROM

La computadora viene con una flash ROM (memoria de sólo lectura) reprogramable. Al establecer una contraseña de configuración en Computer Setup (F10), puede proteger la ROM contra actualizaciones y sobreescrituras accidentales. Esto es importante para garantizar la integridad operativa de la computadora. Si necesita o desea actualizar la ROM, puede:

- Pedir un disquete ROMPaq™ actualizado a HP.
- Descargar las imágenes más recientes de ROMPaq desde http://h18000.www1.hp.com/im/ssmwp.html.

PRECAUCIÓN: Para una máxima protección de la ROM, asegúrese de establecer una contraseña de configuración. La contraseña de configuración impide actualizaciones no autorizadas de la ROM. System Software Manager permite al administrador del sistema establecer la contraseña de configuración en una o más computadoras simultáneamente. Para obtener más información, visite http://h18000.www1.hp.com/im/ssmwp.html.

Remote ROM Flash

Remote ROM Flash permite que el administrador del sistema actualice en forma segura la ROM en computadoras HP remotas, directamente desde la consola centralizada de administración de red. La habilitación del administrador del sistema para que realice esta tarea de manera remota en varias computadoras y computadoras personales, genera un desarrollo uniforme y un mayor control de las imágenes de la ROM de las computadoras HP en la red. También permite una mayor productividad y un menor costo total de propiedad.

La computadora debe estar encendida o se debe encender a través de activación remota (Remote Wakeup) para aprovechar Remote ROM Flash.

Para obtener más información acerca de Remote ROM Flash, consulte el Software HP Client Manager o el System Software Manager en http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

la utilidad HPQFlash es utilizada para actualizar o restaurar localmente la ROM de sistema individualmente en las computadoras, a través de un sistema operativo Windows.

Para obtener más informaciones acerca de HPQFlash, visite http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

FailSafe Boot Block ROM

FailSafe Boot Block ROM permite la recuperación del sistema en el improbable evento de una falla en la flash ROM, por ejemplo, si se produce una falla de alimentación durante una actualización de la ROM. El Bloque de inicialización es una sección de la ROM protegida contra flash que verifica la existencia de flash ROM válida del sistema al encender el equipo.

- Si la ROM del sistema es válida, éste se inicia normalmente.
- Si la ROM del sistema no pasa la comprobación de validación, FailSafe Boot Block ROM entrega un soporte suficiente para iniciar el sistema desde un disquete ROMPaq, el cual programará la ROM del sistema con una imagen válida.

Cuando el bootblock detecta una ROM de sistema inválida, el LED de energía del sistema parpadea en ROJO por 8 veces, una por segundo, seguido de una pausa de 2 segundos. Además, se escucharán 8 señales sonoras simultáneas. En la pantalla aparecerá un mensaje de modo de recuperación del Bloque de inicialización (algunos modelos).

Para recuperar el sistema después de que haya ingresado en el modo de recuperación del bloque de inicialización, realice los siguientes pasos:

1. Si hay un disquete en la unidad de disquetes, retírelo y apague la computadora.
2. Inserte un disquete ROMPaq en la unidad de disquete.
3. Encienda el equipo.
4. Si no se encuentra ningún disquete ROMPaq, se le solicitará que inserte uno y que reinicie la computadora.
5. Si se estableció una contraseña de configuración, la luz Bloq Mayús se encenderá y se le solicitará ingresar la contraseña.
6. Ingrese la contraseña de configuración.
7. Si el sistema se inicia con éxito del disquete y la ROM se reprograma correctamente, las tres luces del teclado se encenderán. Una serie de sonidos de “tono ascendente” también indican un término exitoso del procedimiento.
8. Retire el disquete y apague la computadora.
9. Reencienda la computadora para reiniciarla.

La tabla siguiente lista las varias combinaciones de luces del teclado que utiliza el Boot Block ROM (cuando un teclado PS/2 está conectado a la computadora), y explica el significado y la acción asociada a cada combinación.

Combinaciones de luces del teclado usadas por Boot Block ROM

Modo Failsafe Boot Block	Color del LED del teclado	Teclado Actividad del LED de teclado	Estado/mensaje
Bloq Num	Verde	Encendido	Disquete ROMPaq no está presente, está dañado o la unidad no está lista.*
Bloq Mayús	Verde	Encendido	Ingrese contraseña.
Bloq Num, Mayús y Despl	Verde	Parpadeo de Encendido en secuencia, una a la vez —N, M, D	Teclado bloqueado en el modo de red.
Bloq Num, Mayús y Despl	Verde	Encendido	Flash ROM de bloque de inicialización exitosa. Apague el equipo y enciéndalo para reiniciarlo.

✎ Las luces de diagnóstico no destellan en teclados USB.

Copiando la Configuración

Los procedimientos siguientes permiten que el administrador copie fácilmente una configuración en otras computadoras del mismo modelo. Esto permite una configuración más rápida y más uniforme de varias computadoras.

Ambos procedimientos requieren una unidad de disquete o un dispositivo de medios flash USB admitido, tal como un HP Drive Key.

Copiar en una Única Computadora

PRECAUCIÓN: Cada modelo tiene su configuración específica. Puede ocurrir corrupción del sistema de archivos si las computadoras de origen y destino son de modelos distintos. Por ejemplo, no copie la configuración de una computadora de escritorio Ultra Delgada D510 para una computadora D510 e-pc.

1. Seleccione una configuración para copia. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Pulse la tecla **F10** así que encienda la luz verde del monitor. Pulse **Intro** para saltar la pantalla de título, si fuese necesario.

Si no pulsa la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y pulsar la tecla **F10** otra vez para acceder a la utilidad.

3. Inserte un disquete o un dispositivo de medios flash USB.
4. Haga clic en **Archivo > Guardar en disquete**. Siga las instrucciones en pantalla para crear el disquete o el dispositivo de medios flash USB de configuración.
5. Apague la computadora por configurar e inserte el disquete o dispositivo de medios flash USB de configuración.
6. Encienda la computadora para que se configure. Pulse la tecla **F10** así que encienda la luz verde del monitor. Pulse **Intro** para saltar la pantalla de título, si fuese necesario.
7. Haga clic en **Archivo > Restaurar desde disquete** y siga las instrucciones en pantalla.
8. Reinicie la computadora cuando la configuración esté concluida.

Copiar en Varias Computadoras

PRECAUCIÓN: Cada modelo tiene su configuración específica. Puede ocurrir corrupción del sistema de archivos si las computadoras de origen y destino son de modelos distintos. Por ejemplo, no copie la configuración de una computadora de escritorio Ultra Delgada D510 para una computadora D510 e-pc.

Este método es más lento para preparar la configuración del disquete o del dispositivo de medios flash USB, pero la copia de la configuración en la computadora-blanco es significativamente más rápida.

No se puede crear un disquete arrancable en Windows 2000. Se necesita un disquete arrancable para este procedimiento o para crear un dispositivo arrancable de medios flash USB. Si Windows 9x o Windows XP no está disponible para uso para crear un disquete arrancable, use el método de copia en una única computadora (vea "Copiar en una Única Computadora" en la página 11).

1. Cree un disquete arrancable o un dispositivo de medios flash USB. Vea "Disquete arrancable" en la página 13, "Dispositivo de medios flash USB admitidos" en la página 14, o "Dispositivo de medios flash USB no admitidos" en la página 17.

PRECAUCIÓN: Ni todas las computadoras pueden ser iniciadas desde un dispositivo de medios flash USB. Si el orden predefinido de inicio en Computer Setup (F10) lista el dispositivo USB antes del disco duro, la computadora puede ser iniciada desde un dispositivo de medios flash USB. De lo contrario, se debe utilizar un disquete arrancable.

2. Seleccione una configuración para copia. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
3. Pulse la tecla **F10** así que encienda la luz verde del monitor. Pulse **Intro** para saltar la pantalla de título, si necesario.

Si no pulsa la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y pulsar la tecla **F10** otra vez para acceder a la utilidad.

