

# Guía de Desktop Management

## Ordenadores de empresa HP

© Copyright 2009 Hewlett-Packard Development Company, L.P. La información contenida en el presente documento está sujeta a cambios sin previo aviso.

Microsoft, Windows, Windows Vista y Windows 7 son marcas comerciales o marcas comerciales registradas de Microsoft Corporation en Estados Unidos y otros países.

Intel y vPro son marcas comerciales de Intel Corporation en los Estados Unidos y en otros países.

Las únicas garantías para los productos y servicios de HP quedan establecidas en las declaraciones de garantía expresa que acompañan a dichos productos y servicios. La información contenida aquí no debe interpretarse como garantía adicional. HP no se hace responsable de las omisiones ni de los errores técnicos o de edición que pueda contener este documento.

Este documento contiene información propietaria protegida por copyright y no puede ser fotocopiado, reproducido ni traducido a otro idioma, ya sea parcialmente o en su totalidad, sin el consentimiento previo y por escrito de Hewlett-Packard Company.

Guía de Desktop Management

Ordenadores de empresa HP

Cuarta edición (septiembre de 2009)

Referencia: 581009-071

## Acerca de este libro

Esta guía ofrece definiciones e instrucciones sobre cómo utilizar las funciones de seguridad y manejabilidad preinstaladas en determinados modelos.

- △ **¡ADVERTENCIA!** El texto señalado de esta forma significa que si no se siguen las indicaciones, se podrían producir lesiones personales e incluso la muerte.
- △ **PRECAUCIÓN:** El texto señalado de esta forma significa que si no se siguen las indicaciones, podrían producirse daños en el equipo o pérdida de información.
- 📝 **NOTA:** El texto señalado de esta forma proporciona información complementaria importante.



---

# Tabla de contenido

## 1 Introducción a Desktop Management

## 2 Distribución y configuración inicial

HP Client Automation Agent .....	2
HP Client Manager .....	3

## 3 Instalación remota del sistema

## 4 Actualización y gestión del software

HP Client Management Interface .....	5
HP SoftPaq Download Manager .....	6
HP System Software Manager .....	6
HP ProtectTools Security Manager .....	7
HP Client Automation Starter y Standard Edition .....	8
HP Client Automation Enterprise Edition .....	8
HP Client Manager de Symantec .....	8
Altiris Client Management Suite .....	9
HP Client Catalog para Microsoft System Center & SMS Products .....	10
Tecnología de gestión remota .....	10
Configuración de Intel Management Engine .....	11
Verdiem Surveyor .....	13
HP Proactive Change Notification .....	13
Suscripción .....	13
Soluciones retiradas .....	13

## 5 Memoria flash de la ROM

Memoria flash de la ROM remota .....	14
HPQFlash .....	14

## 6 Modo de recuperación de emergencia del bloqueo de arranque

## 7 Duplicación de la configuración

Copia en un único ordenador .....	16
-----------------------------------	----

Copia en múltiples ordenadores .....	17
Creación de dispositivos con capacidad de arranque .....	18
Dispositivos de medios USB flash compatibles .....	18
Dispositivos de medios USB flash no compatibles .....	19

## 8 Botón de encendido de modo dual

## 9 Asistencia técnica de HP en el sitio Web

## 10 Estándares de la industria

## 11 Seguimiento y seguridad de activos

Seguridad mediante contraseña .....	28
Definición de una contraseña de configuración mediante Computer Setup .....	29
Definición de una contraseña de arranque mediante Computer Setup .....	29
Introducción de una contraseña de arranque .....	30
Introducción de una contraseña de configuración .....	30
Modificación de una contraseña de arranque o de configuración .....	31
Eliminación de una contraseña de arranque o de configuración .....	31
Caracteres delimitadores de un teclado nacional .....	32
Eliminación de contraseñas .....	32
Bloqueo de la unidad .....	32
Utilización de la opción Bloqueo de la unidad .....	33
Aplicaciones de Bloqueo de la unidad .....	33
Sensor de Smart Cover .....	35
Configuración del nivel de protección del sensor de Smart Cover .....	35
Bloqueo de Smart Cover .....	35
Activación de Bloqueo de Smart Cover .....	36
Desactivación de Bloqueo de Smart Cover .....	36
Utilización de la llave de seguridad Smart Cover FailSafe Key .....	36
Candado con cadena .....	37
Tecnología de identificación de huellas digitales .....	37
Notificación y solución de errores .....	37
Sistema de protección de unidades .....	37
Fuente de alimentación con protector de sobretensión .....	37
Sensor térmico .....	38

<b>Índice .....</b>	<b>39</b>
---------------------	-----------

---

# 1 Introducción a Desktop Management

HP Client Management Solutions proporciona soluciones basadas en estándares para gestionar y controlar ordenadores de sobremesa, workstations y ordenadores portátiles en un entorno de red. HP fue pionera en la manejabilidad de ordenadores de sobremesa con la introducción en 1995 de los primeros ordenadores personales de sobremesa completamente manejables de la industria. HP tiene una patente en tecnología de manejabilidad. Desde entonces, HP ha realizado grandes esfuerzos para desarrollar los estándares y la infraestructura necesarios para distribuir, configurar y gestionar de forma efectiva ordenadores de sobremesa, workstations y ordenadores portátiles. HP desarrolla su propio software de gestión y trabaja en estrecha colaboración con los proveedores de soluciones de software de gestión líderes en la industria para garantizar la compatibilidad entre HP Client Management Solutions y estos productos. Las soluciones HP Client Management Solutions representan un aspecto importante de nuestro extenso compromiso por proporcionar soluciones que le ayuden a disminuir los gastos totales de mantenimiento de los ordenadores a lo largo de su ciclo de vida.

Las funciones y características clave de Desktop Management son las siguientes:

- Configuración y distribución inicial
- Instalación remota del sistema
- Actualización y gestión del software
- Memoria flash de la ROM
- Configuración de las opciones de hardware
- Seguimiento y seguridad de activos
- Notificación de fallos y recuperación

---

 **NOTA:** Las funciones específicas admitidas que se describen en esta guía varían según el modelo o la versión de software.

---

---

## 2 Distribución y configuración inicial

El equipo se entrega con una imagen de software del sistema preinstalada. Después de un breve proceso de “desempaquetado” del software, ya se puede utilizar el ordenador.

Si lo desea, puede sustituir la imagen de software preinstalada por un conjunto personalizado de software del sistema y las aplicaciones. Una imagen de software personalizada puede distribuirse de varias formas. Por ejemplo:

- Instalar aplicaciones de software adicionales tras desempaquetar la imagen de software preinstalada.
- Utilizar herramientas de distribución de software, como HP Client Automation Standard Edition o HP Client Automation Enterprise Edition (basado en tecnología Radia) para sustituir el software preinstalado por una imagen de software personalizada.
- Utilizar un proceso de clonación del disco para copiar el contenido de una unidad de disco duro a otra.

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

El hardware ACPI y la configuración basada en ROM proporcionan más ayuda a la hora de recuperar el software del sistema, gestionar la configuración y solucionar problemas, además de gestionar la alimentación.

### HP Client Automation Agent

El agente de gestión que utiliza HP Client Automation Standard Edition y HP Client Automation Enterprise Edition está precargado en el ordenador. Cuando está instalado, permite la comunicación con la consola de gestión HP.

Para instalar HP Client Automation Agent:

1. Haga clic en **Inicio**.
2. Haga clic en **Todos los programas**.
3. Haga clic en **HP Manageability**.
4. Haga clic en el **HP Management Agent Readme** aplicable al idioma que desee.
5. Revise y siga las instrucciones que se incluyen en el archivo Readme para instalar HP Client Automation Agent.

HP Client Automation Agent es un componente de infraestructura clave que permite activar todas las soluciones HP Client Automation. Para obtener más información sobre el resto de componentes de

infraestructura necesarios para implementar las soluciones de administración de configuración de HP, visite <http://h20229.www2.hp.com/solutions/ascm/index.html>.

## HP Client Manager

HP Client Manager (HPCM) es una solución gratuita desarrollada por Symantec para todos los ordenadores HP Blade, estaciones de trabajo, portátiles y ordenadores de sobremesa empresariales de HP compatibles. HPCM incluye herramientas de HP específicas como System Software Manager, HP Instant Support Professional Edition y HP Client Management Interface que permiten que un modelo centralizado administre, supervise y controle todo el hardware de HP compatible.

HP Client Manager 7.0 ofrece un nuevo portal que actúa a modo de tienda de paso en que el administrador puede llevar a cabo las siguientes tareas de gestión:

- Inventario
- Alertas
- Administración de BIOS
- Actualizaciones del controlador
- Activar HP Instant Support Health Scan and Diagnostics
- Realizar tareas de Embedded Security
- Ver HP Health Alert Trend global de los últimos 3-6 meses
- Ver si los ordenadores compatibles cumplen los requisitos de HP Instant Support Health Scan and Diagnostics
- Ver el Resumen de equipos HP, un desglose de los diferentes ordenadores HP Blade, estaciones de trabajo, portátiles y ordenadores de sobremesa compatibles.
- Ver Alertas: Activo, Umbral, Estado del hardware
- Informes
- Tareas administrativas para actualizar herramientas específicas de HP

HPCM se puede descargar de <http://www.symantec.com/business/theme.jsp> haciendo clic en **HP Client Manager** en **Productos de socios estratégicos**. De la página de descarga, también se puede obtener una licencia permanente gratuita.

También hay vídeos sobre la utilización de HPCM en <http://www.symantec.com/connect>. Busque **HP Client Manager 7.0** para ver, paso a paso, vídeos para las diferentes tareas que se incluyen en HPCM.

---

## 3 Instalación remota del sistema

La instalación remota del sistema permite iniciar y configurar el sistema con la información de software y configuración ubicada en un servidor de red con sólo iniciar Preboot Execution Environment (PXE). La función Instalación remota del sistema se utiliza generalmente como una herramienta de configuración e instalación del sistema, que además se puede emplear para llevar a cabo las siguientes acciones:

- Dar formato a la unidad de disco duro
- Distribuir una imagen de software en uno o más PC nuevos
- Actualizar de forma remota el BIOS del sistema en la memoria flash de la ROM ([Memoria flash de la ROM remota en la página 14](#))

---

 **NOTA:** Existen medios para encender la BIOS del sistema desde el sistema operativo Microsoft Windows.

---

- Configurar los ajustes del BIOS del sistema

Para iniciar la función Instalación remota del sistema, pulse **F12** cuando aparezca el mensaje **F12 = Arranque de servicio de red** en la esquina inferior derecha de la pantalla del logotipo de HP al arrancar el ordenador. Siga las instrucciones que aparecen en la pantalla para continuar el proceso. El orden de arranque predeterminado es un ajuste de la configuración del BIOS que se puede cambiar para intentar que se arranque siempre desde PXE.

