Guía de Administración de Desktop
Business Desktop

Guía de Administración de Desktop

Business Desktop

Segunda edición: julio de 2008

Número de referencia del documento: 451272-163

Acerca de esta publicación

Esta guía proporciona definiciones e instrucciones para el uso de los recursos de seguridad y administración que vienen preinstalados en algunos modelos.

⚠ **¡ADVERTENCIA!** El texto presentado de esta forma indica que, si no se siguen las instrucciones, se pueden producir daños físicos o pérdida de la vida.

⚠ **PRECAUCIÓN:** El texto presentado de esta forma indica que, si no se siguen las instrucciones, se pueden producir daños en la computadora o pérdida de información.

NOTA: El texto presentado de esta manera proporciona información importante complementaria.

Tabla de contenido

1 Descripción General de Administración de Desktop

HP Client Management Solutions provee soluciones con base en estándares para administrar y controlar business desktop, workstations y notebooks en un entorno de red. HP es pionera en la capacidad de administración de business desktops desde 1995 con la introducción de las primeras business desktop completamente administrables de la industria. HP posee patentes de tecnología con capacidad de administración. Desde entonces, HP ha realizado un esfuerzo en todo el sector para desarrollar estándares e infraestructuras necesarias para implementar, configurar y administrar eficazmente business desktop, workstations y notebooks. HP desarrolla su propio software de administración y trabaja estrechamente con proveedores de soluciones de software de administración de primera línea en el sector que aseguran la compatibilidad entre soluciones de administración de Clientes de HP y estos productos. HP Client Management Solutions son un aspecto importante de nuestro amplio compromiso de proporcionarle soluciones que lo ayuden a reducir el costo total de propiedad y mantenimiento durante todo el ciclo de vida de las computadoras.

Las capacidades y recursos clave de la administración de desktop son:

- Configuración e implementación iniciales
- Remote System Installation
- Actualización y administración de software
- Flash de memoria ROM
- Configuración opcional de Hardware
- Rastreo y seguridad de activos
- Aviso de fallas y recuperación

NOTA: Soporte para recursos específicos descritos en esta guía puede variar según el modelo o la versión del software.

2 Configuración e Implementación Iniciales

La computadora viene con una imagen preinstalada del software del sistema. Luego de un breve proceso de “desempaquetamiento” del software, la computadora está lista para utilización.

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

- Instalación de aplicaciones de software adicionales, luego de desempaquetar la imagen de software preinstalada.
- Uso de herramientas de implementación de software, como HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (con base en tecnología Radia), o la Solución Altiris Deployment, para reemplazar el software preinstalado con una imagen personalizada de software.
- Uso de un proceso de clonación de disco para copiar el contenido de un disco duro a otro.

El mejor método de implementación depende de los procesos y del entorno de tecnología de la información.

El sistema HP Backup and Recovery (Copia de seguridad y recuperación de HP), configuración con base en memoria ROM y hardware ACPI proveen asistencia adicional con la restauración de software del sistema, administración y solución de problemas de configuración, y administración de energía.

NOTA: Consulte HP Backup and Recovery Manager (Administrador de copia de seguridad y recuperación de HP) en la página 11 para obtener más información acerca de la creación de un Conjunto de Discos de Recuperación.

HP Software Agent

El agente de administración utilizado por ambas HP Client Automation Standard y Enterprise Editions es precargado en la computadora. Cuando instalado, permite comunicación con la consola de administración HP.

Para instalar el HP Software Agent:

1. Haga clic en **Inicio**.
2. Haga clic en **Todos los Programas**.
3. Haga clic en **Capacidad de administración HP**.
4. Haga clic en **Radia Management Agent Readme**.
5. Revise y siga las instrucciones que se encuentran en el archivo Readme (Léame) para instalar el HP Software Agent.

El HP Software Agent es un componente principal de infraestructura que activa todas las soluciones HP Client Automation. Para obtener más información acerca de otros componentes de infraestructura necesarios para la implementación de las soluciones HP Configuration Management, visite http://h20229.www2.hp.com/solutions/ascm/index.html.

Altiris Deployment Solution Agent

Este programa es precargado en la computadora. Cuando instalado, permite comunicación con la consola de Solución de Implementación del administrador.

Para instalar el Altiris Deployment Solution Agent:

1. Haga clic en **Inicio**.
2. Haga clic en **Todos los programas**.
3. Para Windows Vista, haga clic en **Instalar Altiris DAgent**. Para Windows XP, haga clic en **Instalar Altiris AClient**.
4. Siga las instrucciones en pantalla para instalar y configurar el Altiris client.

Este agente es un componente principal de infraestructura para activar la Solución Altiris Deployment que es parte de Altiris Client Management Suite. Para obtener más información acerca de otros componentes de infraestructura necesarios para la implementación de Altiris Client Management Suite, visite http://www.hp.com/go/easydeploy.

3 Remote System Installation

La Instalación Remota del Sistema permite iniciar y configurar el sistema utilizando 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 realizar las siguientes tareas:

- Formateo de una unidad de disco duro
- Implementación de una imagen de software en una o más computadoras nuevas
- Actualización remota del BIOS del sistema en flash de memoria ROM (Flash Remoto de Memoria ROM en la página 15)
- Configuración de los parámetros del BIOS del sistema

Para iniciar Remote System Installation, presione F12 cuando aparezca el mensaje **F12 = Network Service Boot (Inicio de servicio de red)** en la esquina inferior derecha de la pantalla del logotipo HP cuando se inicializa la computadora. Siga las instrucciones en pantalla para continuar con el proceso. El orden de inicialización predeterminado es un parámetro de configuración de BIOS que puede ser alterado para que siempre intente inicialización PXE.

4 Actualización y administración de software

HP provee diversas herramientas para administrar y actualizar software en business desktops, workstations, y notebooks:

- Interfaz HP Client Management
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- Ediciones HP Client Automation Starter (Básica), Standard (Estándar), y Enterprise (Empresarial)
- HP Client Manager de Symantec
- Altiris Client Management Suite
- HP Client Catalog para Microsoft System Center y Productos SMS
- HP Backup and Recovery Manager (Administrador de copia de seguridad y recuperación de HP)
- PC marca Intel vPro con tecnología Active Management
- Verdiem Surveyor
- Notificación Proactiva de Cambios de HP
- HP Subscriber's Choice

HP Client Management Interface

A pesar de las herramientas de administración del sistema que utilice su departamento de TI, la administración de los activos de hardware y software es importante para mantener sus costos de TI bajos y su empresa dinámica. El administrador de TI puede acceder la Interfaz HP Client Management escribiendo script simples e integrando aquellos script a la solución de administración de su preferencia.

Con la interfaz HP Client Management (HP CMI), las nuevas Business PC HP se integran de forma continua en la administración de su entorno de TI. La HP CMI proporciona una interfaz que simplifica la integración de las Business PC HP con herramientas de administración de sistema populares de la industria(incluyendo Microsoft Systems Management Server, software IBM Tivoli, y operaciones HP), y aplicaciones personalizadas de administración desarrolladas internamente. Al utilizar la HP CMI, las herramientas y aplicaciones de administración de sistema pueden solicitar inventarios exhaustivos de Client, recibir información del estado de integridad, y administrar la configuración de BIOS del sistema

comunicándose directamente con la computadora Client, reduciendo la necesidad de software de agentes o conectores para realizar la integración.

HP Client Management Interface se basa en estándares de primera línea en el sector que incluyen Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS), y Advanced Configuration and Power Interface (ACPI). HP CMI es una plataforma de tecnología utilizada en HP Client Management Solutions. Con HP CMI, HP le da la flexibilidad de elegir la manera de administrar sus computadoras Client HP.

HP Client Management Interface utilizado junto con el software de administración del sistema puede:

- Solicitar de información de inventario en profundidad de Client – Capture información detallada acerca de los procesadores, unidades de disco duro, memoria, BIOS, controladores, incluyendo información de sensores (como velocidad del ventilador, voltaje, y temperatura).
- Recibir información sobre el estado de funcionamiento – Subscríbase a un amplio conjunto de alertas de hardware cliente (como temperatura excesiva, interrupción del ventilador y cambios de configuración de hardware) que serán enviadas a la consola de administración del sistema, aplicaciones o a la computadora Cliente local. Las alertas son enviadas en tiempo real cuando son activadas por eventos de hardware.
- Administrar la configuración de BIOS del sistema – Realice funciones con la tecla F10 que incluyen la configuración y los cambios de contraseña de BIOS y el orden de inicio de la computadora a distancia desde su consola de administración del sistema en cualquier o en todos sus sistemas cliente sin tener que visitar cada máquina.

