Guía HP ProtectTools Embedded Security

Computadoras de Escritorio Empresariales
HP dx5150

Número de Parte del Documento: 376352-161

Deciembre de 2004

Esta guía proporciona instrucciones para la utilización del software que le permite definir las configuraciones para el chip de HP ProtectTools Embedded Security.

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

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

Guía HP ProtectTools Embedded Security

Primera Edición: Deciembre de 2004

Número de Parte del Documento: 376352-161

Contenido

HP ProtectTools Embedded Security

HP ProtectTools Embedded Security

HP ProtectTools Security Manager es el software que permite configurar HP ProtectTools Embedded Security. El Manager es una interfaz (máscara) que señala varias opciones disponibles en el software Embedded Security. HP ProtectTools Embedded Security es el conjunto de software que incluye Personal Secure Drive (PSD), interfaz de chip TPM/encriptación, migración de seguridad, creación de archivo y control de contraseñas.

Requisitos

Con el fin de utilizar los recursos de seguridad, se necesitan las siguientes herramientas:

- Software HP ProtectTools Embedded Security
- Software HP ProtectTools Security Manager
- Chip de HP ProtectTools Embedded Security instalado en la computadora

Para obtener información sobre la configuración de la solución Embedded Security, consulte "Procedimientos de Configuración" en la página 8.

Conceptos Básicos sobre ProtectTools Embedded Security

Esta sección contiene información de alto nivel sobre conceptos que debe comprender para utilizar HP ProtectTools Embedded Security y HP ProtectTools Security Manager.

Chip de HP ProtectTools Embedded Security

El chip de Embedded Security es un componente de hardware que ofrece recursos de seguridad y encriptación y proporciona un área de almacenamiento a prueba de violaciones para proteger claves públicas y privadas. El chip viene instalado de fábrica y no se debe acceder a él ni se debe retirar, excepto por un proveedor de servicio autorizado por HP.

Personal Secure Drive

Uno de los recursos de Embedded Security es la Personal Secure Drive (PSD). La PSD es una unidad virtual creada en el disco duro durante el proceso de inicialización de Usuario de HP ProtectTools Embedded Security. Proporciona un área de almacenamiento protegida para datos sensibles. La PSD le permite crear y obtener acceso a archivos y carpetas, del mismo modo que otras unidades.

El acceso a la PSD requiere tanto acceso físico a la computadora en la cual reside la PSD como a la contraseña de la PSD. Cuando ingresa la contraseña de PSD, ésta se torna visible y los archivos se tornan disponibles para su utilización. Los archivos permanecen accesibles hasta que cierre la sesión, momento en el cual la PSD automáticamente oculta su presencia. No se puede acceder a las PSD desde una red.

Los datos encriptados se almacenan en la PSD. Las claves utilizadas para encriptar los archivos se almacenan en el chip de HP ProtectTools Embedded Security, asegurando que los datos sean protegidos contra el uso no autorizado y que sean “bloqueados” para la computadora. Esto significa que sólo se puede obtener acceso a los datos protegidos en la computadora de destino.

Correo electrónico

Secure email es otro importante recurso de Embedded Security. Permite que los usuarios compartan información confidencialmente y que tengan la seguridad de que se mantiene la autenticidad de la información durante la transferencia. Secure email le permite:

- Seleccionar un certificado de clave pública emitido por una Autoridad de Certificación (CA).
- Firmar Mensajes digitalmente.
- Encriptar mensajes.

HP ProtectTools Embedded Security y HP ProtectTools Security Manager optimizan la funcionalidad segura del correo electrónico proporcionando protección adicional para la clave utilizada para encriptar, desencriptar y firmar digitalmente mensajes. Optimizan la seguridad del correo electrónico cuando se usan los siguientes clientes de correo electrónico:

- Microsoft Outlook Express (versión 4 o superior)
- Microsoft Outlook 2000
- Microsoft Outlook 2002
- Netscape Messenger 4.79
- Netscape Messenger 7.0

Para obtener instrucciones sobre la utilización de clientes de correo electrónico, consulte la Ayuda de Integración de Correo Electrónico de HP ProtectTools Embedded Security.

Sistema de Archivos Encriptado Optimizado (EFS)

EFS es el servicio de encriptación de archivos ofrecido por Microsoft Windows 2000 y Windows XP Professional. EFS proporciona privacidad de datos ofreciendo la siguiente funcionalidad:

- Encriptación de archivos por el usuario cuando se almacena en un disco
- Rápido y fácil acceso a archivos encriptados
- Encriptación automática (y transparente) de datos
- Capacidad del administrador del sistema para recuperar datos encriptados por otro usuario

HP ProtectTools Embedded Security y HP ProtectTools Security Manager optimizan el EFS proporcionando protección adicional para la clave usada para encriptar y desencriptar datos.