---

## 4 Actualización y gestión del software

HP proporciona varias herramientas para la gestión y actualización del software de los equipos de sobremesa y portátiles, y workstations:

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, Standard y Enterprise Edition
- HP Client Manager de Symantec
- Altiris Client Management Suite
- HP Client Catalog para Microsoft System Center & SMS Products
- Ordenadores Intel vPro con Tecnología de gestión activa
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

### HP Client Management Interface

Independientemente de las herramientas de gestión del sistema que se utilicen en el departamento de TI, la gestión de los soportes de hardware y software es importante para mantener bajos los costes del departamento y que la empresa sea ágil. El administrador de TI puede acceder a HP Client Management Interface programando scripts sencillos e integrándolos en la solución de gestión de su elección.

Gracias a HP Client Management Interface (HP CMI), los nuevos ordenadores empresariales de HP se integran sin problemas en un entorno de tecnología de la información gestionado. HP CMI incluye una interfaz que ayuda a simplificar la integración de los ordenadores empresariales de HP con las conocidas herramientas de gestión del sistema del sector (entre las que se incluyen Microsoft Systems Management Server, IBM Tivoli Software y HP Operations) y aplicaciones de gestión personalizadas desarrolladas in situ. Mediante el empleo de HP CMI, las herramientas y aplicaciones de gestión de sistemas pueden solicitar información exhaustiva de inventario de los clientes, recibir información de estado del ordenador y gestionar la configuración de la BIOS del sistema mediante la comunicación directa con el ordenador del cliente, con lo que se reduce la necesidad de disponer de un software conector o agente para lograr la integración.

HP Client Management Interface está basado en los estándares del 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 utiliza la tecnología foundation de HP Client Management Solutions. Con HP CMI, HP ofrece la flexibilidad de elegir cómo gestionar los ordenadores clientes HP.

HP Client Management Interface utilizado junto con un software de gestión de sistemas puede realizar lo siguiente:

- Solicitar información exhaustiva de inventarios de los clientes y capturar información detallada sobre los procesadores, unidades de disco duro, memorias, BIOS y controladores, incluidos sensores de información (como velocidad del ventilador, voltaje y temperatura)
- Recibir información sobre el estado del ordenador: suscripción a una gran variedad de alertas de hardware cliente (como, por ejemplo, exceso de temperatura, ventiladores y cambios en la configuración del hardware) para enviarlos a la consola de gestión del sistema, a la aplicación o al ordenador del cliente local. Las alertas se envían en tiempo real cuando las provocan conflictos de hardware
- Gestión de la configuración del BIOS del sistema: realizar funciones F10 como poner y cambiar contraseñas del BIOS y solicitar el arranque en modo remoto de algún sistema cliente, o de todos, desde la consola de gestión sin tener que ir a cada máquina

Para obtener más información sobre HP Client Management Interface, consulte <http://www.hp.com/go/hpcmi/>.

## HP SoftPaq Download Manager

HP SoftPaq Download Manager es una interfaz gratuita y fácil de utilizar que sirve para ubicar y descargar las actualizaciones de software de los modelos de PC HP client en el entorno. Podrá ubicar, clasificar y seleccionar rápidamente los softpaqs que necesita con sólo especificar los modelos, el sistema operativo y el idioma. Para descargar HP SoftPaq Download Manager, visite <http://www.hp.com/go/sdm>.

## HP System Software Manager

HP System Software Manager (SSM) es una utilidad que automatiza la distribución remota de los controladores de dispositivos y las actualizaciones del BIOS de los ordenadores HP para empresa en red. Cuando se ejecuta SSM, esta utilidad determina de manera silenciosa (sin interacción del usuario) la revisión de los niveles de controladores y del BIOS instalados en cada sistema cliente en red y compara este inventario con el sistema de software SoftPaqs que se ha aprobado y almacenado en un almacén central de archivos. A continuación, SSM actualiza automáticamente cualquier software de sistema que se tenga que revisar entre los ordenadores de la red a los niveles más recientes disponibles en el almacén de archivos. Como SSM sólo permite la distribución de actualizaciones SoftPaq a los modelos de sistema cliente correctos, los administradores de sistemas pueden utilizar SSM con confianza y eficiencia para mantener actualizado el software de los sistemas.

System Software Manager se integra con herramientas de distribución de software para empresas, como, por ejemplo, las soluciones HP Client Automation, HP Client Manager de Symantec y Microsoft Systems Management Server (SMS). El uso de SSM le permite distribuir actualizaciones de terceros o creadas por el usuario que se han empaquetado en formato SSM.

SSM se puede descargar gratuitamente en <http://www.hp.com/go/ssm>.

---

 **NOTA:** SSM no admite actualmente memoria flash de ROM en sistemas que tienen Windows BitLocker Drive Encryption habilitada y que utilizan mediciones TPM para proteger las claves BitLocker porque encender la BIOS invalidaría la firma de confianza que BitLocker creó para la plataforma. Deshabilite BitLocker a través de Group Policy para encender la BIOS del sistema.

Puede habilitar la compatibilidad con BitLocker sin medidas TPM del BIOS para evitar invalidar las claves de BitLocker. HP recomienda mantener una copia de seguridad de las credenciales de BitLocker por si se produce alguna situación de recuperación de emergencia.

---

## HP ProtectTools Security Manager

El software de seguridad HP ProtectTools proporciona características de seguridad que contribuyen a proteger los equipos, redes y datos vitales frente a cualquier acceso no autorizado. Los siguientes módulos de software mejoran la funcionalidad de seguridad y se puede acceder a ellos a través de HP ProtectTools Security Manager:

HP ProtectTools Security Manager es la única consola a través de la cual se accede a los demás módulos.

- Credential Manager for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Privacy Manager for HP ProtectTools
- File Sanitizer for HP ProtectTools
- Java Card Security para HP ProtectTools
- Embedded Security for HP ProtectTools
- Device Access Manager for HP ProtectTools
- LoJack Pro para HP ProtectTools

HP ProtectTools ofrece dos versiones que se pueden utilizar: HP ProtectTools Security Manager y HP ProtectTools Administrative Console. Tanto la versión del administrador como la del usuario se encuentran disponibles en el menú **Inicio > Todos los programas**.

Los módulos de software disponibles para su ordenador pueden variar dependiendo del modelo. Por ejemplo, Embedded Security for HP ProtectTools sólo está disponible para equipos en los que esté instalado el chip de seguridad integrada del módulo Trusted Platform Module (TPM).

Es posible que los módulos de software HP ProtectTools ya estén preinstalados, precargados o disponibles para llevar a cabo la descarga en la página Web de HP. Para seleccionar los ordenadores de sobremesa HP Pro, HP ProtectTools se encuentra disponible como un producto con coste independiente. Para obtener más información, visite <http://www.hp.com/products/security>.

## HP Client Automation Starter y Standard Edition

HP Client Automation es una solución de gestión de hardware y software para entornos de Windows Vista, Windows XP y HP Thin Client de uso sencillo y rápida implantación que proporciona una sólida base para requisitos futuros. Existen dos ediciones disponibles:

- Starter Edition es un producto gratuito para gestionar ordenadores de escritorio, portátiles y estaciones de trabajo de HP, e incluye inventario de hardware y software, control remoto, control de alertas de HP, actualizaciones de HP BIOS y de controlador, integración con HP Protect Tools y soporte complementario para Intel AMT. Asimismo, admite la implantación y gestión de HP Thin Client.
- Standard Edition, disponible a la venta, incluye todas las funciones de la edición anterior, además de implantación y migración de Windows, capacidades de gestión de parches, distribución de software y medición de uso de software.

HP Client Automation Starter y Standard Edition proporcionan un ruta de migración a HP Client Automation Enterprise Edition (basado en tecnología Radia) para la gestión automatizada de entornos de TI de gran tamaño, heterogéneos y en constante cambio.

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

## HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition es una solución basada en directivas que permite a los administradores realizar inventarios, implantar, trabajar con parches y gestionar de manera constante el software y los contenidos en plataformas de cliente heterogéneas. Gracias a HP Client Automation Enterprise Edition, los profesionales de TI pueden realizar lo siguiente:

- Automatizar el proceso de gestión de ciclo de vida en su totalidad, desde la detección y la implantación hasta la migración y la eliminación, pasando por la gestión continua
- Implantar automáticamente y gestionar de manera constante un conjunto de software en su totalidad (sistemas operativos, aplicaciones, parches, configuraciones y contenidos) como mejor le convenga
- Gestionar software en prácticamente cualquier dispositivo, incluyendo equipos de escritorio, estaciones de trabajo y portátiles, en una infraestructura heterogénea o independiente
- Gestionar software en la mayoría de sistemas operativos

Gracias a la gestión continua de la configuración, los clientes de HP disfrutan de notables ahorros en costes de TI, tiempos acelerados de salida al mercado del software y de su contenido y una mayor productividad y satisfacción en su uso.

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

## HP Client Manager de Symantec

HP Client Manager de Symantec, desarrollado con Altiris, se encuentra disponible de manera gratuita para todos los modelos de estaciones de trabajo, portátiles y ordenadores de sobremesa empresariales de HP compatibles. SSM se integra en HP Client Manager y permite el seguimiento, supervisión y gestión central de los aspectos de hardware de los sistemas HP client.

HP Client Manager de Symantec se puede utilizar para lo siguiente:

- Obtener importante información de hardware como CPU, memoria, vídeo y configuración de seguridad
- Supervisar el estado del sistema para solucionar los problemas antes de que ocurran
- Adquirir e instalar de forma automática actualizaciones de controladores y el BIOS sin ir a cada ordenador
- Configurar de forma remota el BIOS y realizar la configuración de seguridad
- Automatizar los procesos para solucionar con rapidez los problemas de hardware

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

- Diagnósticos: ejecución y visualización remota de informes con ordenadores de sobremesa, portátiles y workstations de HP
- Examen del estado del sistema: búsqueda de problemas de hardware conocidos en la base instalada de los sistemas clientes de HP
- Sesiones de chat activas: conexión con atención al cliente de HP para resolver problemas.
- Base de conocimientos de HP: enlace a información experta
- Colección de SoftPaq automatizada y proceso de entrega para una rápida resolución de problemas de hardware.
- Identificación, realización de inventarios e inicio de los sistemas con el chip de seguridad integrada de HP ProtectTools
- Opción de visualización de las alertas del estado de modo local, en el sistema cliente
- Entrega de inventarios de información básica para los no clientes de HP
- Instalación y configuración del chip de seguridad TPM
- Programación central de las copias de seguridad y la recuperación del cliente
- Compatibilidad con complementos para administrar Intel AMT

Para obtener más información sobre 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 usar para gestionar software de ciclo de vida completo en ordenadores de sobremesa, portátiles y estaciones de trabajo. Client Management Suite incluye los siguientes productos Altiris:

- Inventory Solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution

- Application Metering Solution
- Application Management Solution
- Carbon Copy Solution

Para obtener más información sobre Altiris Client Management Suite, visite <http://www.symantec.com/business/client-management-suite>.