4. Inserte el disquete o el dispositivo de medios flash USB arrancable.

5. Haga clic en **Archivo > Guardar en disquete.** Siga las instrucciones en pantalla para crear el disquete o el dispositivo de medios flash USB de configuración.
6. Descargue una utilidad de la BIOS para copiar la configuración (repset.exe) y cópiela en el disquete de configuración o en el dispositivo de medios flash USB. Se puede encontrar dicha utilidad en http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.
7. En el disquete de configuración o en el dispositivo de medios flash USB, cree un archivo autoexec.bat que contenga el siguiente comando:

   repset.exe
8. Apague la computadora por configurar. Inserte el disquete o el dispositivo de medios flash USB de configuración y encienda la computadora. La utilidad de configuración será ejecutada automáticamente.
9. Reinicie la computadora cuando la configuración esté concluida.

Creación de un dispositivo arrancable

Disquete arrancable

Estas instrucciones son para el Windows XP Professional y Home Edition. Windows 2000 no admite la creación de disquetes arrancables.

1. Inserte un disquete en la unidad de disquetes.
2. Haga clic en **Inicio**, luego haga clic en **Mi PC**.
3. Haga clic con el botón derecho en la letra de la unidad de disquete y haga clic en **Formatear.**
4. Seleccione la casilla de verificación **Crear un disco de inicio del MS-DOS**, luego haga clic en **Inicio**.

Vuelva a “Copiar en Varias Computadoras” en la página 12.

Dispositivo de medios flash USB admitidos

Los dispositivos admitidos, tales como un HP Drive Key o un DiskOnKey, tienen una imagen precargada para simplificar el proceso de inicio. Si el Drive Key utilizado no posee dicha imagen, utilice el procedimiento presentado más adelante en esta sección (vea "Dispositivo de medios flash USB no admitidos" en la página 17).

PRECAUCIÓN: Ni todas las computadoras pueden ser iniciadas desde un dispositivo de medios flash USB. Si el orden predefinido de inicio en Computer Setup (F10) lista el dispositivo USB antes del disco duro, la computadora puede ser iniciada desde un dispositivo de medios flash USB. De lo contrario, se debe utilizar un disquete arrancable.

Para crear un dispositivo de medios flash USB arrancable, usted necesita:

- Uno de los sistemas siguientes:
  - Computadora de escritorio Compaq Evo D510 Ultra delgada
  - Compaq Evo D510 Minitorre Convertible/Fator de Forma Pequeña
  - Computadora de Escritorio empresarial HP Compaq d530 - Ultra-slim Desktop, Small Form Factor, o Convertible Minitower
  - Notebook Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c, o N1000c
  - Notebook Compaq Presario 1500 o 2800

  Dependiendo de cada BIOS, sistemas futuros también pueden admitir el inicio con el HP Drive Key.

PRECAUCIÓN: Si está utilizando una computadora que no sea una de las indicadas arriba, verifique si el orden predefinido de inicio de Computer Setup (F10) lista el dispositivo USB antes del disco duro.

- Uno de los siguientes módulos de almacenamiento:
  - 16MB HP Drive Key
  - 32MB HP Drive Key
  - 32MB DiskOnKey

- ❏ 64MB HP Drive Key
- ❏ 64MB DiskOnKey
- ❏ 128MB HP Drive Key
- ❏ 128MB DiskOnKey

■ Un disquete arrancable de DOS con los programas FDISK y SYS. Si SYS no está disponible, se puede usar FORMAT, pero todos los archivos existentes en el Drive Key serán perdidos.

1. Apague la computadora.
2. Inserte el Drive Key en uno de los puertos USB de la computadora y retire todos los dispositivos USB de almacenamiento, excepto las unidades USB de disquetes.
3. Inserte un disquete arrancable de DOS con FDISK.COM y los archivos SYS.COM o FORMAT.COM en una unidad de disquete y encienda la computadora para arrancar desde el disquete de DOS.
4. Ejecute FDISK desde el prompt A:\ , escribiendo **FDISK** y pulsando Intro. Cuando se solicite, haga clic en **Sí** (**Y**) para activar el reconocimiento de discos grandes.
5. Presione Choice [**5**] para exhibir las unidades del sistema. El Drive Key será la unidad más semejante al tamaño de una de las unidades listadas. Será usualmente la última unidad de la lista. Observe la letra de la unidad.

   Unidad Drive Key: _____

PRECAUCIÓN: Si una unidad no corresponde al Drive Key, no siga adelante. Puede ocurrir la pérdida de datos. Verifique todos los puertos USB para ver si contienen otros dispositivos de almacenamiento. Si se encuentra alguno, retírelo, reinicie la computadora y prosiga desde el paso 4. Si no se encuentra ninguno, el sistema no admite el Drive Key o el Drive Key es defectuoso. NO siga adelante en su intento de hacer arrancable el Drive Key.

6. Salga de FDISK pulsando la tecla **Esc** para regresar al prompt A:\.
7. Si su disquete arrancable de DOS contiene SYS.COM, salte al paso 8. De lo contrario, salte al paso 9.
8. En el prompt A:\, ingrese **SYS x:** donde la 'x' representa la letra de la unidad observada arriba. Salte al paso 13.

PRECAUCIÓN: Verifique si informó la letra correcta de la unidad del Drive Key.

Luego de la transferencia de los archivos de sistema, SYS regresará al prompt A:\.

9. Copie todos los archivos que desea desde su Drive Key para un directorio temporal de otra unidad (por ejemplo, el disco duro interno del sistema).
10. En el prompt A:\, ingrese **FORMAT /S X:** donde la 'x' representa la letra de la unidad observada arriba.

PRECAUCIÓN: Verifique si informó la letra correcta de la unidad del Drive Key.

FORMAT exhibirá una o más advertencias y preguntará, todas las veces, si desea continuar. Pulse **s** en todas las veces. FORMAT formateará el Drive Key, incluirá los archivos de sistema y solicitará una Etiqueta de Volumen.

11. Pulse **Intro** para no informar ninguna etiqueta, o informe una, si desea.
12. Copie todos los archivos que guardó en el paso 9 en su Drive Key.
13. Retire el disquete y reinicie la computadora. La computadora reiniciara a través del Drive Key como unidad C.

El orden predefinido de inicio varía según la computadora, y se lo puede cambiar en Computer Setup (F10).

Si utilizó una versión DOS desde Windows 9x, verá una breve pantalla con el logotipo de Windows. Si no desea esta pantalla, incluya un archivo con longitud cero llamado LOGO.SYS en el directorio raíz del Drive Key.

Vuelva a "Copiar en Varias Computadoras" en la página 12.

Dispositivo de medios flash USB no admitidos

PRECAUCIÓN: Ni todas las computadoras pueden ser iniciadas desde un dispositivo de medios flash USB. Si el orden predefinido de inicio en la Computer Setup (F10) lista el dispositivo USB antes del disco duro, la computadora puede ser iniciada desde un dispositivo de medios flash USB. De lo contrario, se debe utilizar un disquete arrancable.

Para crear un dispositivo de medios flash USB arrancable, usted necesita:

- Uno de los sistemas siguientes:
  - Computadora de escritorio Compaq Evo D510 Ultra delgada
  - Compaq Evo D510 Minitorre Convertible/Fator de Forma Pequeña
  - Computadora de Escritorio empresarial HP Compaq d530 - Ultra-slim Desktop, Small Form Factor, o Convertible Minitower
  - Notebook Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c, o N1000c
  - Notebook Compaq Presario 1500 o 2800

  Dependiendo de cada BIOS, sistemas futuros también pueden admitir el inicio con un dispositivo de medios flash USB.

PRECAUCIÓN: Si está utilizando una computadora que no sea una de las indicadas arriba, verifique si el orden predefinido de inicio de Computer Setup (F10) lista el dispositivo USB antes del disco duro.

- Un disquete arrancable de DOS con los programas FDISK y SYS. Si SYS no está disponible, se puede usar FORMAT, pero todos los archivos existentes en el Drive Key serán perdidos.

1. Si existe alguna tarjeta PCI en el sistema que posee unidades SCSI, ATA RAID o SATA conectadas, apague la computadora y desconecte el cable de energía.

PRECAUCIÓN: El cable de energía DEBE ser desconectado.