Para obtener más información sobre EFS, consulte la Ayuda en línea del sistema operativo.

Usuarios y Administradores

Usuarios

Los usuarios tienen acceso básico a Embedded Security y pueden:

- enviar y recibir correo electrónico encriptado
- visualizar archivos y carpetas encriptadas
- inicializar la Clave del Usuario Básico personal
- crear, eliminar o modificar cuentas personales de usuario dentro de embedded security
- configurar, crear, utilizar y eliminar PSD individual

Administradores

Los Administradores inicializan la solución Embedded Security en una computadora y pueden:

- configurar la máquina local y los criterios de usuario de Embedded Security
- preparar claves de usuario y certificados para migración
- cambiar la contraseña de propietario de Embedded Security
- desactivar o activar Embedded Security
- autorizar computadoras de destino para migración de certificados y claves de usuario
- recuperar datos que hayan sido almacenados y encriptados utilizando Embedded Security

Para obtener más información sobre los usuarios y administradores de Embedded Security, consulte la Ayuda en línea del sistema operativo. Para obtener más información sobre propietarios de Embedded Security, consulte la Ayuda de HP ProtectTools Embedded Security.

Certificados Digitales

Los certificados digitales son una forma de "claves" electrónicas que confirman la identidad de un individuo o empresa. Las claves son números o cadenas de caracteres conocidos sólo por el remitente y/o destinatario. Un certificado digital autentica al propietario del certificado digital proporcionándole una firma digital que se adjunta al mensaje de correo electrónico enviado por el propietario del certificado digital.

Un certificado digital es emitido por la Autoridad de Certificación (CA) y contiene la siguiente información:

- Clave pública de propietario
- Nombre del propietario
- Fecha de vencimiento del certificado digital
- Número de serie del certificado digital
- Nombre de la Autoridad de Certificación (CA) que emitió el certificado digital

- Firma digital de la Autoridad de Certificación (CA) que emitió el certificado digital

Firma Digital

Una firma digital exhibe el nombre de la Autoridad de Certificación (CA) que emite el certificado digital. Se utiliza para:

- verificar la identidad del remitente de un certificado digital.
- certificar que el contenido no sea modificado después de que el remitente haya firmado digitalmente el documento.

Para obtener más información sobre firmas digitales, consulte la Ayuda en línea del sistema operativo.

Clave Pública y Clave Privada

Criptografía Asimétrica, que es un método utilizado por Embedded Security para encriptar información, requiere el uso de dos claves, una clave pública y una clave privada.

Una clave pública puede distribuirse gratuitamente a mucho usuarios, mientras que una clave privada pertenece a un único usuario.

Por ejemplo, para enviar correo electrónico encriptado, el Usuario A puede usar la clave pública (disponible gratuitamente) del Usuario B para encriptar el contenido del correo electrónico enviado por el Usuario B. Dado que sólo el Usuario B tiene la posesión de su propia clave privada, éste es el único que puede desencriptar el contenido del correo electrónico enviado por el Usuario A.

La tecnología de clave pública le permite transmitir información privada en redes públicas, utilizar firmas digitales para asegurar la autenticidad de su correo electrónico y proporciona autenticación entre un servidor y un cliente.

Recuperación de Emergencia

El Archivo de Recuperación de Emergencia, creado por el administrador durante la configuración de Embedded Security, es un archivo que almacena información importante acerca de la computadora, sus usuarios y las claves privadas utilizadas para proteger datos encriptados o privados. En el caso de una falla de sistema, se necesita esta información importante para restaurar el acceso a los datos protegidos.

Una Señal de Recuperación de Emergencia, también creada por el administrador durante la configuración de Embedded Security, es un archivo que almacena las claves utilizadas para proteger los datos en el Archivo de Recuperación de Emergencia. Se necesita la señal para acceder al archivo. El acceso a la Señal de Recuperación de Emergencia está protegido por una contraseña. Se necesita esta contraseña cuando sea necesario restaurar el sistema de Embedded Security.

Criterios

Los Criterios son reglas que rigen el comportamiento de una computadora o software. El administrador del sistema generalmente especifica los criterios de seguridad para garantizar la utilización consistente de Embedded Security dentro de una organización. Los dos tipos de criterios de seguridad son criterios de máquina y de usuario.

Criterios de Máquina

Los criterios de máquina son reglas que rigen el comportamiento general de Embedded Security en la medida en que se relaciona con una computadora específica.