Para obtener más información acerca de la Interfaz HP Client Manager, visite http://www.hp.com/go/hpcmi/.

HP SoftPaq Download Manager

HP SoftPaq Download Manager es una interfaz gratuita y fácil de utilizar para ubicar y descargar actualizaciones de software para los modelos PC Client HP en su entorno. Al especificar sus modelos, sistema operativo, e idioma, usted puede rápidamente ubicar, clasificar, y seleccionar softpaqs que necesita. Para descargar el HP SoftPaq Download Manager, visite http://www.hp.com/go/sdm.

HP System Software Manager

HP System Software Manager (SSM) es una utilidad gratuita que automatiza la implementación remota de controladores de dispositivo y actualizaciones del BIOS para sus HP Business PC en red. Cuando el SSM es ejecutado, en segundo plano (sin interacción del usuario) determina la revisión de los niveles de controladores y del BIOS, instalados en cada sistema cliente en red y los compara este inventario contra SoftPaq de software de sistema que fue probado y almacenado en un depósito central de archivos. En seguida, el SSM actualiza automáticamente todos los software del sistema de revisión no actualizados en los equipos en rede para niveles posteriores disponibles en la memoria de archivos. Como el SSM solo permite distribución de actualizaciones de SoftPaq a los modelos correctos del sistema cliente, los administradores pueden utilizar el SSM confidencial y eficientemente para mantener actualizado el software del sistema.

El System Software Manager se integra con las herramientas de distribución de software corporativo, como las soluciones HP Client Automation, HP Client Manager de Symantec, y Microsoft Systems Management Server (SMS). Con la utilización del SSM, usted puede distribuir actualizaciones creadas por el cliente o por otros proveedores empaquetadas en el formato SSM.

Es posible descargar el SSM gratuitamente visitando http://www.hp.com/go/ssm.

NOTA: SSM actualmente no admite flash remoto de la memoria ROM en sistemas que tienen activado Windows Vista BitLocker y están utilizando recursos TPM para proteger las claves BitLocker porque al hacer flash en el BIOS invalida la firma confiable que BitLocker creó para la plataforma. Desactive BitLocker a través de los criterios de grupo a fin de hacer flash en el BIOS del sistema.

Es posible activar soporte BitLocker sin medidas TPM de BIOS para evitar invalidar las claves de BitLocker. HP recomienda que mantenga una copia de seguridad protegida de las credenciales del BitLocker en el evento de emergencias de recuperación.

HP ProtectTools Security Manager

El software HP ProtectTools Security Manager proporciona recursos de seguridad que ayudan a proteger contra al acceso no autorizado a las computadoras, redes y datos críticos. La funcionalidad de seguridad optimizada se suministra a través de los siguientes módulos de software:

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Device Access Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Privacy Manager for HP ProtectTools

Los módulos de software disponibles para su computadora pueden variar según el modelo. Por ejemplo, Embedded Security for HP ProtectTools está disponible solamente para computadoras en las cuales está instalado el Chip TPM (Trusted Platform Module) embedded security.

Los módulos del software HP ProtectTools pueden estar preinstalados, precargados, o disponibles para descarga desde el sitio Web de HP. Para algunas Desktops HP Compaq, HP ProtectTools está

disponible como una opción en el mercado de accesorios. Visite http://www.hp.com/products/security para obtener más información.

Ediciones HP Client Automation Starter (Básico) y Standard (Estándar)

HP Client Automation es una solución de administración de hardware y software para entornos de Windows Vista, Windows XP y HP Thin Client que es fácil de utilizar y rápida de implementar, mientras que provee una base sólida para necesidades futuras. Se ofrece en dos ediciones:

- Starter Edition (Edición Básica) es un producto gratuito para la administración de desktop, Notebook y Workstation HP, proporcionando inventario de hardware y software, control remoto, monitoreo de alertas HP, actualizaciones de BIOS y controladores HP, integración con HP Protect Tools y soporte adicional para Intel AMT. Starter Edition también admite la implementación y administración de HP Thin Client.
- Standard Edition (Edición Estándar), disponible para compra, incluye toda la funcionalidad que se proporciona en la Starter Edition y agrega implementación y migración de Windows, recursos de administración de parches, distribución de software y medición del uso de software.

Las Ediciones HP Client Automation Starter (Básica) y Standard (Estandár) proveen una ruta de migración para la Edición HP Client Automation Enterprise (con base en tecnología Radia) para administrar automáticamente entornos de TI grandes, heterogéneos y continuamente cambiantes.

Para obtener más información acerca de las soluciones HP Client Automation, visite http://www.hp.com/go/client.

HP Client Automation Enterprise Edition (Edición Empresarial)

HP Client Automation Enterprise Edition (Edición Empresarial) es una solución con base en criterios que permite que los administradores realicen inventarios, implementaciones, parches, y administren continuamente software y contenido en todas las plataformas heterogéneas de Client. Con la HP Client Automation Enterprise Edition (Edición Empresarial), el profesional de TI puede:

- Automatizar el proceso completo de la administración del ciclo de vida desde búsqueda, implementación, y administración continua a través de migración y retiro
- Implementar automáticamente y administrar continuamente todo un conjunto de software (sistemas operativos, aplicaciones, parches, configuraciones, y contenido) a un estado deseado
- Administrar software en virtualmente todos los dispositivos, incluyendo desktops y notebooks, en una infraestructura heterogénea e independiente
- Administrar software en la mayoría de sistemas operativos

Con la administración continua de la configuración, los clientes de HP informan ahorros dramáticos en los costos de TI, acelerando el tiempo de lanzamiento de software y contenido al mercado, aumentando la productividad y satisfacción de los usuarios.

Para obtener más información acerca de las soluciones HP Client Automation, visite http://www.hp.com/go/client.

HP Client Manager de Symantec

HP Client Manager de Symantec, desarrollado en conjunto con Altiris, está disponible gratuitamente para todas las Business Desktop, Notebook, y Workstation HP. SSM está integrado en el HP Client Manager, y permite rastreo central, monitoreo y administración de los aspectos de hardware de los sistemas Client HP

Utilice el HP Client Manager de Symantec para:

- Obtener valiosa información de hardware como las configuraciones de la CPU, memoria, video y seguridad
- Monitorear el estado del sistema para resolver problemas antes de que ocurran
- Adquierir e instalar automáticamente controladores y actualizaciones de BIOS sin intervención física de cada a la computadora
- Configurar remotamente el BIOS y las configuraciones de seguridad
- Automatizar procesos para resolver rápidamente problemas de hardware

La estrecha integración con las herramientas del HP Instant Support reduce el tiempo para solucionar problemas de hardware.

- Diagnóstico – ejecute remotamente y vea reportes en los modelos de desktops, notebooks workstations
- Escaneo del estado de funcionamiento del sistema – verifique conocidos problemas de hardware en la base instalada de los sistemas cliente HP
- Chat activo – contacte al soporte al cliente de HP para resolver problemas.
- Base de conocimiento HP – enlace con información de expertos
- Proceso de captación y entrega automatizada de SoftPaq para rápida resolución de problemas de hardware
- Identificación, inventario e inicialización de sistemas con el chip embedded security de HP ProtectTools.
- Opción para mostrar alertas de estado de funcionamiento localmente en el sistema cliente
- Reporte de información básica de inventario para clientes que no son de HP
- Instalación y configuración del chip TPM security
- Copia de seguridad y recuperación de Client programada centralmente
- Soporte adicional para administrar AMT de Intel

Para obtener más información acerca del HP Client Manager de Symantec, visite http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite es una solución fácil de utilizar para la admninistración completa del ciclo de vida de software para desktops, notebooks, y workstations. Client Management Suite Nivel 1 incluye los siguientes productos Altiris:

- Solución de Inventario
- Solución de Implementación
- Solución de Entrega de Software
- Solución de Administración de Parches
- Solución de Medición de Aplicaciones
- Solución de Administración de Aplicación
- Solución Carbon Copy (Copia Exacta)

Para obtener más información acerca de Altiris Client Management Suite, visite http://www.altiris.com/Products/ClientManagementSuite.aspx.