## HP Client Catalog para Microsoft System Center & SMS Products

HP Client Catalog permite que los profesionales de TI puedan utilizar los productos de Microsoft para automatizar la distribución de las actualizaciones de software de HP (Softpaqs) en ordenadores empresariales de HP. El archivo del catálogo contiene información detallada sobre la plataforma de las estaciones de trabajo, portátiles y ordenadores de sobremesa empresariales de HP. Se puede utilizar junto con las funciones de actualización e inventario actualizadas de los productos Microsoft con el fin de proporcionar actualizaciones automáticas de correctores y controladores para los ordenadores HP client gestionados.

Entre los productos Microsoft compatibles con HP Client Catalog se encuentran los siguientes:

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

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

## Tecnología de gestión remota

Los modelos incluyen tecnología vPro o tecnología estándar. Ambas tecnologías permiten la mejora de la detección, recuperación y protección de recursos informáticos de red. Asimismo, permiten la gestión de los PC independientemente de que el sistema esté encendido, apagado o el sistema operativo esté bloqueado.

Las tres formas posibles de gestión remota disponibles en ordenadores empresariales de sobremesa son Alert Standard Format (ASF), Intel Active Management Technology (AMT) y Desktop and mobile Architecture for Systems Hardware (DASH).

Las funciones de tecnología de gestión remota incluyen lo siguiente:

- Detección de red
- Información de inventario de hardware
- Control del estado de la plataforma
- Gestión del estado encendido/apagado, energía del ciclo

- Diagnósticos y reparación remotos
  - El redireccionamiento de la consola de texto permite que la consola controle el ordenador remoto durante la fase de arranque
  - El redireccionamiento multimedia permite que el sistema arranque desde una unidad, un disco o una imagen ISO remotos (las dos variantes son IDE-Redirect [IDE-R] en plataformas AMT y USB Media Redirection).
- Aislamiento y recuperación basado en hardware: limita y corta el acceso a la red, si se detecta la actividad de un posible virus
- Supervisión y auditoría de eventos de plataforma
- Portal de gestión de servidores web integrados para acceso y configuración remotos
- Las tecnologías de gestión remota están integradas a los socios de consola de gestión de HP

---

 **NOTA:** Todas las funciones anteriores no se encuentran disponibles en todas las plataformas.

---

## Configuración de Intel Management Engine

---

 **NOTA:** Para obtener una descripción general sobre la tecnología Intel vPro, visite la página Web <http://www.intel.com/vpro>.

Para obtener información específica sobre la tecnología Intel vPro de HP, consulte la documentación técnica en la dirección <http://www.hp.com/support>. Seleccione el país y el idioma, seleccione **Ver información para la resolución de problemas y ayuda**, introduzca el número del modelo del ordenador y pulse **Intro**. En la categoría **Recursos**, haga clic en **Manuales (guías, suplementos, apéndices, etc.)**. En **Salto rápido a manuales por categorías**, haga clic en **Libro blanco**.

---

Las tecnologías de gestión disponibles incluyen lo siguiente:

- AMT (incluye DASH 1.0)
- ASF
- DASH 1.1 (mediante NIC de Broadcom)

Puede que ASF y AMT no se puedan configurar al mismo tiempo, pero sean compatibles.

Configuración de sistemas Intel vPro para AMT o ASF:

1. Encienda o reinicie el equipo. Si trabaja con Microsoft Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Tan pronto como se encienda el ordenador, pulse la teclas de acceso rápido **Ctrl+P** antes de que arranque el sistema operativo.

---

 **NOTA:** Si no pulsa **Ctrl+P** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo el conjunto de teclas **Ctrl+P** antes de que arranque el sistema operativo que accede a la utilidad.

---

Esta tecla de acceso rápido introduce la utilidad de configuración de Intel Management Engine BIOS Execution (MEBx). Esta utilidad permite al usuario configurar varios aspectos de la tecnología de gestión. A continuación, se enumeran algunas opciones de configuración:

- Menú principal
  - Configuración de Intel® ME
  - Configuración de Intel® AMT
  - Cambio de contraseña de Intel® ME
  - Salir
- Configuración de la plataforma de Intel® ME
  - Control de estado de Intel® ME (activar/desactivar)
  - Actualización local del firmware de Intel® ME (activar/desactivar)
  - Control de funciones de Intel® ME
  - Control de alimentación de Intel® ME
- Configuración de Intel® AMT
  - Nombre de host
  - TCP/IP
  - Modelo de disposición (Enterprise, SMB)
  - Configuración e instalación
  - Eliminar disposición
  - SOL/IDE-R (activar/desactivar)
  - Directiva de contraseñas
  - Actualización segura del firmware (activar/desactivar)
  - Configurar PRTC
  - Límite de tiempo de inactividad
- Cambio de la contraseña de Intel® ME (HP recomienda encarecidamente cambiar la contraseña. La contraseña predeterminada es **admin**.)

Para gestionar de manera remota los sistemas AMT, el administrador debe utilizar una consola remota compatible con AMT. Las consolas de gestión para empresas se pueden obtener a través de proveedores como HP, Altiris y Microsoft SMS. En modo SMB, el cliente proporciona una interfaz de explorador Web. Para acceder a esta opción, abra un explorador desde cualquier otro sistema de la red e introduzca `http://host_name:16992` donde `host_name` es el nombre asignado al sistema. Como alternativa, se puede utilizar la dirección IP en lugar del nombre de host.

Para configurar sistemas con un NIC con capacidad DASH de Broadcom:

Consulte la documentación más reciente en el sitio <http://www.hp.com>, en **Asistencia técnica & Solución de problemas**, y seleccione su modelo específico y, a continuación, seleccione **Manuales y Libro blanco** en relación con DASH o el NIC de Broadcom.

## Verdiem Surveyor

Verdiem Surveyor es una solución de software que ayuda a gestionar el coste energético del equipo. Surveyor mide y notifica el consumo de energía del equipo. También permite controlar la configuración de la alimentación del equipo, lo que permite a los administradores implementar fácilmente estrategias de ahorro energético en sus redes. Un HP SoftPaq que incluya el agente Surveyor se puede descargar del sitio de web de soporte de HP e instalar en modelos de equipos de escritorio comerciales compatibles. Las licencias de Surveyor para gestionar equipos se pueden adquirir a través de su representante de HP.

## HP Proactive Change Notification

El programa Notificación de cambios proactiva utiliza la página Web Subscriber's Choice para lograr, de una forma proactiva y automática:

- Enviar mensajes de correo electrónico PCN (Proactive Change Notification o Notificación de cambios proactiva) informando de los cambios de hardware y software que tendrán lugar en la mayoría de los ordenadores y servidores del mercado hasta con 60 días de antelación.
- Enviar mensajes de correo electrónico con boletines para el cliente, consejos, notas, boletines de seguridad y alertas de controladores para la mayoría de los ordenadores y servidores del mercado.

El usuario crea su propio perfil para garantizar que sólo recibe la información relevante para su entorno de TI específico. Si desea más información sobre el programa Proactive Change Notification y sobre cómo crear un perfil personalizado, visite <http://h30046.www3.hp.com/subhub.php>

## Suscripción

Subscriber's Choice es un servicio de HP basado en el cliente.

De acuerdo con su perfil, HP le proporcionará sugerencias personalizadas del producto, artículos de funciones o alertas/notificaciones sobre soporte y controladores.

Las alertas/notificaciones sobre soporte y controladores de Subscriber's Choice le enviarán mensajes de correo electrónico indicándole que la información a la que está suscrito en su perfil está disponible para su consulta y recuperación. Si desea más información sobre Subscriber's Choice y cómo crear un perfil personalizado, visite <http://h30046.www3.hp.com/subhub.php>.

## Soluciones retiradas

Dos paquetes de software, Altiris Local Recovery y Dantz Retrospect, se dejarán de enviar en estaciones de trabajo, portátiles y ordenadores empresariales de HP.

---

## 5 Memoria flash de la ROM

La BIOS del ordenador se guarda en una memoria flash de ROM programable (memoria de solo lectura). Si se crea una contraseña de configuración en la utilidad Computer Setup (F10), se puede proteger la ROM de actualizaciones o sobreescrituras involuntarias. Esto es importante para asegurarse de que el ordenador funciona perfectamente. Si necesita o quiere actualizar la BIOS, puede descargar las últimas imágenes BIOS desde el controlador de HP y la página de asistencia <http://www.hp.com/>.

- △ **PRECAUCIÓN:** Para una protección máxima de la ROM, asegúrese de crear una contraseña de configuración. La contraseña de configuración impide actualizaciones de ROM involuntarias. System Software Manager permite que el administrador del sistema cree una contraseña de configuración en uno o más ordenadores al mismo tiempo. Para obtener más información, visite <http://www.hp.com/go/ssm>.

### Memoria flash de la ROM remota

Gracias a la memoria flash de la ROM remota, el administrador del sistema puede actualizar de forma segura el BIOS de los ordenadores HP remotos desde la consola de gestión de red centralizada. Al permitir al administrador del sistema realizar esta tarea de forma remota en múltiples ordenadores, se consigue una distribución uniforme y un mayor control de las imágenes de la memoria ROM de PC de HP en toda la red. También se logra una mayor productividad y un menor coste total de propiedad.

- 📝 **NOTA:** SSM no admite actualmente memoria flash de ROM en sistemas que tienen Windows BitLocker Drive Encryption habilitada y que utilizan mediciones TPM para proteger las claves BitLocker porque encender la BIOS invalidaría la firma de confianza que BitLocker creó para la plataforma. Deshabilite BitLocker a través de Group Policy para encender la BIOS del sistema.

El equipo debe estar encendido, o en estado de activación remota, para poder aprovechar la memoria flash de la ROM remota.

Para obtener más información sobre la memoria flash remota de ROM, consulte HP Client Manager Software o System Software Manager en <http://www.hp.com/go/ssm/>.

### HPQFlash

La utilidad HPQFlash se utiliza para restaurar y actualizar de forma local el BIOS del sistema de PC independientes desde un sistema operativo Windows.

Para obtener más información sobre HPQFlash, visite <http://www.hp.com/> e introduzca el número de modelo del ordenador cuando se le pida.

---

## 6 Modo de recuperación de emergencia del bloqueo de arranque

Modo de recuperación de emergencia del bloqueo de arranque permite la recuperación del sistema en el caso improbable de fallo de la memoria ROM. Por ejemplo, si se produjera un fallo de alimentación durante la actualización del BIOS, la memoria flash de la ROM quedaría incompleta. Esto estropearía el BIOS del sistema de manera inservible. El bloqueo de arranque es una sección protegida de la memoria flash de la ROM que contiene código que comprueba si existe una imagen del BIOS válida cuando se enciende el sistema.

- Si la imagen BIOS del sistema es válida, el sistema se inicia normalmente.
- Si la imagen BIOS del sistema no es válida, un BIOS del bloqueo de arranque seguro proporciona suficiente soporte para buscar medios extraíbles para los archivos de imagen BIOS. Si se encuentra un archivo de imagen BIOS apropiado, automáticamente se muestra en la ROM.