Criterios de Usuario

Los criterios de usuario son reglas que rigen los derechos del usuario de Embedded Security.

Para obtener más información sobre criterios de seguridad de máquina y de usuario, consulte la Ayuda de HP ProtectTools Embedded Security.

Procedimientos de Configuración

Siga estos pasos para activar e inicializar el chip de Embedded Security mediante la utilidad Computer Setup en la BIOS del sistema:

PRECAUCIÓN: Para evitar riesgos contra la seguridad, HP recomienda que una persona autorizada por su organización inicialice inmediatamente el chip de Embedded Security (consulte el paso 4). Si no se inicializa el chip de Embedded Security es posible que el sistema sea dominado por un usuario no autorizado, un gusano o un virus de computadora.

La contraseña del supervisor de la BIOS debe establecerse en Computer Setup antes de poder acceder a las configuraciones del chip. Para obtener más información, consulte la *Guía de la Utilidad Computer Setup (F10)* en el *CD de Documentación* que viene con la computadora.

Activación del Chip

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
2. Apenas se encienda la computadora, presione la tecla **F10** y manténgala presionada hasta que ingrese a Computer Setup.

Si usted no presiona la tecla **F10** en el momento apropiado, deberá reiniciar la computadora y presionar nuevamente la tecla **F10** para tener acceso a la utilidad.

3. Utilice las teclas de flecha para seleccionar **Definir Contraseña de Supervisor** y presione **Intro**.
4. Escriba la contraseña del supervisor y presione **Intro**.
5. Reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
6. Tan pronto como aparezca el comando **Presione cualquier tecla para ingresar la Configuración TPM**, presione una tecla.
7. Ingrese la contraseña del supervisor y presione **Intro**.

8. Presione **E** para activar el chip TPM.

   El chip está ahora activado.

Inicialización del Chip de Embedded Security

En la mayoría de los casos, el Administrador de Sistemas de TI inicializa el chip de Embedded Security.

1. Haga clic con el botón derecho en el icono **HP ProtectTools** en la bandeja del sistema; luego haga clic con el botón izquierdo en **Inicialización de Embedded Security**.

   Aparecerá el **Asistente de Inicialización de HP ProtectTools Embedded Security**.

2. Haga clic en **Siguiente**.
3. Escriba y confirme una contraseña para Tomar Propiedad, luego haga clic en **Siguiente**.

Escriba con cuidado; por razones de seguridad, los caracteres que escriba no aparecerán en pantalla.

4. Haga clic en **Siguiente** para aceptar la ubicación del archivo de Recuperación predeterminado.
5. Escriba y confirme una contraseña para la Señal de Recuperación de Emergencia, luego haga clic en **Siguiente**.
6. Haga clic en **Navegar** y seleccione el destino apropiado.

PRECAUCIÓN: La Clave de Señal de Recuperación de Emergencia se utiliza para recuperar datos encriptados en el caso de falla de una computadora o del chip de embedded security. Los datos no pueden ser recuperados sin la clave. (Tampoco se puede obtener acceso a los datos sin la contraseña de Usuario Básico). Guarde la Clave en un lugar seguro.

7. Haga clic en **Guardar** para aceptar la ubicación y el nombre de archivo predeterminado, luego haga clic en **Siguiente**.
8. Haga clic en **Siguiente** para confirmar la configuración antes de inicializar la Plataforma de Seguridad.

PRECAUCIÓN: Es posible que aparezca un mensaje que diga que los recursos de Embedded Security no se han inicializado. No haga clic en el mensaje; esto se efectuará más tarde en el procedimiento y el mensaje se cerrará después de algunos segundos.

9. Si va a configurar la cuenta de usuario ahora, asegúrese de que esté marcada la casilla de verificación **Iniciar Asistente de Inicialización de Usuario de Embedded Security**. Haga clic en **Finalizar**.

Configuración de Cuenta de Usuario

La configuración de una cuenta de usuario:

- produce una clave de Usuario Básico que protege los datos encriptados
- configura una PSD para almacenar archivos y carpetas encriptados

PRECAUCIÓN: Proteja la contraseña de Usuario Básico. No se puede obtener acceso a los datos encriptados, ni recuperarlos, sin la contraseña.

Para configurar una cuenta de Usuario Básico y activar los recursos de seguridad del usuario:

1. Si no está abierto el **Asistente de inicialización de Usuario de Embedded Security**, haga clic con el botón derecho en el icono de **HP ProtectTools** en la bandeja del sistema, luego haga clic con el botón izquierdo en **Inicialización de Usuario de Embedded Security**.