HP Client Catalog para Microsoft System Center y Productos SMS

El HP Client Catalog permite que profesionales de TI utilizando productos Microsoft automaticen la implementación de actualizaciones de software HP (Softpaqs) para Business PC HP. El archivo del catálogo contiene información detallada de plataformas de Business Desktop, Notebook y Workstation. Puede utilizarse en conjunto con los recursos personalizados de inventario y actualización de productos Microsoft para proporcionar actualizaciones automáticas de controladores y parches para la administración de Computadoras Client HP.

Los productos Microsoft admitidos por el HP Client Catalog incluyen:

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server (SMS) 2003 R2

Para obtener más información acerca del HP Client Catalog para SMS, visite http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

HP Backup and Recovery Manager (Administrador de copia de seguridad y recuperación de HP)

El HP Backup and Recovery Manager (Administrador de Copia de Seguridad y Recuperación de HP) es una aplicación versátil y fácil de utilizar que le permite realizar copias de seguridad y recuperación de la unidad de disco duro primaria en la PC. La aplicación funciona en Windows para crear copias de seguridad de Windows, todas las aplicaciones, y todos los archivos de datos. Las copias de seguridad pueden ser programadas automáticamente en intervalos designados o pueden ser iniciadas manualmente. Archivos importantes pueden archivarse separadamente de copias de seguridad frecuentes.

HP Backup and Recovery Manager (Administrador de copia de seguridad y recuperación de HP) está instalado en la unidad C: y crea una Partición de Recuperación.

Puntos de Restauración y copias de seguridad de archivos pueden copiarse en discos de CD o DVD, mientras que todas las copias de seguridad pueden copiarse en la red o unidades de disco duro secundarias.

HP recomienda enfáticamente crear un conjunto de discos de recuperación inmediatamente antes de utilizar la computadora y programar copias de seguridad automáticas periódicas de puntos de recuperación.

Para crear un conjunto de discos de recuperación:

1. Haga clic en **Inicio** > **HP Backup and Recovery** > **HP Backup and Recovery Manager** para abrir el Administrador de Copia de Seguridad y Recuperación, luego haga clic en **Siguiente**.
2. Seleccione **Crear CD/DVD de recuperación para recuperar el sistema (Muy recomendado)** y haga clic en **Siguiente**.
3. Siga las instrucciones del asistente.

Para obtener más información acerca del uso del HP Backup and Recovery Manager (Administrador de Copia de Seguridad y Recuperación de HP), consulte la *Guía del usuario del HP Backup and Recovery Manager* seleccionando **Inicio** > **HP Backup and Recovery** > **Manual de HP Backup and Recovery Manager**.

NOTA: Es posible hacer un pedido del conjunto de discos de recuperación de HP llamando al centro de asistencia técnica HP. Visite el siguiente sitio web, selecionando su región, y haga clic en el enlace **Asistencia técnica después de la compra de productos** en el título **Contactar HP** para obtener el número telefónico del Centro de asistencia técnica para su región.

http://welcome.hp.com/country/us/en/wwcontact_us.html

Tecnología de Administración

Modelos incluyen la tecnolog vPro o la tecnología estándar. Ambos permiten un mejor descubrimiento, recuperación, y protección de activos computacionales en red. Ambas tecnologías permiten que se administren las PC ya sea que el sistema esté encendido, apagado, o el sistema operativo esté colgado.

Los recursos de la tecnología de administración incluyen:

- Información sobre el inventario de hardware
- Avisos
- Administración de energía – encendido/apagado, ciclo de alimentación
- Diagnóstico y reparación remotos
  - Serial-over-LAN (SOL) – permite el control de la consola de PC remota durante su fase de inicialización
  - Redirección de IDE – permite que el inicio del sistema desde una unidad de inicio remoto, disco o imagen ISO
- Aislamiento y recuperación con base en hardware – limita o suprime el acceso a red de equipo, si se detecta actividad típica de virus

NOTA: Para obtener una descripción general de la tecnología Intl vPro, visite http://www.intel.com/vpro.

Para obtener información específica de HP acerca de la tecnología Intel vPro, consulte los documentos técnicos en http://www.hp.com/support. Elija su país e idioma, y seleccione **Ver información sobre soporte y solución de problemas**, ingrese el número de modelo de la computadora y presione intro. En la categoría **Recursos**, haga clic en **Manuales (guías, suplementos, adendas, etc.)**. En **Salto rápido a los manuales por categoría**, haga clic en **Informes**.

Tecnologías de administración disponibles incluyen lo siguiente:

- AMT (incluye DASH 1.0)
- ASF

ASF y AMT pueden no ser configurados al mismo tiempo, pero ambos son admitidos.

Para configurar sistemas Intel vPro para AMT o ASF:

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio** > **Apagar** > **Reiniciar**.
2. Tan pronto se enciende la computadora, presione la tecla de acceso rápido, Ctrl+P, antes de que la computadora inicie el sistema operativo.

   NOTA: Si no presiona Ctrl+P en el momento adecuado, usted debe reiniciar la computadora y nuevamente presionar Ctrl+P para acceder la utilidad, antes que la computadora inicie el sistema operativo.

Esta tecla de acceso rápido ingresa a la utilidad de configuración de Intel Management Engine BIOS Execution (MEBx). Esta utilidad permite que el usuario configure los varios aspectos de la tecnología de administración. Algunas de las opciones de configuración se listan a continuación:

- Menú Principal
  - Configuración Intel ® ME
  - Configuración Intel ® AMT
  - Cambiar Contraseña Intel ® ME
  - Salir
- Configuración de Plataforma Intel ® ME
  - Control de Estado Intel ® ME (activar/desactivar)
  - Actualización Local de firmware Intel ® ME (activar/desactivar)
  - Control de Recursos Intel ® ME
  - Control de Energía Intel ® ME
- Configuración Intel ® AMT
  - Nombre de Host
  - TCP/IP
  - Modelo de Provisión (Empresarial, SMB)
  - Instalación y Configuración
  - Sin Provisión
  - SOL/IDE-R (activar/desactivar)
  - Criterio de Contraseña
  - Actualización Segura de Firmware (activar/desactivar)
  - Establecer PRTC
  - Intervalo de Inactividad
- Cambiar Contraseña Intel ® ME (HP recomienda enfáticamente que se cambie esta contraseña. La configuración predeterminada es **admin**).

A fin de administrar sistemas AMT de forma remota, el administrador debe utilizar una consola remota que admita AMT. Las consolas de administración corporativas están disponibles de proveedores como HP, Altiris y Microsoft SMS. En el modo SMB, el Client proporciona una interfaz de explorador Web. Para acceder este recurso, abra el explorador desde cualquier otro sistema en la red e ingrese `http://host_name:16992` donde `host_name` es el nombre designado al sistema. Alternativamente, es posible utilizar la dirección IP en lugar del nombre host.

Verdiem Surveyor

Verdiem Surveyor es una solución de software que ayuda a administrar los costos de energía de la PC. Surveyor mensura e informa cuanta energía consume cada PC. También proporciona control sobre la configuración de energía de la PC permitiendo que los administradores implementen fácilmente las estrategias de ahorro de energía en todas las redes. Un HP SoftPaq qiue contiene el agente Surveyor puede descargarse desde el sitio de soporte HP e instalarse en modelos de desktop comerciales. Es posible adquirir licencias de Surveyor para administrar PC a través de su representante HP.

Notificación Proactiva de Cambios HP

El programa Notificación Proactiva de Cambios utiliza el sitio web Subscriber's Choice para enviarle proactivamente y automáticamente:

- Correo electrónico de Proactive Change Notification (PCN) en los cuales se le informa sobre cambios de hardware y software para la mayoría de equipos y servidores comerciales, con hasta 60 días de anticipación.
- Enviarle correo electrónico que contiene boletines al cliente, avisos al cliente, notas al cliente, boletines de seguridad y alertas de controladores para la mayoría de computadoras y los servidores comerciales.