Cuando se detecta una imagen BIOS del sistema no válida, los indicadores luminosos de alimentación del sistema parpadean en rojo 8 veces, un parpadeo por segundo. Al mismo tiempo, el altavoz emitirá 8 pitidos. Si la porción de la ROM del sistema que contiene la imagen ROM en la opción vídeo no está dañada, **Modo de recuperación de emergencia del bloqueo de arranque** se mostrará en la pantalla.

Para recuperar el sistema cuando se encuentra en Modo de recuperación de emergencia del bloqueo de arranque, siga estos pasos:

1. Apague el ordenador.
2. Inserte un CD o dispositivo flash USB que contenga en el directorio raíz el archivo de imagen BIOS que desee.

 **NOTA:** Los medios deben estar formateados con el sistema de archivos FAT12, FAT16 o FAT32.

3. Encienda el equipo.

Si no se encuentra un archivo de imagen BIOS apropiado, se le solicitará insertar un medio que contenga un archivo de imagen BIOS.

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

4. Extraiga los medios extraíbles utilizados para actualizar el BIOS.
5. Encienda el ordenador para reiniciarlo.

 **NOTA:** BitLocker evita que Windows Vista se inicie cuando hay un CD que contiene el archivo de imagen BIOS en una unidad óptica. Si está activado BitLocker, extraiga este CD antes de intentar arrancar desde Windows Vista.

---

---

# 7 Duplicación de la configuración

Los siguientes procedimientos permiten al administrador copiar fácilmente una configuración en otros ordenadores del mismo modelo. Esto facilita la configuración rápida y más coherente de varios equipos.

 **NOTA:** Ambos procedimientos precisan una unidad de disquete o una unidad USB flash compatible.

**NOTA:** System Software Manager (SSM) se puede utilizar para duplicar información de configuración del ordenador desde el sistema operativo Windows. Para obtener más información, consulte la Guía del usuario de SSM en <http://www.hp.com/go/ssm>.

## Copia en un único ordenador

△ **PRECAUCIÓN:** Una configuración es específica para cada modelo. El sistema de archivos puede fallar si el ordenador inicial y el ordenador destino no son del mismo modelo. Por ejemplo, no copie la configuración de un ordenador dc7xxx a un ordenador dx7xxx.

1. Seleccione la configuración que desea copiar. Apague el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Apagar**.
2. Si utiliza un dispositivo de medios USB flash, insértelo ahora.
3. Encienda el equipo.
4. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

5. Si utiliza un disquete, insértelo ahora.
6. Haga clic en **Archivo > Configuración duplicada > Guardar en medio extraíble**. Siga las instrucciones que aparecen en la pantalla para crear el dispositivo de medios USB flash o disquete de configuración.
7. Apague el ordenador para configurarlo e inserte el dispositivo de medios USB flash o el disquete de configuración.
8. Encienda el ordenador para configurarlo.
9. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

10. Haga clic en **Archivo > Configuración duplicada > Restaurar desde medio extraíble** y siga las instrucciones que aparecen en la pantalla.
11. Reinicie el ordenador cuando la configuración se complete.

## Copia en múltiples ordenadores

△ **PRECAUCIÓN:** Para cada modelo hay una configuración específica. El sistema de archivos puede fallar si el ordenador inicial y el ordenador destino no son del mismo modelo. Por ejemplo, no copie la configuración de un ordenador dc7xxx en un ordenador dx7xxx.

Con este método se tarda un poco más en el momento de preparar el dispositivo de medios USB flash o disquete de configuración, pero el proceso de copia la configuración en los ordenadores destino es significativamente más rápido.

📝 **NOTA:** Se necesita una unidad de disquete de arranque para este procedimiento o crear un dispositivo de medios USB flash de arranque. Si no dispone de Windows XP para crear una unidad de disquete de arranque, utilice el método para copiar en un único ordenador (consulte [Copia en un único ordenador en la página 16](#)).

1. Creación de un dispositivo de medios USB flash o disquete de arranque. Consulte [Dispositivos de medios USB flash compatibles en la página 18](#) o [Dispositivos de medios USB flash no compatibles en la página 19](#).

△ **PRECAUCIÓN:** No todos los ordenadores se pueden arrancar desde un dispositivo de medios USB flash. Si el orden de arranque predeterminado en la utilidad Computer Setup (F10) muestra el dispositivo USB antes que el disco duro, el ordenador se puede arrancar desde un dispositivo de medios USB flash. Si no es así, hay que utilizar un disquete de arranque.

2. Seleccione la configuración que desea copiar. Apague el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Apagar**.
3. Si utiliza un dispositivo de medios USB flash, insértelo ahora.
4. Encienda el equipo.
5. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

📝 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

6. Si utiliza un disquete, insértelo ahora.
7. Haga clic en **Archivo > Configuración duplicada > Guardar en medio extraíble**. Siga las instrucciones que aparecen en la pantalla para crear el dispositivo de medios USB flash o disquete de configuración.
8. Descargue la utilidad BIOS para duplicar la configuración (repset.exe) y cópiela en el disquete de configuración o en el dispositivo de medios USB flash. Para obtener esta utilidad, vaya a <http://welcome.hp.com/country/us/en/support.html> e introduzca el número de modelo del ordenador.
9. En el dispositivo de medios USB flash o la unidad de disquete de configuración, cree un archivo autoexec.bat que contenga el siguiente comando:

repsset.exe

10. Apague el ordenador para configurarlo. Inserte el dispositivo de medios USB flash o la unidad de disquete de configuración y encienda el ordenador. La utilidad de configuración se ejecutará automáticamente.
11. Reinicie el ordenador cuando haya terminado con la configuración.

## Creación de dispositivos con capacidad de arranque

### Dispositivos de medios USB flash compatibles

Los dispositivos compatibles tienen una imagen preinstalada para simplificar el proceso de convertirlos en dispositivos de arranque. Todos los ordenadores HP o Compaq y muchos otros dispositivos de medios USB flash tienen esta imagen preinstalada. Si el dispositivo de medios USB flash que se está utilizando no cuenta con esta imagen, utilice el procedimiento que se indica más adelante en esta misma sección (consulte [Dispositivos de medios USB flash no compatibles en la página 19](#)).

Para crear un dispositivo de medios USB flash de arranque, debe tener lo siguiente:

- un dispositivo de medios USB flash compatible,
- un disquete DOS de arranque con los programas FDISK y SYS, y (Si el programa SYS no está disponible, puede utilizar FORMAT, pero se perderán todos los archivos existentes en el dispositivo de medios USB flash.)
- un ordenador que se arranque desde un dispositivo de medios USB flash.

△ **PRECAUCIÓN:** Quizá algunos ordenadores antiguos no se puedan arrancar con un dispositivo de medios USB flash. Si el orden de arranque predeterminado en la utilidad Computer Setup (F10) muestra el dispositivo USB antes que el disco duro, el ordenador se puede arrancar desde un dispositivo de medios USB flash. Si no es así, hay que utilizar un disquete de arranque.

1. Apague el equipo.
2. Introduzca el dispositivo de medios USB flash en uno de los puertos USB del ordenador y desconecte el resto de los dispositivos de almacenamiento que tenga conectados a otros puertos USB excepto las unidades de disquete USB.
3. Introduzca un disquete DOS de arranque con FDISK.COM y SYS.COM o FORMAT.COM en una unidad de disquete. A continuación, encienda el equipo para arrancar desde el disquete DOS.
4. Ejecute FDISK en el mensaje **A:\** introduciendo `FDISK` y pulsando **Intro**. Si el sistema lo solicita, haga clic en **Sí (Y)** para lograr un mayor rendimiento de disco.
5. Seleccione la opción [5] para ver las unidades del sistema. El dispositivo de medios USB flash será la unidad que más coincida con el tamaño de una de las unidades de la lista. Normalmente será la última unidad de la lista. Tome nota de la letra de la unidad.

Unidad del dispositivo de medios USB flash: \_\_\_\_\_

△ **PRECAUCIÓN:** Si no hay ninguna unidad que coincida con el dispositivo de medios USB flash, no siga adelante. Se podrían perder los datos. Compruebe todos los dispositivos de almacenamiento adicionales del resto de los puertos USB. Si se encuentra alguno, desconéctelo, reinicie el equipo y siga en el paso 4. Si no se encuentra ninguno, el sistema no admite el dispositivo de medios USB flash o éste está defectuoso. NO siga intentando hacer del dispositivo de medios USB flash la unidad de arranque.

6. Salga de FDISK pulsando la tecla **Esc** para regresar a la pantalla **A:\**.
7. Si el disquete DOS de arranque incluye SYS.COM, siga en el paso 8. En caso contrario, siga en el paso 9.
8. En la pantalla **A:\**, introduzca `SYS x:`, donde x representa la letra de la unidad indicada arriba.

**PRECAUCIÓN:** Asegúrese de que ha introducido la letra de la unidad correcta para el dispositivo de medios USB flash.

Una vez que se hayan transferido los archivos de sistema, SYS volverá a la pantalla **A:\**. Siga en el paso 13.

9. Copie los archivos del dispositivo de medios USB flash que desee guardar en un directorio temporal de otra unidad (por ejemplo, la unidad de disco duro interna del sistema).
10. En la pantalla **A:\**, introduzca `FORMAT /S X:` donde X representa la letra de la unidad indicada anteriormente.

**PRECAUCIÓN:** Asegúrese de que ha introducido la letra de la unidad correcta para el dispositivo de medios USB flash.

FORMAT mostrará uno o varios mensajes y le preguntará si desea continuar con el proceso cada vez. Introduzca **Y** en cada una de las ocasiones. FORMAT formateará el dispositivo de medios USB flash, añadirá los archivos del sistema y solicitará una etiqueta de volumen.

11. Pulse **Intro** si no desea ninguna etiqueta o introdúzcala si lo desea.
12. Copie los archivos que guardó en el paso 9 esta vez en el dispositivo de medios USB flash.
13. Extraiga el disquete y reinicie el ordenador. El equipo arrancará como si el dispositivo de medios USB flash fuera la unidad C.

**NOTA:** El orden de arranque predeterminado varía de un equipo a otro y se puede cambiar en la utilidad Computer Setup (F10).

Si ha utilizado una versión DOS de Windows 9x, es posible que aparezca brevemente la pantalla con el logotipo de Windows. Si no desea que aparezca esta pantalla, agregue un archivo de longitud cero llamado LOGO.SYS al directorio raíz del dispositivo de medios USB flash.

Vuelva a [Copia en múltiples ordenadores en la página 17](#).

## Dispositivos de medios USB flash no compatibles

Para crear un dispositivo de medios USB flash de arranque, debe tener lo siguiente:

- un dispositivo de medios USB flash,
- un disquete DOS de arranque con los programas FDISK y SYS, y (Si el programa SYS no está disponible, puede utilizar FORMAT, pero se perderán todos los archivos existentes en el dispositivo de medios USB flash.)
- un ordenador que se arranque desde un dispositivo de medios USB flash.

△ **PRECAUCIÓN:** Quizá algunos ordenadores antiguos no se puedan arrancar con un dispositivo de medios USB flash. Si el orden de arranque predeterminado en la utilidad Computer Setup (F10) muestra el dispositivo USB antes que el disco duro, el ordenador se puede arrancar desde un dispositivo de medios USB flash. Si no es así, hay que utilizar un disquete de arranque.