2. Abra la computadora y quite las tarjetas PCI.

3. Inserte el dispositivo de medios flash USB en uno de los puertos USB de la computadora y retire todos los dispositivos USB de almacenamiento, excepto las unidades USB de disquetes. Cierre la cubierta de la computadora.
4. Conecte el cable de energía y encienda la computadora. Cuando se vuelva verde la luz del monitor, presione la tecla **F10** para entrar en Computer Setup.
5. Va a los dispositivos Avanzados/PCI para desactivar los controladores IDE y SATA. Al desactivar el controlador SATA, observe el IRQ al cual el controlador está asignado. Necesitará reasignar el IRQ después. Salga de la configuración confirmando los cambios.

   IRQ de SATA: _____
6. Inserte un disquete arrancable de DOS con FDISK.COM y los archivos SYS.COM o FORMAT.COM en una unidad de disquete y encienda la computadora para arrancar desde el disquete de DOS.
7. Ejecute el FDISK y excluya todas las particiones existentes en el dispositivo de medios flash USB. Cree una nueva partición y márquela como activa. Salga del FDISK pulsando la tecla **Esc**.
8. Si el sistema no reinició automáticamente al salir de FDISK, pulse **Ctrl**+**Alt**+**Supr** para reiniciar a través del disquete de DOS.
9. En el prompt A:\, escriba **FORMAT C: /S** y presione **Intro**. FORMAT formateará el dispositivo de medios flash USB, incluirá los archivos de sistema y solicitará una Etiqueta de Volumen.
10. Presione **Intro** para no informar ninguna etiqueta, o informe una, si desea.
11. Apague la computadora y desconecte el cable de energía. Abra la computadora y reinstale todas las tarjetas PCI anteriormente retiradas. Cierre la cubierta de la computadora.
12. Conecte el cable de energía, retire el disquete y encienda la computadora.
13. Cuando se vuelva verde la luz del monitor, presione la tecla **F10** para entrar en Computer Setup.
14. Va a Dispositivos Avanzados/PCI y reactive los controladores IDE y SATA que fueron desactivados en el paso 5. Devuelva al controlador SATA su IRQ original.

15. Guarde los cambios y salga. La computadora reiniciará a través del dispositivo de medios flash USB como la unidad C.

El orden predefinido de inicio varía según la computadora, y se lo puede cambiar en Computer Setup (F10).

Si utilizó una versión DOS desde Windows 9x, verá una breve pantalla con el logotipo de Windows. Si no desea esta pantalla, incluya un archivo con longitud cero llamado LOGO.SYS en el directorio raíz del Drive Key.

Vuelva a "Copiar en Varias Computadoras" en la página 12.

Botón de encendido de dos estados

Con Advanced Configuration and Power Interface (ACPI) activada para Windows 2000 y Windows XP Professional y Home Edition, el botón de encendido puede funcionar como interruptor de encendido/apagado o como un botón de suspensión. El recurso de suspensión no apaga completamente el equipo, sino que hace que la computadora entre en una suspensión de baja alimentación. Esto permite un apagado rápido sin cerrar aplicaciones y un regreso rápido al mismo estado operacional sin pérdida de datos.

Para cambiar la configuración del botón de encendido, realice los siguientes pasos:

1. En Windows 2000, haga clic en el **botón Inicio,** luego seleccione **Configuración > Panel de control > Opciones de energía.**

   En Windows XP Professional y Home Edition, haga clic en el **botón Inicio,** luego seleccione **Panel de control > Rendimiento y mantenimiento > Opciones de energía.**

2. En **Propiedades de Opciones de energía,** seleccione la ficha **Avanzadas**.

3. En la sección **botones de Encendido**, seleccione la configuración del botón de energía deseado.

Después de configurar el botón de encendido para que funcione como botón de suspensión, presione el botón de encendido para poner el sistema en un estado de muy baja alimentación (suspensión). Presione nuevamente el botón para sacar rápidamente el sistema de la suspensión y dejarlo en estado de alimentación completa. Para apagar completamente todo el equipo, mantenga presionado el botón de encendido durante cuatro segundos.

PRECAUCIÓN: No utilice el botón de encendido para apagar la computadora, a menos que el sistema no responda; apagar la computadora sin interacción con el sistema operativo puede causar daños o pérdida de datos en el disco duro.

Sitio World Wide Web

Los ingenieros de HP prueban y depuran rigurosamente el software desarrollado por HP y por proveedores externos, desarrollando software de soporte específico del sistema operativo a fin de garantizar el más alto nivel de rendimiento, compatibilidad y fiabilidad para las computadoras HP.

Al hacer la transición a sistemas operativos nuevos o corregidos, es importante implementar el software de soporte diseñado para ese sistema operativo. Si piensa ejecutar una versión de Microsoft Windows distinta a la versión que viene con la computadora, debe instalar los controladores de dispositivos y las utilidades correspondientes para asegurarse de que todas los recursos sean admitidos y funcionen correctamente.

HP hizo que la tarea de ubicar, acceder, evaluar e instalar el software de soporte más reciente sea más sencilla. Puede descargar el software desde http://www.hp.com/la/soporte.

El sitio Web contiene los controladores de dispositivos, utilidades y las imágenes de la ROM apta para flash más recientes, necesarios para ejecutar el último sistema operativo Microsoft Windows en la computadora HP.

Bloques de creación y socios

Las soluciones de administración de HP se integran con otras aplicaciones de administración de sistemas, y están basadas en estándares del ramo, tales como:

- Desktop Management Interface (DMI) 2.0
- Tecnología Wake on LAN
- ACPI
- SMBIOS
- Soporte de Pre-boot Execution (PXE)

Seguimiento y seguridad de activos

Los recursos de seguimiento de activos incorporados a la computadora suministran datos esenciales de seguimiento de activos que se pueden administrar a través del HP Insight Manager, HP Client Manager o de otras aplicaciones de administración de sistemas. Una integración total y automática entre los recursos de seguimiento de activos y estos productos permite seleccionar la herramienta de administración que se adapta mejor al entorno y aprovechar la inversión en las herramientas existentes.

HP también ofrece varias soluciones para controlar el acceso a componentes e información valiosos. ProtectTools Embedded Security, si está instalado, evita el acceso no autorizado a los datos, verifica la integridad del sistema y autentica usuarios externos que intenten acceder al sistema. Los recursos de seguridad tales como el ProtectTools, el sensor inteligente de cubierta y el bloqueo inteligente de cubierta , disponibles en modelos seleccionados, ayudan a impedir el acceso no autorizado a los componentes internos de la computadora personal. Al desactivar los puertos paralelos, seriales o USB, o al desactivar la capacidad de inicio desde medios extraíbles, usted puede proteger valiosos activos de datos. Los alertas de cambio de memoria y del sensor inteligente de cubierta se pueden reenviar automáticamente a las aplicaciones de administración del sistema para la entrega de notificaciones proactivas de manipulación indebida de los componentes internos de una computadora.

Protect Tools, el sensor inteligente de cubierta y el bloqueo inteligente de cubierta están disponibles como opciones en sistemas seleccionados.

Use las siguientes utilidades para administrar la configuración de seguridad en la computadora HP:

- Localmente, usando las Utilidades de Computer Setup. Consulte la *Guía de la utilidad de Configuración de la computadora (F10)* que viene con la computadora para obtener información adicional e instrucciones acerca del uso de las Utilidades de Computer Setup.
- A distancia, utilizando HP Client Manager o el System Software Manager. Este software permite el desarrollo y el control seguro y coherente de la configuración de seguridad desde una utilidad simple de línea de comandos.

La siguiente tabla y las siguientes secciones se refieren a la administración local de los recursos de seguridad de la computadora mediante las Utilidades de Computer Setup (F10).

Información general acerca de los recursos de seguridad

Recurso	Propósito	Cómo se establece
Control de inicio desde medios extraíbles	Impide el inicio desde las unidades de medios extraíbles. (disponible en unidades seleccionadas)	Desde el menú Utilidades de Computer Setup(F10).
Control de interfaz serial, paralela, USB o infrarroja	Impide la transferencia de datos a través de las interfaces serial, paralela, USB (universal serial bus) o infrarroja.	Desde el menú Utilidades de Computer Setup (F10).
Contraseña de encendido	Impide el uso de la computadora hasta que se ingrese la contraseña. Esto se puede aplicar al inicio y a los reinicios del sistema.	Desde el menú Utilidades de Computer Setup (F10).
Contraseña de configuración	Impide la reconfiguración de la computadora (el uso de las utilidades de Computer Setup) hasta que se ingrese la contraseña.	Desde el menú Utilidades de Computer Setup (F10).
Dispositivo Embedded Security	Impide el acceso no autorizado a los datos mediante encriptación y protección por contraseña. Verifica la integridad del sistema y autentica usuarios externos que intentan acceder al sistema.	Desde el menú Utilidades de Computer Setup (F10).