   Aparecerá el **Asistente de inicialización de Usuario de Embedded Security**.

2. Haga clic en **Siguiente**.
3. Escriba y confirme una contraseña para Clave de Usuario Básico, luego haga clic en **Siguiente**.

Escriba con cuidado; por razones de seguridad, los caracteres que escriba no aparecerán en pantalla.

4. Haga clic en **Siguiente** para confirmar la configuración.
5. Seleccione los Recursos de Seguridad apropiados y haga clic en **Siguiente**.
6. Haga clic en **Siguiente** para omitir archivos de Ayuda.
7. Si existe más de un Certificado de Encriptación, haga clic en el certificado apropiado.

   Haga clic en **Siguiente** para aplicar el Certificado de Encriptación.
8. Configure la PSD con la configuración apropiada y haga clic en **Siguiente**.
9. Configure nuevamente la PSD con la configuración apropiada y haga clic en **Siguiente**.

El tamaño mínimo de la PSD es 50 MB; el tamaño máximo es 2.000 MB.

10. Haga clic en **Siguiente** para confirmar la configuración.

Dependiendo del tamaño de la PSD, la computadora llevará unos minutos para procesar la confirmación.

11. Haga clic en **Finalizar**.
12. Haga clic en **Sí** para reiniciar la computadora.

Tareas Comúnmente Realizadas

Esta sección aborda las tareas básicas que son realizadas más frecuentemente por el usuario y el propietario.

Tareas de Usuario

Las tareas de usuario básico incluyen la configuración de la PSD, la encriptación de archivos y carpetas y el envío y recepción de correo electrónico a través de encriptación y/o firmas digitales.

Uso de la PSD

Para usar la PSD, ingrese su contraseña de PSD. La PSD se torna visible y los archivos se desencriptan. La PSD puede utilizarse como cualquier otra unidad.

Cuando haya terminado de usar la PSD, cierre la sesión de modo apropiado. La PSD automáticamente ocultará su presencia.

Encriptación de Archivos y Carpetas

Al trabajar con EFS en Windows 2000 y Windows XP Professional, tenga en cuenta lo siguiente:

- Sólo se pueden encriptar archivos y carpetas en particiones NTFS. (No se pueden encriptar archivos y carpetas en particiones FAT).
- Los archivos de sistema y los archivos comprimidos no pueden ser encriptados ni los archivos encriptados pueden ser comprimidos.
- Las carpetas temporales deben encriptarse, porque los archivos temporales son potencialmente de interés de atacantes.
- Un criterio de recuperación se configura automáticamente cuando los usuarios encriptan un archivo o carpeta por primera vez. Esto asegura que los usuarios que pierden sus certificados y claves privadas sean capaces de utilizar un agente de recuperación para desencriptar sus datos.

Para encriptar archivos y carpetas:

1. Seleccione el archivo o la carpeta que desea encriptar.
2. Haga clic con el botón derecho del mouse o del Touchpad.
3. Haga clic en **Encriptar**.
4. Haga clic en **Aplicar cambios sólo a esta carpeta** o **Aplicar cambios a esta carpeta, subcarpeta y archivos**.
5. Haga clic en **Aceptar**.

Envío y Recepción de Correo Electrónico por Encriptación y/o Firmas Digitales

Para obtener instrucciones sobre firmas digitales y encriptación de correo electrónico, consulte la Ayuda en línea de cliente de correo electrónico.

Para utilizar correo electrónico seguro, primero debe configurar el cliente de correo electrónico para utilizar un certificado digital creado con Embedded Security. Si no está disponible un certificado digital, debe obtener uno de la Autoridad de Certificación (CA). Para obtener instrucciones sobre la configuración de correo electrónico y la obtención de certificados digitales, consulte la Ayuda en línea de cliente de correo electrónico.

Para enviar un mensaje de correo electrónico encriptado, necesitará una copia de la clave pública del destinatario o del certificado de encriptación. (El certificado contiene una copia de la clave pública del destinatario.)

Microsoft Outlook usa la clave pública del destinatario para encriptar su correo electrónico; por lo tanto no se le solicitará que inserte su clave privada. Sin embargo, sí necesitará la clave privada para leer un mensaje de correo electrónico encriptado porque la desencriptación requiere la clave privada que corresponde a la clave pública utilizada para encriptar el mensaje.

Tareas del Administrador

El administrador puede realizar varias tareas, algunas de las cuales se describen a continuación. Para obtener más información, consulte la Ayuda de HP ProtectTools Embedded Security.