1. Si el sistema tiene alguna tarjeta PCI con unidades SCSI, ATA RAID o SATA conectadas a la misma, apague el equipo y desenchufe el cable de alimentación.

△ **PRECAUCIÓN:** El cable de alimentación DEBE estar desenchufado.

2. Abra el ordenador y extraiga las tarjetas PCI.
3. Introduzca el dispositivo de medios USB flash en uno de los puertos USB del ordenador y desconecte el resto de los dispositivos de almacenamiento que tenga conectados a otros puertos USB excepto las unidades de disquete USB. Cierre la cubierta del equipo.
4. Enchufe el cable de alimentación y encienda el ordenador.
5. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

6. Vaya a **Avanzado > Dispositivos PCI** para desactivar los controladores PATA y SATA. Cuando desactive el controlador SATA, anote el IRQ al que está asignado el controlador. Será necesario que reasigne el IRQ posteriormente. Salga de la configuración previa confirmación de los cambios.

SATA IRQ: \_\_\_\_\_

7. Introduzca un disquete DOS de arranque con FDISK.COM y SYS.COM o FORMAT.COM en una unidad de disquete. A continuación, encienda el equipo para arrancar desde el disquete DOS.
8. Ejecute FDISK y elimine las particiones existentes en el dispositivo de medios USB flash. Cree una partición nueva y márkela como activa. Salga de FDISK pulsando la tecla **Esc**.
9. Si el sistema no se reinicia automáticamente cuando salga de FDISK, pulse la combinación de teclas **Ctrl+Alt+Del** para reiniciar el sistema desde el disquete DOS.
10. En la pantalla **A:\**, introduzca `FORMAT C: /S` y presione **Intro**. FORMAT formateará el dispositivo de medios USB flash, agregará los archivos de sistema y le pedirá una etiqueta de volumen.
11. Pulse **Intro** si no desea ninguna etiqueta o introdúzcala si lo desea.
12. Apague el ordenador y desenchufe el cable de alimentación. Abra el ordenador y vuelva a instalar las tarjetas PCI que quitó anteriormente. Cierre la cubierta del equipo.
13. Enchufe el cable de alimentación, saque el disquete y encienda el ordenador.
14. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.
15. Vaya a **Avanzado > Dispositivos PCI** y reactive los controladores PATA y SATA que se desactivaron en el paso 6. Asigne el controlador SATA a su IRQ original.
16. Guarde los cambios y salga. El equipo arrancará como si el dispositivo de medios USB flash fuera la unidad C.

 **NOTA:** La orden de arranque por defecto varía de un ordenador a otro, y se puede modificar con la utilidad Computer Setup (F10). Consulte *Utilidad Computer Setup (F10)* para ver las instrucciones.

Si ha utilizado una versión DOS de Windows 9x, es posible que aparezca brevemente la pantalla con el logotipo de Windows. Si no desea que aparezca esta pantalla, agregue un archivo de longitud cero llamado LOGO.SYS al directorio raíz del dispositivo de medios USB flash.

Vuelva a [Copia en múltiples ordenadores en la página 17](#).

---

## 8 Botón de encendido de modo dual

Cuando ACPI (Interfaz de alimentación y configuración avanzada) está activada, el botón de encendido puede funcionar como un interruptor de encendido y apagado, o como un botón de modo en espera. La función de espera no apaga completamente el ordenador, sino que hace que entre en modo de estado de espera de bajo consumo. Esto permite desactivar rápidamente el sistema sin tener que cerrar las aplicaciones y volver rápidamente al mismo estado operativo en que se encontraba sin que se produzcan pérdidas de datos.

Para cambiar la configuración del botón de encendido, siga estos pasos:

1. Haga clic con el botón izquierdo del ratón en el botón **Inicio**, seleccione **Panel de control > Opciones de energía**.
2. En **Propiedades de Opciones de energía**, seleccione la pestaña **Opciones avanzadas**.
3. En la sección **Botones de encendido**, seleccione **Suspender**.

Tras configurar el botón de encendido para que funcione como un botón de modo en espera, pulse el botón de encendido para que el sistema pase al estado de ahorro de energía (espera). Pulse el botón de nuevo para que el sistema pase rápidamente al estado normal de funcionamiento. Para apagar completamente el sistema, mantenga pulsado el botón de encendido durante cuatro segundos.

---

△ **PRECAUCIÓN:** No utilice el botón de encendido para apagar el ordenador a menos que el sistema no responda; si apaga el equipo sin la interacción del sistema operativo, podría dañar el disco duro o perder datos.

---

---

## 9 Asistencia técnica de HP en el sitio Web

Los ingenieros de HP prueban y depuran de forma rigurosa el software desarrollado tanto por HP como por otros fabricantes, y desarrollan software de soporte específico para el sistema operativo con el fin de garantizar el nivel de rendimiento, compatibilidad y fiabilidad de los ordenadores de HP.

Cuando se realiza la transición a sistemas operativos nuevos o revisados, es importante implementar el software de soporte diseñado para el sistema operativo en cuestión. Si planea ejecutar una versión de Microsoft Windows que no sea la versión incluida con el ordenador, deberá instalar los controladores de dispositivo y las utilidades correspondientes para garantizar la compatibilidad y el funcionamiento adecuado de todas las funciones.

HP ha llevado a cabo la tarea de localizar, acceder, evaluar e instalar el software de asistencia más reciente de manera más fácil. Puede descargarse el software en <http://www.hp.com/support>.

La página Web contiene los controladores de dispositivo, las utilidades y las imágenes de la memoria flash de la ROM más actuales necesarios para ejecutar el sistema operativo Microsoft Windows más reciente en el ordenador de HP.

---

## 10 Estándares de la industria

Las soluciones de gestión de HP se integran con otras aplicaciones de administración de sistemas y se basan en estándares de la industria como:

- Administración de empresas basada en Web (WBEM, del inglés Web-Based Enterprise Management)
- Interfaz de administración de Windows (WMI, del inglés Windows Management Interface)
- Tecnología WOL (Wake on LAN)
- ACPI
- SMBIOS
- Soporte de ejecución previa al arranque (PXE)

# 11 Seguimiento y seguridad de activos

Las funciones de seguimiento de activos incorporadas en el ordenador proporcionan datos de seguimiento de activos clave que se pueden gestionar con HP Systems Insight Manager, HP Client Manager, HP OpenView Configuration Management y Asset Management Solutions u otras aplicaciones de administración de sistemas. Del mismo modo, la perfecta integración automática entre las funciones de seguimiento de activos y dichos productos permite al usuario seleccionar la herramienta de gestión que mejor se adapta a su entorno y equilibrar la inversión en herramientas existentes.

HP también ofrece varias soluciones para controlar el acceso a componentes e información valiosos. HP Embedded Security for ProtectTools, si está instalado, impide el acceso no autorizado a los datos, verifica la integridad del sistema y autentica a los usuarios externos que intentan acceder al sistema. (Si desea obtener más información, consulte la *Guía de HP ProtectTools Security Manager* en <http://www.hp.com/products/security>). Las características de seguridad, como por ejemplo, HP Embedded Security for ProtectTools, Sensor de Smart Cover y Smart Cover Lock, disponibles en algunos modelos, ayudan a impedir el acceso no autorizado a los componentes internos del ordenador. Para proteger los activos de datos valiosos, desactive los puertos paralelo, serie o USB, o bien las capacidades de arranque de soporte extraíble. Las alertas de Memory Change y del sensor de Smart Cover pueden enviarse automáticamente a las aplicaciones de gestión de sistemas como notificación proactiva de alerta de seguridad en los componentes internos del ordenador.

 **NOTA:** HP Embedded Security for ProtectTools, Sensor de Smart Cover y Bloqueo de Smart Cover están disponibles como opciones en algunos sistemas.

Utilice las utilidades siguientes para gestionar valores de seguridad en el ordenador de HP:

- Localmente, utilizando las utilidades Computer Setup. Consulte la *Guía de la utilidad Computer Setup (F10)* que se incluye con el ordenador para ver información adicional e instrucciones sobre la utilización de las utilidades Computer Setup.
- De forma remota, con HP Client Manager de Symantec, HP Client Automation o System Software Manager. Este software permite la distribución segura y coherente, además del control de los valores de seguridad.

La tabla y las secciones siguientes hacen referencia a la gestión de características de seguridad del equipo, de forma local, mediante las utilidades de Computer Setup (F10).

**Tabla 11-1 Descripción general de las características de seguridad**

Opción	Descripción
<b>Contraseña de configuración</b>	Sirve para establecer y activar la contraseña de configuración (administrador).  <b>NOTA:</b> Si se establece una contraseña de configuración, es necesario cambiar algunas opciones de la configuración del equipo, crear una memoria flash de la ROM y realizar cambios en determinados valores plug and play en Windows.

**Tabla 11-1 Descripción general de las características de seguridad (continuación)**

<b>Contraseña de arranque</b>	<p>Sirve para establecer y activar la contraseña de arranque. La solicitud de contraseña de arranque aparece tras un ciclo de alimentación. Si el usuario no introduce la contraseña de arranque correcta, la unidad no arrancará.</p> <p><b>NOTA:</b> Esta contraseña no aparece en arranques en caliente, como <b>Ctrl+Alt+Supr</b> o <b>Reinicio desde Windows</b>, a menos que esté activado en <b>Opciones de contraseña</b> (consulte a continuación).</p>
<b>Opciones de contraseña</b>  (Esta opción aparecerá únicamente si se ha establecido una contraseña de arranque o de configuración).	<p>Sirve para:</p> <ul style="list-style-type: none"><li>• Bloquear recursos de legado (aparecen si se establece una contraseña de configuración).</li><li>• Activar/desactivar el modo de servidor de red (aparece si se ha establecido una contraseña de arranque).</li><li>• Especificar si la contraseña es obligatoria para un arranque en caliente (<b>Ctrl+Alt+Supr</b>). Aparece si se ha establecido una contraseña de arranque.</li><li>• Activar/desactivar Setup Browse Mode (aparece si se ha establecido una contraseña de configuración). Permite visualizar, pero no cambiar, F10 Setup Options al introducir la contraseña de configuración.</li><li>• Activar/desactivar una contraseña estricta (aparece si se ha configurado una contraseña de arranque), que cuando se encuentra activada omite el puente de contraseña en placa para deshabilitar la contraseña de arranque.</li></ul> <p>Consulte la <i>Guía de Desktop Management</i> para obtener más información.</p>
<b>Smart Cover</b> (en algunos modelos)	<p>Sirve para lo siguiente:</p> <ul style="list-style-type: none"><li>• Bloquear/desbloquear Smart Cover.</li><li>• Configurar el sensor de eliminación de Smart Cover como Desactivar/Notificar al usuario/Contraseña de configuración.</li></ul> <p><b>NOTA:</b> <i>Notificar al usuario</i> avisa al usuario de que el sensor ha detectado que se ha retirado la cubierta. <i>Contraseña de configuración</i> requiere que se introduzca la contraseña de configuración para arrancar el equipo si el sensor detecta que se ha retirado la cubierta.</p> <p>Esta función sólo se admite en algunos modelos.</p>
<b>Seguridad de dispositivos</b>	<p>Permite establecer Dispositivo disponible/Dispositivo oculto para lo siguiente:</p> <ul style="list-style-type: none"><li>• Puertos de serie</li><li>• Puerto paralelo</li><li>• Puertos USB posteriores</li><li>• Puertos USB del panel frontal</li><li>• Puertos USB internos</li><li>• Audio del sistema</li><li>• Controladores de red (en algunos modelos)</li><li>• Unidad de disquete de legado</li><li>• Dispositivo de seguridad integrada (en algunos modelos)</li><li>• SATA0</li><li>• SATA1 (en algunos modelos)</li><li>• SATA2 (en algunos modelos)</li></ul>