✎ Para obtener más información acerca de la Computer Setup, consulte la *Guía de la utilidad de configuración de la computadora (F10)*.

La compatibilidad para los recursos de seguridad puede variar dependiendo de la configuración específica de la computadora.

Información general acerca de los recursos de seguridad *(Continuación)*

Recurso	Propósito	Cómo se establece
DriveLock	Impide el acceso no autorizado a los datos de discos duros del Compartimento para Múltiples Dispositivos. Este recurso está disponible sólo en modelos seleccionados.	Desde el menú Utilidades de Computer Setup (F10).
Sensor inteligente de cubierta	Indica el retiro de la cubierta o del panel lateral de la computadora. Se puede configurar para que requiera la contraseña de configuración al reiniciar la computadora, después del retiro de la cubierta o del panel lateral. Consulte la *Guía de Hardware* en el *CD de Documentación* para obtener más información acerca de este recurso. Este recurso está disponible sólo en modelos seleccionados.	Desde el menú Utilidades de Computer Setup (F10).
Seguridad de registro de inicio principal	Puede impedir cambios accidentales o maliciosos al registro de inicio principal del disco apto para inicio actual y proporciona una forma de recuperar el "último MBR bueno conocido".	Desde el menú Utilidades de Computer Setup (F10).

✎ Para obtener más información acerca de la Computer Setup, consulte la *Guía de la utilidad de configuración de la computadora (F10).*

La compatibilidad para los recursos de seguridad puede variar dependiendo de la configuración específica de la computadora.

Información general acerca de los recursos de seguridad *(Continuación)*

Recurso	Propósito	Cómo se establece
Alertas de cambio de memoria	Detecta la adición, movimiento o retirada de módulos de memoria; notifica al usuario y al administrador del sistema.	Para obtener información acerca de la activación de alertas de cambio de memoria, consulte *Guía de Intelligent Manageability* en línea.
Etiqueta de propiedad	Muestra información de propiedad, definida por el administrador del sistema, durante el inicio del sistema (protegida por una contraseña de configuración).	Desde el menú Utilidades de Computer Setup (F10).
Mediante cable de bloqueo	Impide el acceso al interior de la computadora para evitar cambios no deseados en la configuración o la retirada de componentes. También se puede usar para asegurar la computadora a un objeto fijo con el fin de impedir robos.	Instale un cable de bloqueo para asegurar la computadora a un objeto fijo.
Mediante anillo de seguridad	Impide el acceso al interior de la computadora para evitar cambios no deseados en la configuración o el retiro de componentes.	Instale un bloqueo en el anillo de seguridad para impedir cambios no deseados en la configuración o la retirada de componentes.

✎ Para obtener más información acerca de Computer Setup, consulte la *Guía de la utilidad de configuración de la computadora (F10)*.

La compatibilidad para los recusros de seguridad puede variar dependiendo de la configuración específica de la computadora.

Seguridad con contraseña

La contraseña de encendido impide el uso no autorizado de la computadora al requerir el ingreso de una contraseña para acceder a aplicaciones o a datos cada vez que la computadora se enciende o se reinicia. La contraseña de configuración impide específicamente el acceso no autorizado a la configuración de la computadora y también se puede usar para anular la contraseña de encendido. Es decir, cuando se solicita la contraseña de encendido, el ingreso de la contraseña de configuración en su lugar permite el acceso a la computadora.

Es posible establecer una contraseña de configuración en toda la red para permitir que el administrador del sistema inicie una sesión en todos los sistemas de red para realizar mantenimiento sin tener que conocer la contraseña de encendido, incluso si se estableció una.

Establecimiento de una contraseña de configuración mediante Computer Setup

Si el sistema está equipado con un dispositivo incorporado de seguridad, consulte "Seguridad incorporada (Embedded Security)" en la página 31.

El establecimiento de una contraseña de configuración mediante Computer Setup impide la reconfiguración de la computadora (uso de la utilidad Computer Setup (F10)) hasta el ingreso de la contraseña.

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Presione la tecla **F10** así que encienda la luz verde del monitor. Presione **Intro** para saltar la pantalla de título, si fuese necesario.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Seleccione **Seguridad,** luego **Contraseña de configuración** y siga las instrucciones en pantalla.
4. Antes de salir, haga clic en **Archivo > Guardar cambios** y **Salir.**

Estableciendo una contraseña de encendido mediante Computer Setup

El establecimiento de una contraseña de encendido mediante Computer Setup impide el acceso a la computadora cuando ésta se apaga, a menos que se ingrese la contraseña. Cuando se establece una contraseña de encendido, Computer Setup presenta Opciones de contraseña en el menú Seguridad. Las opciones de contraseña incluyen el Mensaje de Contraseña en el Inicio en Caliente. Cuando Mensaje de contraseña en Inicio en caliente está activado, la contraseña también se debe ingresar cada vez que la computadora se reinicia.

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Presione la tecla **F10** así que encienda la luz verde del monitor. Presione **Intro** para saltar la pantalla de título, si fuese necesario.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Seleccione **Seguridad,** luego **Contraseña de encendido** y siga las instrucciones en pantalla.
4. Antes de salir, haga clic en **Archivo > Guardar cambios** y **Salir.**

Ingreso de una contraseña de encendido

Para ingresar una contraseña de encendido, realice los siguientes pasos:

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Cuando el icono de llave aparezca en el monitor, escriba la contraseña actual y luego presione **Intro.**

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

Si ingresa incorrectamente la contraseña, aparecerá un icono de llave rota. Vuelva a intentarlo. Después de tres intentos sin éxito, deberá apagar la computadora y volver a encenderla antes de continuar.

Ingreso de una contraseña de configuración

Si el sistema está equipado con un dispositivo embedded security, consulte "Seguridad incorporada (Embedded Security)" en la página 31.

Si se estableció una contraseña de configuración en la computadora, se le solicitará ingresarla cada vez que ejecute Computer Setup.

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Presione la tecla **F10** así que encienda la luz verde del monitor.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Cuando aparezca el icono de llave en el monitor, escriba la contraseña de configuración y luego presione la tecla **Intro** .

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

Si ingresa incorrectamente la contraseña, aparecerá un icono de llave rota. Vuelva a intentarlo. Después de tres intentos sin éxito, deberá apagar la computadora y volver a encenderla antes de continuar.

Cambio de una contraseña de encendido o de configuración

Si el sistema está equipado con un dispositivo embedded security, consulte "Seguridad incorporada (Embedded Security)" en la página 31.

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.** Para mudar la contraseña de configuración, ejecute la **Computer Setup.**
2. Cuando aparezca el icono de llave, escriba la contraseña actual, una barra diagonal (/) o un carácter delimitador alternativo, la nueva contraseña, otra barra diagonal (/) o un carácter delimitador alternativo y otra vez la nueva contraseña de la siguiente manera: **contraseña actual/nueva contraseña/nueva contraseña**

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

3. Presione **Intro**.

La nueva contraseña entrará en vigencia la próxima vez que encienda la computadora.

Consulte "Caracteres delimitadores del teclado nacional" en la página 30 para obtener información sobre los caracteres delimitadores alternativos. Las contraseñas de encendido y de configuración también se pueden cambiar mediante las opciones de seguridad de Computer Setup.

Eliminación de una contraseña de encendido o de configuración

Si el sistema está equipado con un dispositivo embedded security, consulte "Seguridad incorporada (Embedded Security)" en la página 31.

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.** Para eliminar la contraseña de configuración, ejecute **Computer Setup.**
2. Cuando aparezca el icono de llave, escriba la contraseña actual seguida de una barra diagonal (/) o de un carácter delimitador alternativo de la siguiente manera:
   contraseña actual/
3. Presione **Intro**.

Consulte "Caracteres delimitadores del teclado nacional" para obtener información sobre los caracteres delimitadores alternativos. Las contraseñas de encendido y de configuración también se pueden cambiar mediante las opciones de seguridad de Computer Setup.