Cree su propio perfil para asegurar que reciba sólo la información relevante para un entorno específico de TI. Para obtener más información acerca del programa Notificación Proactiva de Cambios y crear un perfil personalizado, visite http://h30046.www3.hp.com/subhub.php

Subscriber’s Choice

Subscriber’s Choice es un servicio con base en clientes de HP.

Con base en su propio perfil, HP le proporciona sugerencias personalizadas sobre productos, articulos relacionados y/o notificaciones o alertas de soporte para controladores.

El programa Selección del Subscriptor de Alertas/Notificaciones de Soporte y Controladores le enviará correo electrónico para notificarle que la información a la cual se subscribió en su perfil está disponible para revisión y descarga. Para obtener más información acerca del programa Selección del Subscriptor y crear un perfil personalizado, visite http://h30046.www3.hp.com/subhub.php.

Soluciones descontinuadas

Dos paquetes de software, Altiris Local Recovery y Dantz Retrospect, ya no serán comercializados en los business desktop, notebooks o workstations HP. Comenzando con los business desktop, notebooks o workstations HP lanzadas en 2006, todos serán comercializados con HP Backup and Recovery Manager (Administrador de copia de seguridad y recuperación de HP).

5 Flash de Memoria ROM

El BIOS de la computadora es almacenado en flash de la memoria ROM programable (memoria solamente de lectura). Al establecer una contraseña de configuración en la Guía de la Utilidad de Configuración del Equipo (F10), es posible proteger la memoria ROM contra actualizaciones y regrabaciones accidentales. Esto es importante para garantizar la integridad operativa de la computadora. Si necesita o desea actualizar el BIOS, es posible descargar las imágenes más recientes del BIOS desde la página de Soporte y Controladores de HP, http://www.hp.com/support/files.

△ **PRECAUCIÓN:** Para obtener una máxima protección de la memoria ROM, asegúrese de establecer una contraseña de configuración. La contraseña de configuración evita actualizaciones no autorizadas de la memoria ROM. El System Software Manager permite al administrador del sistema establecer la contraseña de configuración en un o más PC simultáneamente. Para obtener más información, visite http://www.hp.com/go/ssm.

Flash Remoto de Memoria ROM

El Flash Remoto de la Memoria ROM permite que el administrador del sistema actualice en forma segura la memoria ROM en computadoras HP remotas, directamente desde la consola centralizada de administración de red. Al permitir que el administrador del sistema realice ésta tarea remotamente en múltiples computadoras resulta en una implementación consistente y, con un mayor control de imágenes del BIOS de computadora HP a través de la red. También da como resultado un incremento de la productividad y una disminución del costo total de propiedad (TCO).

NOTA: SSM actualmente no admite flash remoto de la memoria ROM en sistemas que tienen activado Windows Vista BitLocker y están utilizando recursos TPM para proteger las claves BitLocker porque al hacer flash en el BIOS invalida la firma confiable que BitLocker creó para la plataforma. Desactive BitLocker a través de los criterios de grupo a fin de hacer flash en el BIOS del sistema.

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

Para obtener más información acerca del flash remoto de la memoria ROM, consulte el Software HP Client Manager o el System Software Manager en http://www.hp.com/go/ssm/.

HPQFlash

La utilidad HPQFlash es utilizada para actualizar o restaurar localmente la memoria ROM del sistema en computadoras individuales, a través de un sistema operativo Windows.

Para obtener más información sobre HPQFlash, visite http://www.hp.com/support/files y escriba el número de modelo de la computadora, cuando se le solicite.

6 Modo Boot Block Emergency Recovery

El modo Boot Block Emergency Recovery permite la recuperación de sistema en el caso improbable de falla de la flash ROM. Por ejemplo, sí ocurre un corte de energía durante una actualización del BIOS, la flash ROM quedaría incompleta. Esto tornaría el BIOS inservible. Boot Block es una sección flash protegida de la ROM, que contiene un código que verifica si hay una imagen válida del BIOS del sistema, cuando el sistema es encendido.

- Si la memoria ROM del sistema es válida, éste se inicia normalmente.
- Sí la imagen del BIOS del sistema no es válida, el BIOS Boot Block a prueba de fallas, provee soporte suficiente para buscar multimedia extraíble por archivos de imagen del BIOS. Si se encuentra un archivo adecuado de imagen del BIOS, éste es automáticamente cargado en la memoria ROM.

Cuando se detecta una imagen inválida del BIOS del sistema, la luz de alimentación del sistema parpadea en rojo ocho veces, una vez por segundo. Simultáneamente, el parlante sonará ocho veces. Si parte de la memoria ROM del sistema que contiene la imagen de la memoria ROM de opción de video no está dañada, el **Modo Boot Block Emergency Recovery** será exhibido en la pantalla.

Para recuperar el sistema después de que haya ingresado en el modo de recuperación Boot Block, realice los siguientes pasos:

1. Desconecte la energía.
2. Inserte un CD o un dispositivo flash USB, que contenga el archivo de imagen del BIOS deseado en el directorio raíz.

   NOTA: Los medios deben ser formateados utilizando el sistema de archivos FAT12, FAT16 o FAT32.

3. Encienda la computadora.

   Si no se encuentra una imagen de BIOS adecuada, será solicitado que inserte multimedia que contenga un archivo de la imagen del BIOS.

   Si el sistema reprograma con éxito la memoria ROM, éste se apagará automáticamente.

4. Retire el medio extraíble utilizado para actualizar el BIOS.
5. Reencienda la computadora para reiniciarla.

NOTA: BitLocker evita el inicio desde Windows Vista cuando un CD que contenga la imagen de BIOS esté en la unidad óptica. Si BitLocker está activado, extraiga el CD antes de tentar inicio en Windows Vista.

7 Replicación de 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.

NOTA: Ambos procedimientos requieren una unidad de disquete o una unidad flash USB admitida.

Copia en una única computadora

PRECAUCIÓN: Cada modelo tiene su configuración específica. Es posible que ocurran daños al sistema de archivos si las computadoras de origen y destino son de modelos diferentes. Por ejemplo, no copie una configuración de instalación de una computadora dc7xxx para una dx7xxx.

1. Seleccione una configuración definida para copia. Apague la computadora. Si está en Windows, haga clic en **Inicio** > **Apagar** > **Apagar**.
2. Si está utilizando un dispositivo de medios flash USB, insértelo ahora.
3. Encienda la computadora.
4. Tan pronto como se encienda la computadora, presione F10 para ingresar a la utilidad de configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

   NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.
5. Si está utilizando un disquete, insértelo ahora.
6. Haga clic en **File (Archivo)** > **Replicated Setup (Configuración replicada)** > **Save to Removable Media (Guardar para medios extraíbles)**. Siga las instrucciones que aparecen en pantalla para crear el disquete o el dispositivo de medios flash USB de configuración.
7. Apague la computadora por configurar e inserte el disquete o dispositivo de medios flash USB de configuración.
8. Encienda la computadora por configurar.
9. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

10. Haga clic en **File (Archivo)** > **Replicated Setup (Configuración replicada)** > **Restore from Removable Media (Restaurar desde medios extraíbles)**, y siga las instrucciones que aparecen en pantalla.

11. Reinicie la computadora cuando la configuración esté concluida.

Copia en múltiples computadoras

△ **PRECAUCIÓN:** Cada modelo tiene su configuración específica. Es posible que ocurran daños al sistema de archivos si las computadoras de origen y destino son de modelos diferentes. Por ejemplo, no copie una configuración de instalación de una computadora dc7xxx para una dx7xxx.

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-objetivo es significativamente más rápida.

NOTA: Un disquete de reinicio es necesario para este procedimiento o para crear un dispositivo de medios flash USB apto para inicio. Si Windows XP no está disponible para uso para crear un disquete apto para inicio, utilice el método de copia en una única computadora (consulte Copia en una única computadora en la página 17).

1. Cree un disquete o un dispositivo de medios flash USB apto para inicio. Consulte Dispositivos de Medios Flash USB Admitidos en la página 19 o Dispositivos de medios Flash USB no admitidos en la página 20.

   △ **PRECAUCIÓN:** Ni todas las computadoras pueden ser iniciadas a partir de un dispositivo de medios flash USB. Si el orden predefinido de inicio en la Guía de la utilidad de Configuración del Equipo (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 de inicio.