**Tabla 11-1 Descripción general de las características de seguridad (continuación)**

	<ul style="list-style-type: none"><li>• SATA3 (en algunos modelos)</li><li>• eSATA (en algunos modelos)</li></ul>
<b>LoJack para HP ProtectTools</b>	<p>Permite controlar, gestionar y supervisar el ordenador a distancia.</p> <p>Una vez activado, LoJack Pro para HP ProtectTools se configura desde Absolute Software Customer Center. Desde Centro de atención al cliente, el administrador puede configurar LoJack para HP ProtectTools para controlar o gestionar el ordenador. Si el sistema se coloca en un lugar incorrecto o se roba, el centro de atención al cliente puede ayudar a las autoridades locales a localizar y recuperar el ordenador. Si está configurado, LoJack Pro puede seguir funcionando, aunque la unidad de disco duro se borre o se cambie.</p>
<b>Arranque de servicio de red</b>	<p>Sirve para activar o desactivar la posibilidad de que el equipo arranque desde un sistema operativo instalado en un servidor de red. (Esta característica sólo está disponible en modelos NIC; el controlador de red debe ser una tarjeta de expansión PCI o estar incorporado en la placa del sistema.)</p>
<b>Identificadores de sistema</b>	<p>Permite establecer:</p> <ul style="list-style-type: none"><li>• Identificador de activo (compuesto por 18 bytes), un número identificativo de propiedad que la empresa haya asignado al equipo.</li><li>• Identificador de propiedad (compuesto por 80 bytes) que se visualiza durante la POST.</li><li>• Número de serie del chasis o número identificador exclusivo universal (UUID). Este número UUID sólo se puede actualizar si el número de serie del chasis actual no es válido. (Estos números identificativos se establecen normalmente en la fábrica y se utilizan para identificar de forma exclusiva el sistema.)</li><li>• La configuración regional del teclado (por ejemplo, inglés o alemán) para la introducción del identificador del sistema.</li></ul>
<b>Seguridad de Bloqueo de la unidad</b>	<p>Sirve para asignar o modificar una contraseña maestra o de usuario para unidades de disco duro. Cuando esta función está activada, el sistema solicita al usuario que proporcione una de las contraseñas de Bloqueo de la unidad durante la POST. Si la información proporcionada no es correcta, no se podrá acceder a la unidad de disco duro hasta que se introduzca una contraseña correcta durante la secuencia de arranque en frío posterior.</p> <p><b>NOTA:</b> Esta selección sólo aparecerá cuando por lo menos una unidad que admita la función Bloqueo de la unidad esté conectada al sistema.</p>
<b>Nivel de seguridad de configuración</b>	<p>Proporciona un método que permite el acceso limitado a los usuarios finales para cambiar las opciones de configuración determinadas, sin tener que conocer la contraseña de configuración.</p> <p>Esta característica proporciona al administrador flexibilidad para proteger cambios en las opciones de configuración esenciales, mientras que permite al usuario visualizar la configuración del sistema y configurar opciones no esenciales. El administrador especifica los derechos de acceso en las opciones de configuración individuales caso a caso mediante el menú Nivel de seguridad de configuración. Por defecto, todas las opciones de configuración tienen asignada una contraseña de configuración que indica al usuario que debe introducir una contraseña de configuración correcta durante POST para realizar cambios en cualquiera de las opciones. El administrador puede establecer elementos individuales como Ninguno, indicando que el usuario puede realizar cambios en las opciones especificadas cuando se ha accedido a la configuración con contraseñas inválidas. La elección, Ninguno, se reemplaza por contraseña de arranque si una contraseña de arranque se activa.</p> <p><b>NOTA:</b> Se debe establecer Setup Browse Mode en Activar para que el usuario introduzca la configuración sin conocer la contraseña de configuración.</p>
<b>Seguridad del sistema (en algunos modelos: estas opciones dependen del hardware)</b>	<p>Prevención de ejecución de datos (activar/desactivar), sólo en algunos modelos: contribuye a evitar infracciones de seguridad en el sistema operativo.</p> <p>Tecnología de virtualización (activar/desactivar), sólo en algunos modelos: permite controlar las características de virtualización del procesador. Para modificar esta opción es necesario apagar el ordenador y volver a encenderlo.</p>

**Tabla 11-1 Descripción general de las características de seguridad (continuación)**

Tecnología de virtualización para E/S dirigida (activar/desactivar), sólo en algunos modelos: permite controlar las características de reasignación de DMA del conjunto de chips. Para modificar esta opción es necesario apagar el ordenador y volver a encenderlo.

Tecnología de ejecución de confianza (activar/desactivar), sólo en algunos modelos: permite controlar las características del procesador y el conjunto de chips subyacentes necesarios para admitir un dispositivo virtual. Para modificar esta opción es necesario apagar el ordenador y volver a encenderlo. Para activar esta característica, deberá activar las siguientes funcionalidades:

- Compatibilidad con dispositivos de seguridad integrada
- Tecnología de virtualización
- Tecnología de virtualización para E/S dirigida

Compatibilidad con dispositivos de seguridad integrada (activar/desactivar), sólo en algunos modelos: permite activar y desactivar el dispositivo de seguridad integrada. Para modificar esta opción es necesario apagar el ordenador y volver a encenderlo.

**NOTA:** Para configurar el dispositivo de seguridad integrada debe definirse una contraseña de configuración.

- Restablecer a los valores de configuración de fábrica (no restablecer/restablecer), sólo en algunos modelos: permite restablecer a los valores predeterminados de fábrica, aunque se borrarán todas las claves de seguridad. Para modificar esta opción es necesario apagar el ordenador y volver a encenderlo.

**PRECAUCIÓN:** El dispositivo de seguridad integrada es un componente crucial en numerosos programas de seguridad. Si se borran las claves de seguridad, se impedirá el acceso a los datos protegidos por el dispositivo de seguridad integrada. Si se selecciona la opción Restablecer a los valores de configuración de fábrica, pueden perderse datos importantes.

- Restablecer las credenciales de autenticación (no restablecer/restablecer), sólo en algunos modelos: permite desactivar la compatibilidad con la autenticación de arranque si se restablece y borra la información de autenticación del dispositivo de seguridad integrada. Para modificar esta opción es necesario apagar el ordenador y volver a encenderlo.

Administración del sistema operativo del dispositivo de seguridad integrada (activar/desactivar), sólo en algunos modelos: permite al usuario limitar el control del sistema operativo del dispositivo de seguridad integrada. Para modificar esta opción es necesario apagar el ordenador y volver a encenderlo. Esta opción permite al usuario limitar el control del sistema operativo del dispositivo de seguridad integrada.

- Restablecer el dispositivo de seguridad integrada a través del sistema operativo (activar/desactivar), sólo en algunos modelos: permite al usuario limitar la capacidad del sistema operativo de solicitar un restablecimiento de los valores de configuración de fábrica del dispositivo de seguridad integrada. Para modificar esta opción es necesario apagar el ordenador y volver a encenderlo.

**NOTA:** Para activar esta opción debe definirse una contraseña de configuración.

PAVP (desactivado/mín./máx.), sólo en algunos modelos: permite la ruta de vídeo/audio protegida en el conjunto de chips. De esta manera se podrá visualizar contenido de alta definición protegido que, de otra manera, no podría reproducirse. Al seleccionar Máx., se asignará de manera exclusiva 96 MB de la memoria del sistema a PAVP.

## Seguridad mediante contraseña

La contraseña de arranque impide la utilización no autorizada del equipo ya que se solicita la introducción de una contraseña para acceder a aplicaciones o a datos cada vez que se enciende o reinicia el equipo. La contraseña de configuración impide específicamente el acceso no autorizado a Computer Setup, y también se puede utilizar en sustitución de la contraseña de arranque. Es decir, si

cuando se solicita la contraseña de arranque se introduce en su lugar la contraseña de configuración, se podrá acceder igualmente al ordenador.

Se puede establecer una contraseña de configuración de toda la red para que el administrador del sistema pueda conectarse a todos los sistemas de red y realizar tareas de mantenimiento sin necesidad de conocer la contraseña de arranque, aunque se haya definido una.

 **NOTA:** System Software Manager (SSM) se puede utilizar para crear y administrar contraseñas BIOS desde el sistema operativo Windows. Para obtener más información, consulte la Guía del usuario de SSM en <http://www.hp.com/go/ssm>.

**NOTA:** HP Client Management Interface (HP CMI) proporciona acceso a la gestión de ajustes de BIOS, incluidas las contraseñas BIOS desde el sistema operativo Windows. Si desea obtener más información, consulte el libro blanco técnico de HP Client Management Interface en <http://www.hp.com/go/hpcmi>.

## Definición de una contraseña de configuración mediante Computer Setup

Si el sistema dispone de un dispositivo de seguridad incorporado, consulte la *Guía de HP ProtectTools Security Manager* en <http://www.hp.com>. Al crear una contraseña de configuración con Computer Setup, se impide la reconfiguración del ordenador (mediante la utilidad Computer Security [F10]) hasta que se introduzca la contraseña.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

3. Seleccione **Seguridad** y, a continuación, **Contraseña de configuración** y siga las instrucciones que aparecen en la pantalla.
4. Antes de salir, haga clic en **Archivo > Guardar cambios y salir**.

## Definición de una contraseña de arranque mediante Computer Setup

La definición de una contraseña de arranque mediante Computer Setup impide el acceso al equipo cuando está encendido si no se introduce la contraseña correspondiente. Si ha definido una contraseña de arranque, podrá seleccionar **Opciones de contraseña** en el menú **Seguridad** de Computer Setup. Las opciones de contraseña incluyen la **Solicitud de contraseña durante un arranque en caliente**. Si se ha activado la **solicitud de contraseña durante un arranque en caliente**, la contraseña también debe introducirse cada vez que se reinicie el ordenador.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

3. Seleccione **Seguridad** y, a continuación, **Contraseña de arranque** y siga las instrucciones que aparecen en la pantalla.
4. Antes de salir, haga clic en **Archivo > Guardar cambios y salir**.

## Introducción de una contraseña de arranque

Para introducir una contraseña de arranque, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Cuando aparezca el icono de llave en la pantalla, escriba la contraseña actual y, a continuación, pulse **Intro**.