Caracteres delimitadores del teclado nacional

Cada teclado está diseñado para satisfacer los requisitos específicos de la región. La sintaxis y las teclas que utilice para cambiar o eliminar una contraseña dependerán del teclado que venga con la computadora.

Caracteres delimitadores del teclado nacional

Árabe	/	Griego	-	Ruso	/
Belga	=	Hebreo	.	Eslovaco	-
BHCSY*	-	Húngaro	-	Español	-
Brasileño	/	Italiano	-	Sueco/Finlandés	/
Chino	/	Japonés	/	Suizo	-
Checo	-	Coreano	/	Taiwanés	/
Danés	-	Latinoamericano	-	Tailandés	/
Francés	!	Noruego	-	Turco	.
Francés canadiense	é	Polaco	-	Inglés del Reino Unido	/
Alemán	-	Portugués	-	Inglés de Estados Unidos	/

* Para Bosnia y Hercegovina, Croacia, Eslovenia y Yugoslavia

Borrado de contraseñas

Si olvida la contraseña, no podrá acceder a la computadora. Consulte la *Guía de Solución de Problemas* para obtener instrucciones acerca del borrado de las contraseñas.

Si el sistema está equipado con un dispositivo de seguridad incorporada (Embedded Security), consulte "Seguridad incorporada (Embedded Security)."

Seguridad incorporada (Embedded Security)

La seguridad incorporada (Embedded Security) de ProtectTools combina cifrado y protección por contraseña, para proporcionar una mayor seguridad para el cifrado de archivos/carpetas del Sistema de Archivos Incorporado (EFS) y la protección de e-mail con Microsoft Outlook y Outlook Express. ProtectTools está disponible para computadoras de escritorio comerciales seleccionadas, como opciones Configuradas al Orden (CTO). DriveLock está destinado a clientes de HP para quienes la seguridad de los datos es de vital importancia. el acceso no autorizado a los datos representa un peligro mucho mayor que la pérdida de datos. ProtectTools utiliza cuatro contraseñas:

- (F10) Configuración —para entrar en la utilidad Computer Setup (F10) y activar/desactivar ProtectTools
- Asumir la Propiedad — para ser definido y utilizado por un administrador del sistema, que autorizará usuarios y establecerá parámetros de seguridad
- Marca de Recuperación de Emergencia — para ser definido por el administrador del sistema, permitirá la recuperación si falla el chip de la computadora o de ProtectTools
- Usuario Básico — para ser definido y usado por el usuario final.

Si se pierde la contraseña del usuario final, los datos encriptados no pueden ser recuperados. Por lo tanto, ProtectTools se utiliza con mayor seguridad cuando los datos del disco duro se duplican en un sistema de información corporativo o se respaldan con regularidad mediante copias de respaldo.

ProtectTools Embedded Security es un chip de seguridad compatible con TCPA 1.1, opcionalmente instalado en la placa del sistema de computadoras de escritorio comerciales seleccionadas. Cada chip de ProtectTools Embedded Security es exclusivo, y está vinculado a una computadora específica. Cada chip ejecuta procesos de seguridad esenciales, independientemente de los otros componentes de la computadora (tales como el procesador, la memoria o el sistema operativo).

Una computadora que opera con ProtectTools Embedded Security complementa y perfecciona los recursos de seguridad inherentes al Microsoft Windows 2000 o al Windows XP Professional o Home Edition. Por ejemplo, aunque el sistema operativo pueda cifrar archivos y carpetas locales basado en un EFS, ProtectTools Embedded Security ofrece una capa de seguridad más al crear claves de cifrado desde la clave raíz de la plataforma (que está almacenada en el silicio). Este proceso es conocido como "wrapping" de las claves de encriptado. ProtectTools no impide el acceso por la red a una computadora sin ProtectTools.

Los principales recursos de ProtectTools Embedded Security son:

- Autenticación de plataformas
- Almacenamiento protegido
- Integridad de datos

PRECAUCIÓN: Proteja las contraseñas. **No se puede acceder ni recuperar a los datos cifrados sin las contraseñas**.

Estableciendo contraseñas

Configuración

Una contraseña de configuración puede ser creada y el dispositivo de seguridad incorporada (Embedded Security) puede ser activado mediante la utilidad de Computer Setup (F10).

1. Presione la tecla **F10** así que encienda la luz verde del monitor.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

2. Use la tecla de flecha arriba o abajo para seleccionar un idioma y luego presione **Intro.**
3. Use la tecla de flecha izquierda o derecha para pasar a la ficha **Seguridad**, luego use la tecla de flecha arriba o abajo para pasar a **Contraseña de Configuración**. Presione **Intro**.
4. Escriba y confirme la contraseña. Presione **F10** para confirmar la contraseña.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

5. Use la tecla de flecha arriba o abajo para pasar a **Dispositivo de Seguridad incorporada (Embedded Security)**. Presione **Intro**.
6. Si la selección del cuadro de diálogo es **Dispositivo de Seguridad incorporada (Embedded Security)—Desactivar**, utilice la tecla de flecha izquierda o derecha para cambiarlo a **Dispositivo de Seguridad incorporada (Embedded Security)—Activar**. Presione **F10** para confirmar la alteración.

PRECAUCIÓN: Si selecciona **Restaurar las Configuraciones de Fábrica—Restaurar**, todas las claves serán borradas y los datos encriptados no pueden ser recuperados *a menos que* exista reserva de las claves (vea "Asumir la Propiedad y Marca de Recuperación de Emergencia"). Basta seleccionar **Restaurar** cuando se le solicite en el procedimiento de recuperación de datos encriptados (vea "Recuperación de Datos Encriptados" en la página 36).

7. Use la tecla de flecha izquierda o derecha para pasar a **Archivo**. Use la tecla de flecha arriba o abajo para pasar a **Guardar Cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.

Asumir la Propiedad y Marca de Recuperación de Emergencia

Se requiere la Contraseña de Asunción de Propiedad para activar o desactivar la plataforma de seguridad y autorizar usuarios. Si falla el dispositivo de seguridad incorporada (Embedded Security), el mecanismo de Recuperación de Emergencia permite la autorización de los usuarios y el acceso a los datos.

1. Si utiliza Windows XP Professional o Home Edition, haga clic en **Inicio > Todos los programas > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

   Si utiliza Windows 2000, haga clic en **Inicio > Programas > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

2. Haga clic en **Siguiente**.
3. Escriba y confirme una seña de Asunción de Propiedad, luego haga clic en **Siguiente**.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

4. Haga clic en **Siguiente** para aceptar la ubicación predefinida del archivo de Recuperación.
5. Escriba y confirme una seña de Marca de Recuperación de Emergencia, luego haga clic en **Siguiente**.
6. Inserte un disquete en que se almacenará la Clave de la Marca de Recuperación de Emergencia. Haga clic en **Buscar** y seleccione el disquete.

PRECAUCIÓN: La Clave de la Marca de Recuperación de Emergencia es usada para recuperar datos encriptados si falla una computadora o el chip de seguridad incorporada (Embedded Security). **Es imposible recuperar los datos sin la clave**. (Los datos aún no pueden ser accedidos sin la contraseña de Usuario Básico). Almacene este disquete en un lugar seguro.

7. Haga clic en **Guardar** para aceptar la ubicación y el nombre de archivo predefinido, luego haga clic en **Siguiente**.

8. Haga clic en **Siguiente** para confirmar las configuraciones antes que se inicie la Plataforma de Seguridad.

Un mensaje puede ser exhibido, informando que los recursos de la Seguridad incorporada (Embedded Security) no están iniciadas. No haga clic en el mensaje; se abordará esto más adelante en el procedimiento, y el mensaje se cerrará tras algunos segundos.

9. Haga clic en **Siguiente** para saltar los criterios locales de configuración.
10. Verifique si la casilla de verificación "Iniciar el Asistente de Inicialización de Usuarios de la Seguridad incorporada (Embedded Security)" está seleccionada, luego haga clic en **Terminar**.

Ahora, el Asistente de Inicialización de Usuarios se inicia automáticamente.

Usuario Básico

Durante la inicialización del usuario, se crea la Contraseña de Usuario Básico. Esta contraseña es necesaria para introducir y acceder a los datos encriptados.