2. Seleccione una configuración definida para copia. Apague la computadora. Si está en Windows, haga clic en **Inicio** > **Apagar** > **Apagar**.

3. Si está utilizando un dispositivo de medios flash USB, insértelo ahora.

4. Encienda la computadora.

5. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

   NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

6. Si está utilizando un disquete, insértelo ahora.

7. Haga clic en **File (Archivo)** > **Replicated Setup (Configuración replicada)** > **Save to Removable Media (Guardar para medios extraíbles)**. Siga las instrucciones que aparecen en pantalla para crear el disquete o el dispositivo de medios flash USB de configuración.

8. Descargue una utilidad de BIOS para configuración replicada (repset.exe) y cópiela en el disquete o en el dispositivo de medios flash USB de configuración. Para obtener esta utilidad, visite http://welcome.hp.com/country/us/en/support.html e ingrese el número de modelo de la computadora.

9. 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
```

10. 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.

11. Reinicie la computadora cuando la configuración esté concluida.

Creación de un Dispositivo de Inicio

Dispositivos de Medios Flash USB Admitidos

Los dispositivos admitidos poseen una imagen preinstalada para simplificar el proceso de tornarlos en dispositivos aptos para inicio. Todos los dispositivos HP o Compaq y la mayoría de los dispositivos de medios flash USB, poseen esta imagen preinstalada. Si el dispositivo de medios flash USB utilizado no posee dicha imagen, utilice el procedimiento presentado más adelante en esta sección (consulte Dispositivos de medios Flash USB no admitidos en la página 20).

Para crear un dispositivo de medios flash USB de inicio, necesita:

- Un dispositivo de medios flash USB admitido
- Un disquete de inicialización DOS con los programas FDISK y SYS (si el SYS no está disponible, puede ser utilizado el FORMAT, mas todos los archivos existentes en el dispositivo de medios flash USB serán perdidos).
- Una computadora que puede ser inicializada a partir de un dispositivo de medios flash USB

△ **PRECAUCIÓN:** Algunas computadoras más antiguas pueden no ser inicializados a partir de un dispositivo de medios flash USB. Si el orden predefinido de inicio en la Guía de la utilidad de Configuración del Equipo (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 de inicio.

1. Apague la computadora.

2. Inserte el dispositivo de medios flash USB en uno de los puertos USB de la computadora y extraiga todos los dispositivos de almacenamiento USB, excepto las unidades de disquetes USB.

3. Inserte un disquete de inicio de DOS con FDISK.COM y los archivos SYS.COM o FORMAT.COM en una unidad de disquete y encienda la computadora para iniciar a partir del disquete de DOS.

4. Ejecute FDISK a partir del comando **A:** al escribir `FDISK` y presione intro. Cuando se solicite, haga clic en **Sí** (**S**) para activar el soporte de discos grandes.

5. Ingrese Selección [`5`] para exhibir las unidades del sistema. El dispositivo de medios flash USB será la unidad más semejante al tamaño de una de las unidades listadas. Es usualmente la última unidad de la lista. Observe la letra de la unidad.

   Unidad del dispositivo de medios flash USB: _____

   △ **PRECAUCIÓN:** En el evento que una unidad no corresponde al dispositivo de medios flash USB, no siga adelante. Puede ocurrir pérdida de datos. Verifique todos los puertos USB para ver si contienen dispositivos de almacenamiento adicionales. Si se encuentra alguno, extráigalo, reinicie la computadora y prosiga desde el paso 4. Si no se encuentra ninguno, el sistema no admite el dispositivo de medios flash USB o está defectuoso. NO siga adelante en su intento de hacer el dispositivo de medios flash USB apto para inicio.

6. Salga de FDISK al presionar la tecla Esc para regresar al comando **A:**.
7. Si su disquete de inicio de DOS contiene SYS.COM, salte al paso 8. De lo contrario, vaya al paso 9.
8. En el comando **A:**, ingrese `SYS x:` donde la 'x' representa la letra de la unidad observada arriba.

   △ **PRECAUCIÓN:** Verifique si ingresó la letra correcta de la unidad del dispositivo de medios flash USB.

   Luego de la transferencia de los archivos de sistema, SYS regresará al comando **A:**. Salte al paso 13.
9. Copie todos los archivos que desea del dispositivo de medios flash USB para un directorio temporal de otra unidad (por ejemplo, el disco duro interno del sistema).
10. En el comando **A:**, ingrese `FORMAT /S X:` donde la `X` representa la letra de la unidad observada arriba.

    △ **PRECAUCIÓN:** Verifique si ingresó la letra correcta de la unidad del dispositivo de medios flash USB.

    FORMAT exhibirá una o más advertencias y preguntará, todas las veces, si usted desea continuar. Ingrese `S` todas las veces. FORMAT formateará el dispositivo de medios flash USB, incluirá los archivos de sistema, y solicitará una Etiqueta de Volumen.
11. Presione Intro para no ingresar ninguna etiqueta, o ingrese una, si desea.
12. Copie todos los archivos que guardó en el paso 9 de vuelta para el dispositivo de medios flash USB.
13. Retire el disquete y reinicie la computadora. La computadora reiniciará a través del dispositivo de medios flash USB como la unidad C.

    NOTA: El orden predefinido de inicio varía según la computadora y se puede modificar en la Guía de la utilidad de Configuración del Equipo (F10).

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

Vuelva a Copia en múltiples computadoras en la página 18.

Dispositivos de medios Flash USB no admitidos

Para crear un dispositivo de medios flash USB de inicio, necesita:

- Un dispositivo de medios flash USB
- Un disquete de inicialización DOS con los programas FDISK y SYS (si el SYS no está disponible, puede ser utilizado el FORMAT, mas todos los archivos existentes en el dispositivo de medios flash USB serán perdidos).
- Una computadora que puede ser inicializada a partir de un dispositivo de medios flash USB

△ **PRECAUCIÓN:** Algunas computadoras más antiguas pueden no ser inicializadas a partir de un dispositivo de medios flash USB. Si el orden predefinido de inicio en la Guía de la utilidad de Configuración del Equipo (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 de inicio.

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 alimentación.

   △ **PRECAUCIÓN:** El cable de alimentación DEBE ser desconectado.

2. Abra la computadora y extraiga las tarjetas PCI.
3. Inserte el dispositivo de medios flash USB en uno de los puertos USB de la computadora y extraiga todos los dispositivos de almacenamiento USB, excepto las unidades de disquetes USB. Cierre la cubierta de la computadora.
4. Conecte el cable de alimentación y encienda la computadora.
5. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

   NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

6. Vaya para **Opciones avanzadas** > **Dispositivos PCI** para desactivar los controladores PATA y SATA. Al desactivar el controlador SATA, observe el IRQ al cual el controlador está designado. Necesitará designar nuevamente el IRQ posteriormente. Salga de la configuración confirmando los cambios.

   IRQ de SATA: _____

7. Inserte un disquete de inicio de DOS con FDISK.COM y los archivos SYS.COM o FORMAT.COM en una unidad de disquete y encienda la computadora para iniciar a partir del disquete de DOS.
8. Ejecute el FDISK y elimine todas las particiones existentes en el dispositivo de medios flash USB. Cree una nueva partición y márquela como activa. Salga del FDISK al presionar la tecla Esc.
9. Si el sistema no se ha reiniciado automáticamente al salir de FDISK, presione Ctrl+Alt+Supr para reiniciar a través del disquete de DOS.
10. En el comando **A:**, ingrese `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.
11. Presione Intro para no ingresar ninguna etiqueta, o ingrese una, si desea.
12. Apague la computadora y desconecte el cable de alimentación. Abra la computadora y reinstale todas las tarjetas PCI anteriormente retiradas. Cierre la cubierta de la computadora.
13. Conecte el cable de alimentación, retire el disquete y encienda la computadora.
14. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

15. Vaya para **Advanced (Opciones avanzadas)** > **PCI Devices (Dispositivos PCI)** y reactive los controladores PATA y SATA que fueron desactivados en el paso 6. Defina el controlador SATA a su IRQ original.

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

NOTA: El orden predefinido de inicio varía según la computadora y es posible modificarlo en la Guía de la utilidad de Configuración del Equipo (F10). Para obtener más información, consulte la *Guía de la utilidad de Configuración*.

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

Vuelva a Copia en múltiples computadoras en la página 18.

8 Botón de Alimentación de Dos Estados

Con Advanced Configuration y Power Interface (ACPI) activadas, el botón de alimentación puede funcionar como interruptor de encendido/apagado o como un botón de suspensión. El modo En Espera no apaga completamente la computadora, sino que hace que entre en un estado de Espera de baja alimentación. Esto permite un apagado rápido sin cerrar aplicaciones y un regreso rápido al mismo estado operacional sin pérdida de datos.