---

 **NOTA:** Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

---

Si la contraseña introducida no es correcta, aparecerá un icono de llave rota. Inténtelo de nuevo. Al cabo de tres intentos sin éxito, deberá apagar el equipo y volver a encenderlo para poder continuar.

## Introducción de una contraseña de configuración

Si el sistema dispone de un dispositivo de seguridad incorporado, consulte la *Guía de HP ProtectTools Security Manager* en <http://www.hp.com>.

Si se ha establecido una contraseña de configuración en el ordenador, se le solicitará cada vez que ejecute Computer Setup.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

---

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

---

3. Cuando aparezca el icono de llave en la pantalla, escriba la contraseña de configuración y, a continuación, pulse la tecla **Intro**.

---

 **NOTA:** Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

---

Si la contraseña introducida no es correcta, aparecerá un icono de llave rota. Inténtelo de nuevo. Al cabo de tres intentos sin éxito, deberá apagar el equipo y volver a encenderlo para poder continuar.

## Modificación de una contraseña de arranque o de configuración

Si el sistema dispone de un dispositivo de seguridad incorporado, consulte la *Guía de HP ProtectTools Security Manager* en <http://www.hp.com>.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Para modificar la contraseña de arranque, vaya al paso 3.

Para cambiar la contraseña de configuración, tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

---

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

---

3. Cuando aparezca el icono de llave, escriba la contraseña actual, una barra inclinada (/) o un carácter delimitador alternativo, la nueva contraseña, otra barra inclinada (/) o un carácter delimitador alternativo, y otra vez la nueva contraseña, tal como se indica a continuación: `contraseña actual/nueva contraseña/nueva contraseña`

---

 **NOTA:** Preste atención al escribir la contraseña puesto que, por motivos de seguridad, los caracteres que se escriben no aparecen en la pantalla.

---

4. Pulse **Intro**.

La nueva contraseña se aplicará la próxima vez que encienda el equipo.

---

 **NOTA:** Para obtener información acerca de los caracteres delimitadores alternativos, consulte [Caracteres delimitadores de un teclado nacional en la página 32](#). La contraseña de arranque y la contraseña de configuración también pueden modificarse mediante las opciones de seguridad de Computer Setup.

---

## Eliminación de una contraseña de arranque o de configuración

Si el sistema dispone de un dispositivo de seguridad incorporado, consulte la *Guía de HP ProtectTools Security Manager* en <http://www.hp.com>.

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Para quitar la contraseña de arranque, vaya al paso 3.

Para borrar la contraseña de configuración, tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.

---

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

---

3. Cuando aparezca el icono de llave, escriba la contraseña actual seguida de una barra inclinada (/) o un carácter delimitador alternativo, tal como se muestra a continuación: `contraseña actual/`
4. Pulse **Intro**.

 **NOTA:** Para obtener información acerca de los caracteres delimitadores alternativos, consulte [Caracteres delimitadores de un teclado nacional en la página 32](#). La contraseña de arranque y la contraseña de configuración también pueden modificarse mediante las opciones de seguridad de Computer Setup.

## Caracteres delimitadores de un teclado nacional

Los distintos teclados se diseñan conforme a los requisitos específicos de cada país. La sintaxis y las teclas que utilice para modificar o eliminar la contraseña dependen del teclado que se entregó con el ordenador.

### Caracteres delimitadores de un teclado local

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

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

## Eliminación de contraseñas

Si olvida la contraseña, no podrá acceder al equipo. Para obtener instrucciones acerca de cómo borrar contraseñas, consulte la *Guía de solución de problemas en Documentation and Diagnostics CD*.

Si el sistema dispone de un dispositivo de seguridad incorporado, consulte la *Guía de HP ProtectTools Security Manager* en <http://www.hp.com>.

## Bloqueo de la unidad

Bloqueo de la unidad es una característica de seguridad estándar de la industria que impide el acceso no autorizado a los datos de unidades de disco duro ATA. Esta función se ha implementado como una extensión de Computer Setup. Sólo está disponible cuando se detectan unidades de disco duro que admiten el conjunto de comandos de seguridad ATA. La función de Bloqueo de la unidad ha sido ideada para los clientes de HP cuya preocupación principal es la seguridad de los datos. Para dichos clientes, el coste de la unidad de disco duro y la pérdida de los datos almacenados en ésta es irrelevante en comparación con los daños que pueden resultar del acceso no autorizado al contenido. A fin de equilibrar este nivel de seguridad con la necesidad práctica de facilitar una contraseña olvidada, la implementación de HP de Bloqueo de la unidad utiliza un esquema de seguridad de dos contraseñas. El administrador del sistema establece y utiliza una de las contraseñas, mientras que la otra, la establece y utiliza normalmente el usuario final. La unidad no puede desbloquearse si se han perdido ambas contraseñas. Por lo tanto, la forma más segura de utilizar Bloqueo de la unidad es duplicar los

datos de la unidad de disco duro en un sistema de información corporativo o hacer una copia de seguridad periódicamente. En el caso de que se pierdan ambas contraseñas de bloqueo, la unidad de disco duro queda inutilizada. Para los usuarios que no se ajustan al perfil de cliente anteriormente definido, esto puede suponer un riesgo inaceptable. Para los usuarios que se ajustan al perfil del cliente, puede constituir un riesgo tolerable dada la naturaleza de los datos almacenados en la unidad de disco duro.

## Utilización de la opción Bloqueo de la unidad

Cuando se detectan unidades de disco duro que admiten el conjunto de comandos de seguridad ATA, la opción de Bloqueo de la unidad aparece en el menú Seguridad de Computer Setup. El usuario tiene la posibilidad de establecer la contraseña maestra o de activar Bloqueo de la unidad. Debe proporcionarse una contraseña de usuario para activar Bloqueo de la unidad. Dado que la configuración inicial de Bloqueo de la unidad la realiza normalmente un administrador del sistema, primero debe establecerse una contraseña maestra. HP recomienda a los administradores de sistemas que definan una contraseña maestra tanto si desean activar Bloqueo de la unidad como si lo dejan desactivado. De esta manera, el administrador tiene la posibilidad de modificar los valores de Bloqueo de la unidad en el caso de que, posteriormente, se active esta función. Una vez establecida la contraseña maestra, el administrador del sistema puede activar Bloqueo de la unidad o dejarlo desactivado.

En el caso de una unidad de disco duro bloqueada, la POST solicitará una contraseña para desbloquear el dispositivo. Si se ha establecido una contraseña de arranque que coincide con la contraseña de usuario del dispositivo, la POST no solicitará que se vuelva a introducir la contraseña. De lo contrario, el usuario deberá introducir una contraseña de Bloqueo de la unidad. En un arranque en frío, puede utilizarse tanto la contraseña maestra como la contraseña de usuario. En un arranque en caliente, introduzca la misma contraseña utilizada para desbloquear la unidad durante el arranque en frío anterior. Los usuarios dispondrán de dos intentos para introducir una contraseña correcta. En el arranque en frío, si ninguno tiene éxito, la POST continuará pero no se podrá acceder a los datos de la unidad. En un arranque en caliente o reinicio desde Windows, si no funciona ningún intento, la POST se detendrá y se indicará al usuario mueva la fuente de alimentación.

## Aplicaciones de Bloqueo de la unidad

El uso más práctico de la característica de seguridad de Bloqueo de la unidad es en entornos corporativos. El administrador del sistema será el responsable de configurar la unidad de disco duro para el compartimiento multiusuario que implicará, entre otras cosas, definir la contraseña maestra de Bloqueo de la unidad y una contraseña de usuario temporal. En el caso de que el usuario olvidara su contraseña o que otro empleado utilizara el equipo, siempre podría utilizarse la contraseña maestra para volver a establecer la contraseña de usuario y tener nuevamente acceso a la unidad de disco duro.

HP recomienda a los administradores de sistemas corporativos que optan por activar Bloqueo de la unidad que establezcan también una política corporativa para establecer y mantener las contraseñas maestras. Esto debe realizarse para evitar una situación en la que un empleado modifique de forma intencionada, o no, ambas contraseñas de Bloqueo de la unidad antes de abandonar la compañía. En tal caso, la unidad de disco duro quedaría inutilizada y debería reemplazarse. Asimismo, si no se establece una contraseña maestra, los administradores del sistema pueden encontrarse con el acceso bloqueado a una unidad de disco duro, sin posibilidad de realizar comprobaciones rutinarias para detectar software no autorizado, ni otras funciones de control de activos y soporte técnico.

Para los usuarios con requisitos de seguridad menos estrictos, HP no recomienda que se active Bloqueo de la unidad. Entre los usuarios de esta categoría se incluyen los usuarios particulares o los usuarios que no mantienen datos sensibles en las unidades de disco duro de forma habitual. Para estos usuarios, la pérdida potencial de una unidad de disco duro consecuencia del olvido de ambas contraseñas es más importante que el valor de los datos para los que se ha diseñado la función de Bloqueo de la unidad. Puede restringirse el acceso a Computer Setup y a la función de Bloqueo de la unidad mediante

la contraseña de configuración. Al especificar una contraseña de configuración y no proporcionarla a los usuarios finales, los administradores del sistema restringen el número de usuarios que pueden activar Bloqueo de la unidad.

## Sensor de Smart Cover

El sensor de extracción de cubierta, disponible en algunos modelos, es una combinación de la tecnología de hardware y software capaz de advertirle de la extracción del panel lateral o la cubierta del panel del ordenador. Existen tres niveles de protección, que podrá comprobar en la siguiente tabla.

**Tabla 11-2 Niveles de protección del sensor de Smart Cover**

Nivel	Valor	Descripción
Nivel 0	Desactivado	Sensor de Smart Cover desactivado (valor predeterminado).
Nivel 1	Notificar al usuario	Cuando se reinicia el equipo, la pantalla visualiza un mensaje en el que se indica que se ha extraído la cubierta o el panel lateral del equipo.
Nivel 2	Contraseña de configuración	Cuando se reinicia el equipo, la pantalla visualiza un mensaje en el que se indica que se ha extraído la cubierta o el panel lateral del equipo. Debe introducir la contraseña de configuración para poder continuar.

**NOTA:** Estos valores pueden modificarse mediante Computer Setup. Para obtener más información sobre Computer Setup, consulte la *Guía sobre la utilidad Computer Setup (F10)*.

## Configuración del nivel de protección del sensor de Smart Cover

Para establecer el nivel de protección del sensor de Smart Cover, siga estos pasos:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.  
**NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.
3. Seleccione **Seguridad > Smart Cover > Sensor de extracción de cubierta** y seleccione el nivel de seguridad deseado.
4. Antes de salir, haga clic en **Archivo > Guardar cambios y salir**.

## Bloqueo de Smart Cover

Bloqueo de Smart Cover es un bloqueo de cubierta controlable mediante software incorporado en algunos ordenadores de HP. Este bloqueo impide el acceso no autorizado a los componentes internos. Los ordenadores se entregan con la función Bloqueo de Smart Cover en la posición de desbloqueo.