PRECAUCIÓN: Proteja la contraseña de Usuario Básico. **No se puede acceder ni recuperar a los datos encriptados sin esta contraseña**.

1. Si el Asistente de Inicialización de Usuarios no está abierto:

   Si utiliza Windows XP Professional o Home Edition, haga clic en **Inicio > Todos los programas > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

   Si utiliza Windows 2000, haga clic en **Inicio > Programas > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.
2. Haga clic en **Siguiente**.
3. Escriba y confirme una contraseña de Clave de Usuario Básico, luego haga clic en **Siguiente**.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

4. Haga clic en **Siguiente** para confirmar las configuraciones.
5. Seleccione los Recursos de Seguridad apropiados y haga clic en **Siguiente**.
6. Haga clic en el cliente de e-mail apropiado para seleccionarlo, luego haga clic en **Siguiente**.
7. Haga clic en **Siguiente** para aplicar el Certificado de Encriptado.
8. Haga clic en **Siguiente** para confirmar las configuraciones.
9. Haga clic en **Terminar**.
10. Reinicie la computadora.

Recuperación de Datos Encriptados

Para recuperar datos tras el reemplazo del chip de ProtectTools, usted debe tener lo siguiente:

- SPEmRecToken.xml—la Clave de Marca de Recuperación de Emergencia
- SPEmRecArchive.xml—carpeta oculta, ubicación predefinida: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- Contraseñas de ProtectTools
  - ❏ Configuración
  - ❏ Asumir la Propiedad
  - ❏ Marca de Recuperación de Emergencia
  - ❏ Usuario Básico

1. Reinicie la computadora.
2. Presione la tecla **F10** así que encienda la luz verde del monitor.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Escriba la contraseña de configuración y luego presione **Intro**.
4. Use la tecla de flecha arriba o abajo para seleccionar un idioma y luego presione **Intro.**
5. Use la tecla de flecha izquierda o derecha para pasar a la ficha **Seguridad**, luego use la tecla de flecha arriba o abajo para pasar a **Dispositivo de Seguridad incorporada (Embedded Security)**. Presione **Intro**.
6. Si sólo una selección, **Dispositivo de Seguridad incorporada (Embedded Security)—Desactivar**, está disponible:

   a. Use la tecla de flecha izquierda o derecha para pasar a **Dispositivo de Seguridad incorporada (Embedded Security)—Activar**. Presione **F10** para confirmar la alteración.

   b. Use la tecla de flecha izquierda o derecha para pasar a **Archivo**. Use la tecla de flecha arriba o abajo para pasar a **Guardar Cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.

   c. Salte al paso 1.

   Si están disponibles dos selecciones, salte al paso 7.

7. Use la tecla de flecha arriba o abajo para pasar a **Restaurar las Configuraciones de Fábrica—No Restaurar**. Presione una vez la tecla de flecha izquierda o derecha.

   Se exhibe un mensaje que informa: Esta acción restaurará el dispositivo de seguridad incorporada (Embedded Security) a las configuraciones de fábrica si las configuraciones son guardadas al salir. Pulse cualquier tecla para continuar.

   Presione **Intro**.

8. Ahora, la selección presentará **Restaurar las Configuraciones de Fábrica—Restaurar**. Presione **F10** para confirmar la alteración.
9. Use la tecla de flecha izquierda o derecha para pasar a **Archivo**. Use la tecla de flecha arriba o abajo para pasar a **Guardar Cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.
10. Reinicie la computadora.

11. Presione la tecla **F10** así que encienda la luz verde del monitor.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

12. Escriba la contraseña de configuración y luego presione **Intro**.
13. Use la tecla de flecha arriba o abajo para seleccionar un idioma y luego presione **Intro.**
14. Use la tecla de flecha izquierda o derecha para pasar a la ficha **Seguridad**, luego use la tecla de flecha arriba o abajo para pasar a **Dispositivo de Seguridad incorporada (Embedded Security)**. Presione **Intro**.
15. Si la selección del cuadro de diálogo es **Dispositivo de Seguridad incorporada (Embedded Security)—Desactivar**, utilice la tecla de flecha izquierda o derecha para cambiarlo a **Dispositivo de Seguridad incorporada (Embedded Security)—Activar**. Presione **F10**.
16. Use la tecla de flecha izquierda o derecha para pasar a **Archivo**. Use la tecla de flecha arriba o abajo para pasar a **Guardar Cambios y Salir**. Presione **Intro**, luego presione **F10** para confirmar.

17. Luego que Windows se abra:

    Si utiliza Windows XP Professional o Home Edition, haga clic en **Inicio > Todos los programas > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

    Si utiliza Windows 2000, haga clic en **Inicio > Programas > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

18. Haga clic en **Siguiente**.
19. Escriba y confirme la contraseña de Asunción de Propiedad. Haga clic en **Siguiente**.

Escriba cuidadosamente; por motivos de seguridad, los caracteres que escribe no aparecen en pantalla.

20. Verifique si 'Crear un nuevo archivo de recuperación' está seleccionado. Bajo **Ubicación del archivo de recuperación**, haga clic en **Buscar**.
21. No acepte el nombre de archivo predefinido. Escriba un nuevo nombre de archivo para impedir el reemplazo del archivo original.
22. Haga clic en **Guardar**, luego haga clic en **Siguiente**.
23. Escriba y confirme una seña de Marca de Recuperación de Emergencia, luego haga clic en **Siguiente**.
24. Inserte un disquete en que se almacenará la Clave de la Marca de Recuperación de Emergencia. Haga clic en **Buscar** y seleccione el disquete.
25. No acepte el nombre de clave predefinido. Escriba un nuevo nombre de clave para impedir el reemplazo de la clave original.
26. Haga clic en **Guardar**, luego haga clic en **Siguiente**.
27. Haga clic en **Siguiente** para confirmar las configuraciones antes que se inicie la Plataforma de Seguridad.

Un mensaje puede ser exhibido informando que no se puede cargar la Clave de Usuario Básico. No haga clic en el mensaje; se abordará esto más adelante en el procedimiento, y el mensaje se cerrará tras algunos segundos.

28. Haga clic en **Siguiente** para saltar los criterios locales de configuración.
29. Haga clic para desmarcar la casilla de verifición **Iniciar el Asistente de Inicialización de Usuarios de la Seguridad incorporada (Embedded Security)**. Haga clic en **Terminar**.
30. Haga clic con el botón derecho en el icono de ProtectTools en la barra de herramientas, luego haga clic en **Inicializar la restauración de la Seguridad incorporada (Embedded Security)**.

    Esto iniciará el HP ProtectTools Embedded Security Initialization Wizard.
31. Haga clic en **Siguiente**.
32. Inserte el disquete en que está almacenada la Clave de Marca de Recuperación de Emergencia original. Haga clic en **Buscar**, luego ubique y haga doble clic en la marca para introducir el nombre en el campo. El valor predefinido es A:\SPEmRecToken.xml.
33. Escriba la contraseña de la Marca original y haga clic en **Siguiente**.
34. Haga clic en **Buscar**, luego ubique y haga doble clic en el archivo original de recuperación para introducir el nombre en el campo. El nombre predefinido es C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
35. Haga clic en **Siguiente**.
36. Haga clic en la máquina que ha de ser restaurada, luego haga clic en **Siguiente**.
37. Haga clic en **Siguiente** para confirmar las configuraciones.
38. Si el asistente anuncia que la plataforma de seguridad fue restaurada, salte al paso 39.

    Si el asistente anuncia que la restauración falló, regrese al paso 10. Verifique cuidadosamente las contraseñas, la ubicación y el nombre de la marca, y la ubicación y el nombre del archivo.
39. Haga clic en Finalizar.

40. Si utiliza Windows XP Professional o Home Edition, haga clic en **Inicio > Todos los programas > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

    Si utiliza Windows 2000, haga clic en **Inicio > Programas > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

41. Haga clic en **Siguiente**.
42. Haga clic en **Recuperar su clave de usuario básico** y haga clic en **Siguiente**.
43. Selecione un usuario, escriba la contraseña de la Clave de Usuario básico original del usuario en cuestión, y luego haga clic en **Siguiente**.
44. Haga clic en **Siguiente** para confirmar las configuraciones y aceptar la ubicación predefinida de los datos de Recuperación.