Para modificar la configuración del botón de alimentación, realice los siguientes pasos:

1. Haga clic con el botón izquierdo en **Inicio**, luego seleccione **Panel de control** > **Opciones de energía**.
2. En **Propiedades de opciones de energía**, seleccione la ficha **Opciones avanzadas**.
3. En la sección **Energía** seleccione **Suspensión**.

Después de configurar el botón de alimentación para que funcione como botón de suspensión, presione el botón de alimentación para poner el sistema en un estado de muy baja alimentación (suspensión). Presione nuevamente el botón para que el sistema salga rápidamente de la suspensión y déjelo en estado de alimentación completa. Para desconectar completamente toda la energía a la computadora, presione y mantenga presionado el botón de alimentación durante cuatro segundos.

△ **PRECAUCIÓN:** No utilice el botón de alimentación 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.

9 Sitio Web de Soporte de HP

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 todos los recursos sean admitidos y funcionen correctamente.

HP tornó más fácil la tarea de ubicar, acceder, evaluar e instalar el software de soporte más reciente. Es posible descargar el software desde http://www.hp.com/support.

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

10 Estándares del sector

Las soluciones de administración de HP se integran con otras aplicaciones de administración de sistemas con base en estándares de la industria, tales como:

- Administración de empresas con base en la Web (WBEM)
- Interfaz de la administración de Windows (WMI)
- Tecnología Wake on LAN
- ACPI
- SMBIOS
- Soporte de Pre-boot Execution (PXE)

11 Rastreo y seguridad de activos

Los recursos de rastreo de activos incorporados en la computadora suministran datos esenciales de rastreo de activos que se pueden administrar a través de HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager u otras aplicaciones de administración de sistemas. Una integración continua y automática entre los recursos de rastreo 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 informaciones valiosos. HP Embedded Security for ProtectTools, si está instalado, evita el acceso no autorizado a los datos, verifica la integridad del sistema y autentica usuarios externos que intenten acceder el sistema. (Para obtener más información, consulte la *Guía HP ProtectTools Security Manager* en http://www.hp.com/products/security). Los recursos de seguridad como HP Embedded Security for ProtectTools, el Sensor Inteligente de Cubierta y el Bloqueo Inteligente de Cubierta, disponibles en algunos modelos, ayudan a evitar el acceso no autorizado a los componentes internos de la computadora personal. Al desactivar los puertos paralelos, en serie o USB, o al desactivar la capacidad de inicio desde medios extraíbles, es posible proteger valiosos activos de datos. Alertas de Cambio de Memoria y del Sensor Inteligente de Cubierta pueden ser enviadas automáticamente a las aplicaciones de administración del sistema para entregar notificaciones proactivas de manipulación indebida de los componentes internos de la computadora.

NOTA: HP Embedded Security para ProtectTools, el sensor inteligente de cubierta y el Bloqueo inteligente de cubierta están disponibles como opciones en algunos sistemas.

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

- Localmente, a través de las Utilidades de configuración. Consulte la *Guía de la utilidad de Configuración del Equipo (F10)* que viene con la computadora para obtener información adicional e instrucciones acerca del uso de las Utilidades de configuración del equipo. Algunas computadoras también poseen HP BIOS Configuration for ProtectTools, que es un componente de ProtectTools con base en Windows que permite que los administradores definan la configuración de seguridad de BIOS a partir del sistema operativo en ejecución.
- De forma remota, utilizando HP Client Manager de Symantec, HP Client Automation, o System Software Manager. Estos software permiten la implementación y control de configuraciones seguro y consistente de configuraciones de seguridad.

La siguiente tabla y las siguientes secciones se refieren a la administración local de los recursos de seguridad de la computadora a través de la Guía de la utilidad de Configuración (F10).

Tabla 11-1 Información general sobre los recursos de seguridad

Opción	Descripción
Setup Password (Contraseña de configuración)	Permite definir y activar la contraseña de configuración (administrador).

Tabla 11-1 Información general sobre los recursos de seguridad (continúa)

	NOTA: Si se define la contraseña de configuración, es necesario cambiar las opciones de la Utilidad de Configuración, hacer flash de la memoria ROM y hacer cambios en ciertos parámetros de Plug and play (Conectar y Usar) en Windows.
Power-On Password (Contraseña de inicio)	Permite configurar y activar una contraseña de inicio. Aparecerá una solicitud de contraseña de inicio después del ciclo de alimentación. Si el usuario no ingresa la contraseña de inicio correcta, la unidad no se reiniciará. **NOTA:** Esta contraseña no aparecerá en inicios en caliente, como ctrl+alt+supr o **Reiniciar desde Windows**, a menos que se active en **Opciones de contraseña**, (consulte abajo).
Passwords Options (Opciones de contraseña) (Esta selección sólo aparecerá si se define una contraseña de inicio o una contraseña de configuración.)	Permite: • Recursos de bloqueo heredados (aparece si se define una contraseña de configuración) • Activar/desactivar modo de servidor de red (aparece si se define una contraseña de inicio) • Especifique si se necesita la contraseña para inicio en caliente (Ctrl+Alt+supr) (aparecerá si se ha definido una contraseña de inicio). • Activar/desactivar configuración del modo de exploración (aparecerá si se ha definido una contraseña de configuración) (permite ver, pero no cambiar, las opciones de configuración F10 sin ingresar la contraseña de configuración) • Activar/desactivar Contraseña Estricta (aparece si se establece una contraseña de inicio), que cuando está activada salta el puente de contraseña integrado para desactivar la contraseña de inicio Consulte la *Guía de Administración de Desktop* para obtener más información.
Smart Cover (Cubierta Inteligente) (algunos modelos)	Permite: • Activar/desactivar el bloqueo de la cubierta. • Configurar el sensor de extracción de la cubierta para desactivar/notificar a usuario/contraseña de configuración. **NOTA:** *Notificación al usuario* alerta al usuario que el sensor ha detectado que la cubierta fue retirada. *Contraseña de configuración* require que la contraseña de configuración sea ingresada para iniciar la computadora, si el sensor detecta que la cubierta fue retirada. Este recurso es admitido sólo en algunos modelos.
Device Security (Seguridad de dispositivos)	Permite establecer Dispositivo Disponible/Dispositivo Oculto para: • Puertos en serie • Puerto paralelo • Puertos Traseros USB • Puertos USB frontales • Puertos Internos USB • Audio de sistema • Controladores de red (algunos modelos) • Disquete heredado • Dispositivo embedded security (algunos modelos) • SATA0 • SATA1 (algunos modelos) • SATA2 (algunos modelos)

Tabla 11-1 Información general sobre los recursos de seguridad (continúa)

	• SATA3 (algunos modelos) • eSATA (algunos modelos)
Network Service Boot (Inicio de servicio de red)	Activa/desactiva la capacidad de la computadora de iniciarse desde un sistema operativo instalado en un servidor de red. (Recurso disponible sólo en modelos de tarjeta NIC; el controlador de red debe ser una tarjeta de expansión PCI o estar incorporado en la placa del sistema.)
System Ids (Identificación del sistema)	Permite configurar: • Etiqueta de activos (identificador de 18 bytes), un número de identificación de propiedad asignado por la empresa a la computadora. • Etiqueta de propietario (identificador de 80 bytes) exhibido durante POST. • Número de serie del chasis o número de identificador único universal (UUID). El UUID sólo puede actualizarse si el número de serie del chasis actual no es válido. (Estos números de ID se configuran normalmente en fábrica y se utilizan para identificar al sistema en forma única.) • Opciones regionales del teclado (por ejemplo, inglés o alemán) para la entrada de la identificación del sistema.
DriveLock Security (Seguridad DriveLock)	Permite asignar o modificar la contraseña principal o de usuario para unidades de discos duros. Cuando este recurso se activa, el usuario debe proporcionar una de las contraseñas de DriveLock durante la POST. Si no se ingresa ninguna contraseña válida, el disco duro permanece inaccesible hasta el ingreso exitoso de una de las contraseñas durante una secuencia de inicio en frío subsiguiente. **NOTA:** Esta selección sólo aparecerá cuando haya al menos una unidad conectada al sistema que sea compatible con el recurso DriveLock.