- △ **PRECAUCIÓN:** Para garantizar la máxima seguridad de cierre de cubierta, asegúrese de definir una contraseña de configuración. La contraseña de configuración evita el acceso no autorizado a la utilidad Computer Setup.
- 📖 **NOTA:** Bloqueo de Smart Cover está disponible como opción en algunos sistemas.

## Activación de Bloqueo de Smart Cover

Para activar y bloquear Bloqueo de Smart Cover, siga los pasos siguientes:

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.  

---

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

---
3. Seleccione **Seguridad > Smart Cover > Bloqueo de la cubierta > Opción de bloqueo**.
4. Antes de salir, haga clic en **Archivo > Guardar cambios y salir**.

## Desactivación de Bloqueo de Smart Cover

1. Encienda o reinicie el equipo. Si trabaja con Windows, haga clic en **Inicio > Apagar equipo > Reiniciar**.
2. Tan pronto como se encienda el ordenador, pulse la tecla **F10** antes de que arranque el sistema operativo para acceder a Computer Setup. Pulse **Intro** para omitir la pantalla de título, si procede.  

---

 **NOTA:** Si no pulsa la tecla **F10** en el momento oportuno, tendrá que volver a iniciar el ordenador y pulsar de nuevo la tecla **F10** antes de que arranque el sistema operativo para acceder a la utilidad.

---
3. Seleccione **Seguridad > Smart Cover > Bloqueo de la cubierta > Desbloquear**.
4. Antes de salir, haga clic en **Archivo > Guardar cambios y salir**.

## Utilización de la llave de seguridad Smart Cover FailSafe Key

Si activa Bloqueo de Smart Cover y no puede escribir la contraseña para desactivar el bloqueo, necesitará clave de seguridad de Smart Cover para abrir la cubierta del ordenador. Necesitará la llave en cualquiera de las circunstancias siguientes:

- Corte de alimentación.
- Fallo de arranque.
- Fallo de un componente del PC (por ejemplo, procesador o fuente de alimentación).
- Olvido de la contraseña.

 **PRECAUCIÓN:** HP dispone de una herramienta especializada llamada Smart Cover FailSafe Key. Prepárese, solicítela a su proveedor de servicio o distribuidor autorizado antes de que la necesite.

---

Para obtener la clave de seguridad, siga uno de estos pasos:

- Póngase en contacto con su proveedor de servicio o distribuidor autorizado de HP.
- Llame al número correspondiente que se indica en la garantía.

Para más información sobre cómo utilizar la clave de seguridad de Smart Cover, consulte la *Guía de referencia del hardware*.

## Candado con cadena

En el panel posterior del ordenador (algunos modelos) hay un candado con cadena para sujetar físicamente el ordenador al área de trabajo.

Para obtener instrucciones ilustradas, consulte la *Guía de referencia del hardware*.

## Tecnología de identificación de huellas digitales

Al eliminar la necesidad de introducir contraseñas de usuario, la tecnología de identificación de huellas digitales de HP refuerza la seguridad de la red, simplifica el proceso de conexión y reduce los costes asociados con la gestión de redes corporativas. Esta tecnología, cuyo precio es razonable, ya no está dirigida solamente a organizaciones de alta tecnología y seguridad.

---

 **NOTA:** La compatibilidad con la tecnología de identificación de huellas digitales varía según el modelo.

---

## Notificación y solución de errores

Las funciones de notificación de fallos y de recuperación combinan tecnología de hardware y de software innovadora para impedir la pérdida de datos críticos y minimizar los periodos de no disponibilidad no planeados.

Si el ordenador está conectado a una red gestionada por HP Client Manager, enviará un aviso de avería a la aplicación de gestión de la red. Con el software HP Client Manager, también puede planificar los diagnósticos de forma remota para que se ejecuten automáticamente en todos los PC y crear un informe de resumen de las pruebas fallidas.

## Sistema de protección de unidades

El sistema de protección de unidades (DPS) es una herramienta de diagnóstico incorporada en las unidades de disco duro que están instaladas en algunos ordenadores de HP. El sistema DPS está diseñado para ayudar a diagnosticar problemas que pueden requerir una sustitución de la unidad de disco duro no cubierta por la garantía.

Cuando se fabrican los ordenadores de HP, las unidades de disco duro instaladas se someten a pruebas mediante DPS y se graba un registro permanente de información clave en la unidad. Cada vez que se ejecuta DPS, los resultados de la prueba se graban en la unidad de disco duro. El servicio técnico puede utilizar esta información para diagnosticar las circunstancias que le han llevado a ejecutar el software DPS. Para obtener instrucciones acerca del uso de DPS, consulte la *Guía de solución de problemas*.

## Fuente de alimentación con protector de sobretensión

Una fuente de alimentación con protector de sobretensión integrada proporciona mayor fiabilidad cuando el ordenador se ve afectado por una sobretensión imprevista de la corriente. Esta fuente de alimentación está diseñada para resistir sobretensiones de hasta 2.000 voltios sin causar periodos de no disponibilidad ni pérdidas de datos en el equipo.

## Sensor térmico

El sensor térmico es una función de hardware y software que controla la temperatura interna del ordenador. Esta función emite un mensaje de advertencia si se supera el intervalo normal, con lo que dispondrá de tiempo suficiente para efectuar las acciones pertinentes antes de que se dañen los componentes internos o se pierdan los datos.

---

△ **PRECAUCIÓN:** Los datos pueden perderse y el sistema puede dañarse si se alcanza una temperatura muy elevada.

---

# Índice

## A

activación de Bloqueo de Smart Cover 36  
Altiris  
Client Management Suite 9

## B

BIOS  
HPQFlash 14  
memoria flash de la ROM remota 14  
Modo de recuperación de emergencia del bloqueo de arranque 15  
bloqueo de la cubierta 35  
Bloqueo de la unidad 32  
Bloqueo de Smart Cover  
activar 36  
desactivar 36  
botón de encendido de modo dual 22

## C

cambio de contraseña 31  
cambio de los sistemas operativos, asistencia técnica 23  
cambio de notificación 13  
candado de cadena 37  
caracteres delimitadores del teclado nacional 32  
caracteres delimitadores de teclado nacional 32  
Client Management Interface 5  
Client Manager de Symantec 8  
configuración  
copia en múltiples ordenadores 17  
copia en un único ordenador 16

configuración de encendido de modo dual 22  
configuración del botón de encendido 22  
configuraciones de instalación, duplicación 16  
configuración inicial 2  
configuración remota 4  
contraseña  
arrancar 29, 30  
borrar 32  
configuración 29, 30  
eliminar 31  
modificar 31  
seguridad 28  
contraseña de arranque  
eliminar 31  
introducir 30  
modificar 31  
valor 29  
contraseña de configuración  
eliminar 31  
introducir 30  
modificar 31  
valor 29  
control de acceso al equipo 25  
control del acceso al equipo 25

## D

desactivación de Bloqueo de Smart Cover 36  
direcciones de Internet. *Consulte* Web, sitios  
dispositivo de medios USB flash, con capacidad de arranque 18, 19

dispositivos con capacidad de arranque  
creación 18  
dispositivo de medios USB flash 18

## E

eliminación de contraseña 31, 32  
Entorno de ejecución previa al arranque 4  
equipo, temperatura interna 38  
estándares de la industria 24

## F

FailSafe Key, solicitud 36  
fuente de alimentación con protector de sobretensión 37

## H

herramienta de diagnóstico de unidades de disco duro 37  
herramientas de clonación, software 2  
herramientas de distribución, software 2

## HP

Client Automation Starter, Standard y Enterprise Edition 8  
Client Catalog para Microsoft System Center & SMS Products 10  
Client Management Interface 5  
Client Manager de Symantec 8  
ProtectTools Security Manager 7  
System Software Manager 6

- HP Client Automation Enterprise Edition 8
- HP Client Manager 3
- HPQFlash 14
- I**
- imagen de software preinstalada 2
- instalación inicial 2
- instalación remota del sistema 4
- introducción
  - arranque, contraseña 30
  - contraseña de configuración 30
- M**
- memoria flash de la ROM 14
- memoria flash de la ROM remota 14
- modo de recuperación de bloqueo de arranque de emergencia 15
- modo de recuperación de emergencia de bloqueo de arranque 15
- Modo de recuperación de emergencia del bloqueo de arranque 15
- N**
- notificación de cambios 13
- Notificación y solución de errores 37
- P**
- Proactive Change Notification (PCN) 13
- protección de la unidad 37
- protección de la unidad de disco duro 37
- protector de sobretensión, fuente de alimentación 37
- ProtectTools Security Manager 7
- R**
- recuperación, software 2
- S**
- seguimiento de activos 25
- seguridad
  - Bloqueo de la unidad 32
  - Bloqueo de Smart Cover 35
  - candado con cadena 37
  - características, tabla 25
  - configuración 25
  - contraseña 28
  - ProtectTools Security Manager 7
  - Sensor de Smart Cover 35
  - tecnología de identificación de huellas digitales 37
  - Sensor de Smart Cover niveles de protección 35
  - valor 35
  - sensor térmico 38
  - sistemas operativos, asistencia técnica para el cambio 23
  - Smart Cover FailSafe Key, solicitud 36
  - Smart Cover Lock FailSafe Key 36
  - software
    - Altiris Client Management Suite 9
    - distribución 2
    - herramientas de gestión y actualización 5
    - HP Client Automation Starter, Standard y Enterprise Edition 8
    - HP Client Catalog para Microsoft System Center & SMS Products 10
    - HP Client Management Interface 5
    - HP Client Manager de Symantec 8
    - HP ProtectTools Security Manager 7
    - HP System Software Manager 6
    - instalación remota del sistema 4
    - integración 2
    - Proactive Change Notification (PCN) 13
    - recuperación 2
    - seguimiento de activos 25
    - Sistema de protección de unidades 37
  - Tecnología de gestión remota 10
  - Verdiem Surveyor 13
  - solicitar FailSafe Key 36
  - soluciones retiradas 13
  - Suscripción 13
  - System Software Manager 6
  - T**
  - tabla de caracteres delimitadores 32
  - Tecnología de gestión remota 10
  - tecnología de identificación de huellas digitales 37
  - temperatura interna del equipo 38
  - U**
  - unidades de disco duro, herramienta de diagnóstico 37
  - V**
  - Verdiem Surveyor 13
  - W**
  - Web, sitios
    - Altiris Client Management Suite 10
    - Asistencia técnica de HP 11
    - Descarga de BIOS 14
    - Descargas de Software y Controladores 17
    - HP Business PC Security 7
    - HP Client Automation Agent 3
    - HP Client Automation Center 8
    - HP Client Catalog para Microsoft SMS 10
    - HP Client Management Interface 6
    - HP Client Manager 3
    - HP Client Manager de Symantec 9
    - HPQFlash 14
    - HP Softpaq Download Manager 6
    - HP System Software Manager 6
    - Memoria flash de la ROM 14
    - memoria flash de la ROM remota 14

Proactive Change	
Notification	13
soporte de software	23
Subscriber's Choice	13
tecnología Intel vPro	11