Pasos 45 para 49 reinstalan la configuración original del Usuario Básico.

45. Seleccione los Recursos de Seguridad apropiadas y haga clic en **Siguiente**.
46. Haga clic en el cliente de e-mail apropiado para seleccionarlo, luego haga clic en **Siguiente**.
47. Haga clic en el Certificado de Encriptado y haga clic en **Siguiente** para aplicarlo.
48. Haga clic en **Siguiente** para confirmar las configuraciones.
49. Haga clic en **Terminar**.
50. Reinicie la computadora.

PRECAUCIÓN: Proteja la contraseña de Usuario Básico. **No se puede acceder ni recuperar a los datos encriptados sin esta contraseña**.

DriveLock

DriveLock es un recurso de seguridad estándar de mercado que impide el acceso no autorizado a los datos de discos duros del Compartimento para Múltiples Dispositivos. DriveLock se implementó como una extensión de Computer Setup. Sólo está disponible cuando se detecten discos duros compatibles con el DriveLock.

DriveLock está destinado a clientes de HP para quienes la seguridad de los datos es de vital importancia. Para estos clientes, el costo del disco duro y la pérdida de los datos almacenados en él no tienen ninguna trascendencia en comparación con el daño que se podría producir con el acceso no autorizado a su contenido. Con el objeto de equilibrar este nivel de seguridad con la necesidad práctica de acomodar una contraseña olvidada, la implementación de DriveLock por HP emplea un esquema de seguridad de dos contraseñas. Una contraseña tiene la finalidad de ser configurada y utilizada por un administrador del sistema mientras que la otra es configurada y utilizada generalmente por el usuario final. No hay una forma encubierta que pueda usarse para desbloquear la unidad en caso de que se olviden las contraseñas. Por lo tanto, DriveLock se utiliza con mayor seguridad cuando los datos del disco duro se duplican en un sistema de información corporativo o se respaldan mediante copias de reserva regularmente.

En caso de que ambas contraseñas de DriveLock se pierdan, el disco duro quedará inutilizable. Para un usuario que no se ajuste al perfil de cliente anteriormente definido, éste puede ser un riesgo inaceptable. Para usuarios que sí se ajusten al perfil de cliente, puede tratarse de un riesgo tolerable dada la naturaleza de los datos almacenados en el disco duro.

Uso de DriveLock

La opción DriveLock aparece en el menú Seguridad de Computer Setup. El usuario tiene opciones para configurar la contraseña principal o para activar DriveLock. Se debe proporcionar una contraseña de usuario para activar DriveLock. Debido a que generalmente un administrador del sistema realiza la configuración inicial de DriveLock, se debe establecer primero una contraseña principal. HP recomienda a los administradores del sistema establecer una contraseña principal en el caso de que planeen activar DriveLock o mantenerlo desactivado. Esto proporcionará al administrador la

capacidad de modificar la configuración de DriveLock si la unidad se bloquea en el futuro. Una vez configurada la contraseña principal, el administrador del sistema puede activar DriveLock u optar por mantenerlo desactivado.

Si hay un disco duro bloqueado, la POST requerirá una contraseña para desbloquear el dispositivo. Si hay una contraseña de encendido configurada y ésta coincide con la contraseña de usuario del dispositivo, la POST no solicitará que el usuario vuelva a ingresar la contraseña. De lo contrario, se le solicitará al usuario ingresar una contraseña DriveLock. Se puede usar la contraseña principal o la de usuario. Los usuarios tendrán dos intentos para ingresar una contraseña correcta. Si ninguno de los intentos tiene éxito, la POST continuará, pero los datos de la unidad permanecerán inaccesibles.

Aplicaciones DriveLock

El uso más práctico del recurso de seguridad DriveLock es en un entorno corporativo, en donde un administrador del sistema proporciona a los usuarios discos duros para el Compartimento para Múltiples Dispositivos para uso en algunas computadoras de escritorio. El administrador del sistema es responsable de configurar el disco duro para el Compartimento para Múltiples Dispositivos, lo que implica, entre otras cosas, la configuración de la contraseña principal de DriveLock. En caso de que el usuario olvide la contraseña de usuario o que el equipo se transfiera a otro empleado, la contraseña principal se puede usar siempre para restablecer la contraseña de usuario y volver a obtener acceso al disco duro.

HP recomienda a los administradores corporativos del sistema, que optan por activar DriveLock, que establezcan también criterios corporativos para la configuración y el mantenimiento de contraseñas principales. Esto se debe realizar para evitar una situación en que un empleado establezca, con o sin intención, ambas contraseñas de DriveLock antes de dejar la empresa. En tal caso, el disco duro queda inutilizable y es necesario reemplazarlo. Asimismo, al no establecer una contraseña principal, los administradores del sistema pueden encontrarse privados del acceso a un disco duro y ser incapaces de realizar revisiones de rutina en busca de software no autorizado, otras funciones de control de activos y soporte.

Para los usuarios con requisitos de seguridad menos estrictos, HP no recomienda la activación de DriveLock. Entre los usuarios de esta categoría se incluyen usuarios personales o usuarios que no acostumbran mantener datos importantes en sus discos duros. Para estos usuarios, la posible pérdida de un disco duro como resultado del olvido de ambas contraseñas es mucho mayor que el valor de los datos que DriveLock protege. El acceso a Computer Setup y a DriveLock se puede restringir mediante la contraseña de configuración. Al especificar una contraseña de configuración sin proporcionársela a los usuarios finales, los administradores del sistema pueden impedir que los usuarios activen DriveLock.

Sensor inteligente de cubierta

El sensor inteligente de cubierta, disponible en modelos seleccionados, es una combinación de tecnología de hardware y de software que puede advertirle del retiro de la cubierta o del panel lateral de la computadora. Hay tres niveles de protección, que se describen en la siguiente tabla.

Niveles de protección del sensor inteligente de cubierta

Nivel	Configuración	Descripción
Nivel 0	Desactivado	El sensor inteligente de cubierta está desactivado (valor predeterminado).
Nivel 1	Notificar al usuario	Al reiniciarse la computadora, la pantalla muestra un mensaje que indica la retirada de la cubierta o del panel lateral.
Nivel 2	Contraseña de configuración	Al reiniciarse la computadora, la pantalla muestra un mensaje que indica la retirada de la cubierta o del panel lateral. Debe ingresar la contraseña de configuración para continuar.

✎ Esta configuración se puede cambiar mediante Computer Setup. Para obtener más informaciones acerca de Computer Setup, consulte la *Guía de la utilidad de configuración de la computadora (F10)*.

Configuración del nivel de protección del sensor inteligente de cubierta

Para configurar el nivel de protección del sensor inteligente de cubierta, realice los siguientes pasos:

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Presione la tecla **F10** así que encienda la luz verde del monitor. Presione **Intro** para saltar la pantalla de título, si fuese necesario.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Seleccione **Seguridad,** luego **Cubierta inteligente** y siga las instrucciones en pantalla.
4. Antes de salir, haga clic en **Archivo > Guardar cambios** y **Salir.**

Bloqueo inteligente de cubierta

El bloqueo inteligente de cubierta es un bloqueo de la cubierta controlable por software que viene en computadoras HP seleccionadas. Este bloqueo impide el acceso no autorizado a los componentes internos. Las computadoras vienen con el bloqueo inteligente de cubierta en la posición de desbloqueo.

PRECAUCIÓN: Para una máxima seguridad del bloqueo de la cubierta, asegúrese de establecer una contraseña de configuración. La contraseña de configuración impide el acceso no autorizado a la utilidad Computer Setup.

El bloqueo inteligente de cubierta está disponible como una opción en sistemas seleccionados.