System Security (Seguridad de Sistema) (algunos modelos): estas opciones son dependientes del hardware)	Prevención de Ejecución de Datos (algunos modelos) (activar/desactivar) - Ayuda a evitar violaciones a la seguridad del sistema operativo. Tecnología de Virtualización (algunos modelos) (activar/desactivar) - Controla los recursos de virtualización del procesador. El cambio de esta configuración requiere apagar la computadora y luego encenderla. E/S Direccionada de Tecnología de Virtualización (algunos modelos) (activar/desactivar) - Controla los recursos de reasignación de Virtualización DMA del chipset. El cambio de esta configuración requiere apagar la computadora y luego encenderla. Tecnología de Ejecución Confiable (algunos modelos) (activar/desactivar) - Controla los recursos subyacentes del procesador y chipset necesarios para admitir un dispositivo virtual. El cambio de esta configuración requiere apagar la computadora y luego encenderla. Para activar este recurso usted debe activar los siguientes recursos: • Soporte para Dispositivo Embedded Security • Tecnología de Virtualización • E/S Direccionada de Tecnología de Virtualización Soporte para Dispositivo Embedded Security (algunos modelos) (activar/desactivar) - Permite la activación o desactivación del Dispositivo Embedded Security. El cambio de esta configuración requiere apagar la computadora y luego encenderla.

Tabla 11-1 Información general sobre los recursos de seguridad (continúa)

	NOTA: Para configurar el Dispositivo Embedded Security, debe definirse una contraseña de Configuración. • Restaurar a Valores Predeterminados de Fábrica (algunos modelos) (No restaurar/Restaurar) - La restauración de valores predeterminados de fábrica borrará todas las claves de seguridad. El cambio de esta configuración requiere apagar la computadora y luego encenderla. **PRECAUCIÓN:** El dispositivo embedded security es un componente crítico de muchas combinaciones de seguridad. El borrado de las claves de seguridad evitará el acceso a datos protegidos por el Dispositivo Embedded Security. Al seleccionar Restaurar a Valores Predeterminados de Fábrica puede resultar en una pérdida significativa de datos. • Soporte para autenticación de inicio (algunos modelos) (activar/desactivar) - Controla la combinación de contraseñas de autenticación de inicio que utiliza el Dispositivo Embedded Security. El cambio de esta configuración requiere apagar la computadora y luego encenderla. • Restaurar credenciales de autenticación (algunos modelos) (No restaurar/Restaurar) - Al seleccionar Restaurar desactiva el soporte de autenticación de inicio y borra la información de autenticación del Dispositivo Embedded Security. El cambio de esta configuración requiere apagar la computadora y luego encenderla. Administración del sistema operativo de Dispositivo Embedded Security (algunos modelos) (activar/desactivar) - Esta opción permite que el usuario limite el control del sistema operativo del Dispositivo Embedded Security. El cambio de esta configuración requiere apagar la computadora y luego encenderla. Esta opción permite que el usuario limite el control del Sistema Operativo del Dispositivo Embedded Security. • Restaurar Dispositivo Embedded Security a través del Sistema Operativo (algunos modelos) (activar/desactivar) - Esta opción permite que el usuario limite la capacidad del sistema operativo para solicitar una Restauración de Valores Predeterminados de Fábrica del Dispositivo Embedded Security. El cambio de esta configuración requiere apagar la computadora y luego encenderla. **NOTA:** Es necesario definir una contraseña de Configuración para activar esta opción. Soporte de Contraseña de BIOS para Smart Card (algunos modelos) (activar/desactivar) - Permite que el usuario active y desactive la Smart Card para uso en lugar de Contraseñas de Configuración e Inicio. Esta configuración requiere inicialización adicional en ProtectTools antes de que esta opción entre en vigor. PAVP (algunos modelos) (desactivada/mínimo/máximo) - PAVP activa la Ruta Protegida de Audio y Vídeo en el Chipset. Esto puede permitir la visualización de algún contenido protegido de alta definición que de otra manera sería prohibida su reproducción. La selección de Máximo asignaría 96 Megabites de memoria de sistema exclusivamente para PAVP.
Setupr Security Level (Nivel de seguridad de configuración)	Proporciona un método que permite el acceso limitados de usuarios finales para cambiar opciones de configuración especificadas, sin tener que conocer la contraseña de configuración. Este recurso ofrece al administrador la flexibilidad de proteger cambios de opciones de configuración esenciales, mientras permite que el usuario vea la configuración del sistema y configure opciones no esenciales. El administrador especifica derechos de acceso a opciones de configuración individuales, caso por caso, a través del menú nivel de seguridad de configuración. Por función predeterminada, a todas las opciones de configuración se le asignan contraseñas de configuración, indicándole al usuario que debe ingresar la contraseña de configuración correcta durante la operación POST para hacer cambios en cualquiera de las opciones. El administrador puede definir los elementos individuales en Ninguno, lo que indica que el usuario puede hacer cambios a las opciones especificadas cuando se ha obtenido acceso a la configuración con contraseñas inválidas. La opción, ninguno, es reemplazada por la contraseña de inicio, si ésta ha sido activada. **NOTA:** La configuración de modo de exploración debe ser definida en activar para que el usuario pueda ingresar a la configuración sin conocer la contraseña de configuración.

Seguridad con contraseña

La contraseña de inicio 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 Utilidad de Configuración y también se puede utilizar para anular la contraseña de inicio. Es decir, cuando se solicita la contraseña de inicio, 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 inicio, incluso si se estableció una.

Establecimiento de una contraseña de configuración a través de la Utilidad de Configuración

Si el sistema está equipado con un dispositivo embedded security, consulte la *Guía HP ProtectTools Security Manager* en http://www.hp.com. El establecimiento de una contraseña de configuración a través de la Utilidad de Configuración evita la reconfiguración de la computadora (uso de la Guía de la utilidad de Configuración hasta el ingreso de la contraseña.

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio** > **Apagar** > **Reiniciar**.
2. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

3. Seleccione **Security (Seguridad)**, luego **Setup Password (Contraseña de configuración)** y siga las instrucciones en pantalla.
4. Antes de salir, haga clic en **File (Archivo)** > **Save Changes and Exit (Guardar cambios y salir)**.

Establecimiento de una contraseña de inicio a través de la Utilidad de Configuración

El establecimiento de una contraseña de inicio a través de la Utilidad de Configuración evita el acceso a la computadora cuando ésta se enciende, a menos que se ingrese la contraseña. Cuando se establece una contraseña de inicio, la Utilidad de Configuración presenta **Password Options (Opciones de contraseña)** en el menú **Security (Seguridad)**. Las opciones de contraseña incluyen el **Password Prompt on Warm Boot (Mensaje de contraseña en el inicio en caliente)**. Cuando

Password Prompt on Warm Boot (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**.
2. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

3. Seleccione **Security (Seguridad)**, luego **Power-On Password (Contraseña de inicio)** y siga las instrucciones en pantalla.
4. Antes de salir, haga clic en **File (Archivo)** > **Save Changes and Exit (Guardar cambios y salir)**.

Ingreso de contraseñas de encendido

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

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

NOTA: 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, usted debe apagar la computadora y luego enciéndala nuevamente antes de continuar.

Ingreso de una contraseña de configuración

Si el sistema está equipado con un dispositivo embedded security, consulte la *Guía HP ProtectTools Security Manager* en http://www.hp.com.

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

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio** > **Apagar** > **Reiniciar**.
2. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

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

NOTA: 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, usted debe apagar la computadora y luego enciéndala nuevamente antes de continuar.

Cambio de una contraseña de inicio o de configuración

Si el sistema está equipado con un dispositivo embedded security, consulte la *Guía HP ProtectTools Security Manager* en http://www.hp.com.

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio** > **Apagar** > **Reiniciar**.
2. Para cambiar la contrasena de encendido, vaya a la etapa 3.

   Para cambiar la contraseña de Configuración, tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

3. 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`

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

4. Presione Intro.

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

NOTA: Consulte Caracteres delimitadores del teclado nacional en la página 33 para obtener información sobre los caracteres delimitadores alternativos. Las contraseñas de inicio y de configuración también se pueden cambiar utilizando las opciones de Seguridad en la Utilidad de Configuración.