Activación del bloqueo inteligente de cubierta

Para activar el bloqueo inteligente de cubierta, realice los siguientes pasos:

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Presione la tecla **F10** así que encienda la luz verde del monitor. Presione **Intro** para saltar la pantalla de título, si fuese necesario.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Seleccione **Seguridad,** luego **Cubierta inteligente** y la opción **Bloqueada**.
4. Antes de salir, haga clic en **Archivo > Guardar cambios** y **Salir.**

Desactivación del Bloqueo inteligente de cubierta

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Presione la tecla **F10** así que encienda la luz verde del monitor. Presione **Intro** para saltar la pantalla de título, si fuese necesario.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Seleccione **Seguridad > Cubierta inteligente > Desbloqueada.**
4. Antes de salir, haga clic en **Archivo > Guardar cambios** y **Salir.**

Uso de la llave a prueba de fallas de la cubierta inteligente

Si activa el Bloqueo inteligente de cubierta y no puede ingresar la contraseña para desactivarlo, necesitará una llave a prueba de fallas de la cubierta inteligente para abrir la cubierta de la computadora. Necesitará la llave en cualquiera de las siguientes circunstancias:

- Corte de energía
- Falla de inicio
- Falla de un componente de la computadora (como por ejemplo el procesador o el sistema de alimentación)
- Se olvidó la contraseña

PRECAUCIÓN: La llave a prueba de fallas de la cubierta inteligente es una herramienta especializada disponible en HP. Esté preparado; solicite esta llave antes que necesite una en una reventa autorizada o un prestador de servicios.

Para obtener la llave a prueba de fallas, realice una de las siguientes acciones:

- Póngase en contacto con un revendedor o proveedor de servicio autorizado de HP.
- Llame al número correspondiente de la lista que aparece en la garantía.

Para obtener más informaciones acerca del uso de la llave a prueba de fallas de la cubierta inteligente, consulte la *Guía de Hardware.*

Seguridad de registro de inicio principal

El Registro de inicio principal (MBR) contiene información necesaria para realizar un inicio exitoso desde un disco y para acceder a los datos almacenados en éste. La seguridad del registro de inicio principal puede impedir cambios accidentales o maliciosos en el MBR, como los causados por algunos virus computacionales o por el uso incorrecto de ciertas utilidades para discos. También le permite recuperar el "último MBR bueno conocido", en caso de detectarse cambios en el MBR al reiniciar el sistema.

Para activar la seguridad del MBR, realice los siguientes pasos:

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Presione la tecla **F10** así que encienda la luz verde del monitor. Presione **Intro** para saltar la pantalla de título, si fuese necesario.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Seleccione **Seguridad > Seguridad de registro de inicio principal > Activada.**
4. Seleccione **Seguridad > Guardar registro de inicio principal.**
5. Antes de salir, haga clic en **Archivo > Guardar cambios** y **Salir.**

Cuando la seguridad del MBR está activada, la BIOS impide cambios en el MBR del disco apto para inicio actual mientras se está en modo a prueba de fallas de MS-DOS o Windows.

La mayor parte de los sistemas operativos controla el acceso al MBR del disco apto para inicio actual; la BIOS no puede impedir cambios que puedan producirse mientras el sistema operativo está en funcionamiento.

Cada vez que se enciende o que se reinicia la computadora, la BIOS compara el MBR del disco apto para inicio actual con el MBR anteriormente guardado. Si se detectan cambios y si el disco apto para inicio actual es el mismo disco del cual se guardó anteriormente el MBR, aparecerá el siguiente mensaje:

1999—Registro de inicio principal modificado.

Presione cualquier tecla para entrar en la configuración y configurar la seguridad del MBR.

Al entrar en Computer Setup, deberá

- Guardar el MBR del disco apto para inicio actual.
- Restaurar el MBR anteriormente guardado.
- Desactivar el recurso de seguridad del MBR.

Debe conocer la contraseña de configuración, si existe una.

Si se detectan cambios y el disco apto para inicio actual **no** es el mismo disco del cual se guardó anteriormente el MBR, aparecerá el siguiente mensaje:

2000—Disco duro de registro de inicio principal modificado.

Presione cualquier tecla para entrar en la configuración y configurar la seguridad del MBR.

Al entrar en Computer Setup, deberá

- Guardar el MBR del disco apto para inicio actual.
- Desactivar el recurso de seguridad del MBR.

Debe conocer la contraseña de configuración, si existe una.

En el caso poco probable de que el MBR anteriormente guardado se hubiera dañado, aparecerá el siguiente mensaje:

1998—Registro de inicio principal perdido.

Presione cualquier tecla para entrar en la configuración y configurar la seguridad del MBR.

Al entrar en Computer Setup, deberá

- Guardar el MBR del disco apto para inicio actual.
- Desactivar el recurso de seguridad del MBR.

Debe conocer la contraseña de configuración, si existe una.

Antes de particionar o dar formato al disco apto para inicio actual

Asegúrese de que la seguridad del MBR esté desactivada antes de cambiar la partición o el formato del disco apto para inicio actual. Algunas utilidades para disco, tales como FDISK y FORMAT, intentan actualizar el MBR. Si la seguridad del MBR está activada al cambiar la partición o el formato del disco, es posible que reciba mensajes de error provenientes de la utilidad para disco o una advertencia de la seguridad del MBR la próxima vez que encienda o reinicie la computadora. Para desactivar la seguridad del MBR, siga estos pasos:

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio > Apagar > Reiniciar la computadora.**
2. Presione la tecla **F10** así que encienda la luz verde del monitor. Presione **Intro** para saltar la pantalla de título, si fuese necesario.

Si no presiona la tecla **F10** en el momento correcto, debe apagar la computadora, volver a encenderla y presionar la tecla **F10** otra vez para acceder a la utilidad.

3. Seleccione **Seguridad > Seguridad del registro de inicio principal > Desactivada.**
4. Antes de salir, haga clic en **Archivo > Guardar cambios** y **Salir.**

Medida de cable de bloqueo

El panel posterior de la computadora alberga un cable de bloqueo, para que el equipo se pueda asegurar físicamente a un área de trabajo.

Para obtener instrucciones ilustradas, consulte la *Guía de Hardware* en el *CD de Documentación*.

Tecnología de identificación de huellas digitales

Al eliminar la necesidad de ingresar contraseñas de usuario, la tecnología de identificación de huellas digitales de HP refuerza la seguridad de redes, simplifica el proceso de inicio de sesión y reduce los costos asociados con la administración de redes corporativas. Con un precio accesible, ya no está sólo al alcance de organizaciones de tecnología de punta y alta seguridad.

El soporte para la tecnología de identificación de huellas digitales varía según el modelo.

Para obtener más informaciones, visite:

http://h18000.www1.hp.com/solutions/security.

Notificación y recuperación de fallas

Los recursos de notificación y recuperación de fallas combinan una innovadora tecnología de hardware y software para evitar la pérdida de datos fundamentales y reducir al mínimo el tiempo improductivo no planificado.

Cuando se produce una falla, la computadora muestra un mensaje de alerta local que contiene una descripción de la falla y las acciones recomendadas. Luego, puede ver el estado actual del sistema usando HP Client Manager. Si la computadora está conectada a una red administrada por un producto Insight Manager de HP, HP Client Manager o por otros productos de administración, la computadora también envía un aviso de falla a la aplicación de administración de red.

Sistema de protección de unidades

El Sistema de protección de unidades (DPS) es una herramienta de diagnóstico incorporada en los discos duros instalados en computadoras HP seleccionadas. El DPS está diseñado para ayudar a diagnosticar problemas que podrían generar un reemplazo sin garantía del disco duro.

Cuando se fabrican las computadoras HP, cada disco duro instalado se prueba utilizando el DPS y en la unidad se escribe un registro permanente de información clave. Cada vez que se ejecuta el DPS, los

resultados de las pruebas se escriben en el disco duro. El prestaddor de servicios puede usar esta información como ayuda para diagnosticar las condiciones que hicieron necesario ejecutar el software DPS. Consulte la *Guía de Solución de Problemas* para obtener instrucciones acerca del uso del DPS.

Sistema de alimentación con tolerancia a sobrevoltaje

Un sistema de alimentación con tolerancia a sobrevoltaje integrado proporciona una mayor protección cuando la computadora recibe un sobrevoltaje no previsto. Este sistema de alimentación tiene una capacidad nominal para soportar un sobrevoltaje de hasta 2000 voltios, lo que evita incurrir en tiempos improductivos del sistema o en la pérdida de datos.

Sensor térmico

El sensor térmico es un recurso del hardware y software que efectúa un seguimiento de la temperatura interna de la computadora. Este recurso muestra un mensaje de advertencia cuando se excede el rango normal, lo que da tiempo para adoptar medidas antes de que los componentes internos resulten dañados o que se produzca una pérdida de datos.

Indice

R

S