Eliminación de una contraseña de inicio o de configuración

Si el sistema está equipado con un dispositivo embedded security, consulte la *Guía HP ProtectTools Security Manager* en http://www.hp.com.

1. Encienda o reinicie la computadora. Si está en Windows, haga clic en **Inicio** > **Apagar** > **Reiniciar**.
2. Para eliminar la contrasena de encendido, vaya a la etapa 3.

   Para eliminar la contraseña de Configuración, tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

3. 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/`
4. Presione Intro.

NOTA: Consulte Caracteres delimitadores del teclado nacional en la página 33 para obtener información sobre los caracteres delimitadores alternativos. Las contraseñas de inicio y de configuración también se pueden cambiar utilizando las opciones de Seguridad en la Utilidad de Configuración.

Caracteres delimitadores del teclado nacional

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

Caracteres Delimitadores del Teclado Nacional					
/	Árabe	-	Griego	/	Ruso
=	Belga	.	Hebreo	-	Eslovaco
-	BHCMSE*	-	Húngaro	-	Español
/	Português de Brasil	-	Italiano	/	Sueco/Finlandés
/	Chino	/	Japonés	-	Suizo
-	Checo	/	Coreano	/	Taiwanés
-	Danés	-	América Latina	/	Tailandés
!	Francés	-	Noruego	.	Turco
é	Francés Canadiense	-	Polaco	/	Inglés de Estados Unidos
-	Alemán	-	Portugués		

* Para Bosnia-Herzegovina, Croacia, Montenegro, Serbia y Eslovenia

Borrado de contraseñas

Si olvida la contraseña, usted no podrá acceder la computadora. Consulte la *Guía de solución de problemas* para obtener instrucciones sobre la eliminación de contraseñas.

Si el sistema está equipado con un dispositivo embedded security, consulte la *Guía HP ProtectTools Security Manager* en http://www.hp.com.

DriveLock

DriveLock es un recurso de seguridad estándar de la industria que impide el acceso no autorizado a los datos de discos duros ATA. DriveLock se implementó como una extensión de la Utilidad de Configuración. Está disponible sólo cuando los discos duros que admiten el conjunto de comandos de seguridad ATA son detectados. 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 una combinación 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 utilizarse 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 realizan copias de seguridad 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

Cuando se detectan una o más unidades de disco duro que admiten el conjunto de comandos de seguridad ATA, aparecerá la opción DriveLock en el menú Seguridad de la Utilidad de Configuración. 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 inicio 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. En el inicio en frío, es posible utilizar la contraseña principal o la de usuario. En el inicio en caliente, ingrese la misma contraseña usada para desbloquear la unidad durante el inicio en frío precedente. Los usuarios tendrán dos intentos para ingresar una contraseña correcta. En el inicio en frío, si ninguno de los intentos tiene éxito, la POST continuará, pero los datos de la unidad permanecerán inaccesibles. En el inicio en caliente o durante el reinicio desde Windows, si no tiene éxito en los intentos, se suspenderá la operación POST y el usuario recibirá instrucciones sobre el ciclo de alimentación.

Aplicaciones DriveLock

La utilización más práctica del recurso de seguridad DriveLock es en un ambiente corporativo. El administrador del sistema es responsable de configurar la unidad de disco duro, lo que implica, entre otras cosas, la configuración de la contraseña principal de DriveLock y la contraseña de usuario temporal. En caso de que el usuario olvide la contraseña de usuario o que la computadora se transfiera a otro empleado, la contraseña principal se puede utilizar 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 de trabajar en la empresa. En tal caso, el disco duro queda inutilizable y es necesario reemplazarlo. Asimismo, si no se establece 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 la Utilidad de Configuración y a DriveLock se puede restringir a través de 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 de Extracción de Cubierta, disponible en algunos modelos, es una combinación de tecnología de hardware y de software que puede advertirle sobre la extracción de la cubierta o del panel lateral de la computadora. Existen tres niveles de protección, tal como se describe en la siguiente tabla.

Tabla 11-2 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 exhibe un mensaje que indica la extracción de la cubierta o del panel lateral de la computadora.
Nivel 2	Contraseña de configuración	Al reiniciarse la computadora, la pantalla exhibe un mensaje que indica la extracción de la cubierta o del panel lateral de la computadora. Debe ingresar la contraseña de configuración para continuar.

NOTA: Esta configuración se puede cambiar a través de la Utilidad de Configuración. Para obtener más información acerca de la configuración del equipo, consulte la *Guía de la Guía de la utilidad de Configuración del Equipo (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**.
2. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

   NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.
3. Seleccione **Security (Seguridad)** > **Smart Cover (Cubierta inteligente)** > **Cover Removal Sensor (Sensor de retiro de cubierta)**, y seleccione el nivel deseado de seguridad.
4. Antes de salir, haga clic en **File (Archivo)** > **Save Changes and Exit (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 algunas computadoras HP. 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 obtener una máxima seguridad del bloqueo de cubierta, asegúrese de establecer una contraseña de configuración. La contraseña de configuración evita el acceso no autorizado a la Utilidad de Configuración.

NOTA: El bloqueo inteligente de cubierta está disponible como una opción en algunos sistemas.

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**.
2. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

   NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

3. Seleccione **Security (Seguridad)** > **Smart Cover (Cubierta inteligente)** > **Cover Lock (Bloqueo de cubierta)** > **Lock Option (Opción de bloqueo)**.
4. Antes de salir, haga clic en **File (Archivo)** > **Save Changes and Exit (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**.
2. Tan pronto como se encienda la computadora, presione F10 para ingresar a la Utilidad de Configuración, antes que la computadora inicie el sistema operativo. Presione intro para saltar la pantalla de título, si necesario.

   NOTA: Si no presiona la tecla F10 en el momento apropiado, usted debe reiniciar la computadora y presionar nuevamente la tecla F10 para ingresar a la utilidad, antes que la computadora inicie el sistema operativo.

3. Seleccione **Security (Seguridad)** > **Smart Cover (Cubierta inteligente)** > **Cover Lock (Bloqueo de cubierta)** > **Unlock (Desbloquear)**.
4. Antes de salir, haga clic en **File (Archivo)** > **Save Changes and Exit (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 la fuente 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, a través de un representante de ventas o proveedor de servicios autorizado.

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

- Entre en contacto con un representante de ventas o proveedor de servicios autorizado de HP.
- Llame al número correspondiente de la lista que aparece en la garantía.

Para obtener más información acerca del uso de la Llave a Prueba de Fallas de la Cubierta Inteligente, consulte la *Guía de Hardware.*

Medida de cable de bloqueo

El panel trasero de la computadora (algunos modelos) admite un bloqueo de cable, para fijar físicamente la computadora a un área de trabajo.

Para obtener instrucciones sobre ilustraciones, consulte la *Guía de Hardware*.

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.

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

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.

Si la computadora está conectada a una red administrada por HP Client Manager, la computadora envía un aviso de falla a la aplicación de administración de red. Con el Software HP Client Manager, puede también programar diagnósticos a distancia para ejecutar automáticamente en todos las computadoras administrados y crear informes detallados de las pruebas con fallas.

Sistema de protección de unidades

El sistema de protección de unidades (DPS) es una herramienta de diagnóstico incorporada en los discos duros instalados en algunas computadoras HP. El DPS se ha proyectado para ayudar a diagnosticar problemas que podrían provocar el reemplazo de la unidad de disco duro sin garantía.

Cuando se fabrican las computadoras HP, cada unidad disco duro instalada 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 graban en la unidad de disco duro. El proveedor de servicios puede utilizar esta información como ayuda para diagnosticar las condiciones que causaron la ejecución del 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 2.000 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 monitoreo 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 se dañen o se pierdan datos.

△ **PRECAUCIÓN:** Una condición de alta temperatura puede resultar en daños al sistema o pérdida de datos.

Índice