Claves de Migración a través del Asistente de Migración de Seguridad de la Computadora

La migración es una tarea avanzada del administrador que permite la administración, restauración y transferencia de claves y certificados.

El primer paso para la migración es la autorización, configuración y administración del proceso de migración. Una vez terminada la autorización, el usuario exporta e importa claves y certificados desde la computadora de origen a la computadora de destino.

Para obtener detalles sobre la migración, consulte la Ayuda de HP ProtectTools Embedded Security.

Información de Recuperación

En el caso de fallas en el chip o reinicio:

- El Asistente de Restauración de Emergencia se puede utilizar para recuperar datos desde la PSD.
- La PSD también admite recuperación a través de la utilización de un agente de recuperación, que es un mecanismo similar a los Sistemas de Archivos Encriptados (EFS).

  Para determinar si tiene un agente de recuperación registrado en la computadora, haga clic en **Inicio > Todos los Programas > Herramientas del Administrador > Criterio de Seguridad Local > Criterios de Claves Públicas > Agentes de Recuperación de Datos Encriptados**.

Para obtener más información, consulte la Ayuda en línea del sistema operativo.

Windows XP Professional no crea automáticamente un agente de recuperación registrado. Siga las instrucciones del sistema operativo para configurar el agente de recuperación registrado.

Para recuperar datos, el agente de recuperación registrado debe tener el certificado digital y las claves. Debe exportar el certificado de recuperación de datos y la clave privada al disco, almacenarlos en un lugar seguro y eliminar la clave privada de recuperación de datos de la computadora. La única persona que puede recuperar los datos es la persona que tiene físicamente acceso a la clave privada de recuperación de datos.

Restauración del Chip de Embedded Security a los valores predeterminados de fábrica a través de Computer Setup

PRECAUCIÓN: Esta tarea libera propiedad del chip de Embedded Security. Una vez que la propiedad es liberada, todos pueden inicializar el chip de Embedded Security.

La restauración del chip Embedded Security a los valores predeterminados de fábrica puede provocar la pérdida de datos si tiene archivos encriptados.

Para retornar al chip de Embedded Security a su configuración original de fábrica:

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
2. Tan pronto como aparezca el comando **Presione cualquier tecla para ingresar la Configuración TPM**, presione una tecla.
3. Ingrese la contraseña del supervisor y presione **Intro**.
4. Presione **C** para borrar el chip TPM.
5. Presione **S** para confirmar.

   El chip está ahora borrado.

Mejores Prácticas

HP recomienda seguir las siguientes pautas al utilizar Embedded Security.

- Un administrador de seguridad de TI debe configurar la contraseña del supervisor de la BIOS en Computer Setup e inicializar el chip de Embedded Security antes de distribuir la computadora a los usuarios.
- El administrador de seguridad de TI debe configurar el Archivo de Recuperación de Emergencia durante el proceso de configuración de la solución Embedded Security e incentivar para que los usuarios guarden y hagan copias de seguridad de los datos regularmente. En caso de falla del sistema, ésta es la única forma de recuperar los datos encriptados. El Archivo de Recuperación de Emergencia y la Señal de Recuperación de Emergencia deben ser almacenados por separado.
- Encripte carpetas en lugar de archivos individuales de modo que los archivos temporales que se creen durante la edición también sean encriptados.
- Encripte datos confidenciales en computadoras que sean miembros de un dominio. Esto protege contra el riesgo a los datos a través de ataques criptográficos cuando se está fuera de línea.
- Haga copias de seguridad periódicamente de todo el servidor que almacena los datos encriptados con base en el servidor. Esto garantiza que en el caso de recuperación de datos, los perfiles que incluyen las claves de desencriptación puedan también ser restaurados.
- Si va a encriptar tipos de archivos que sean monitoreados por la Restauración de Sistema, coloque los archivos en un volumen que no sea monitoreado por la Restauración del Sistema.
- El sistema no admite múltiples niveles de encriptación. Por ejemplo, el usuario no debe almacenar un archivo encriptado EFS en la PSD, ni intentar encriptar un archivo ya almacenado en la PSD.

Preguntas Más Frecuentes

¿Cómo sé que mi computadora tiene un chip de HP ProtectTools Embedded Security?

El chip es un componente de hardware construido en el sistema. El componente será listado en el Administrador de Dispositivos.

¿Cómo obtengo el software HP ProtectTools Embedded Security?

Descargue el software, los controladores y la Ayuda en línea visitando el sitio web de HP en http://www.hp.com/products/security.

¿Puede el software HP ProtectTools Embedded Security ser desinstalado? ¿Cómo?

Sí. El software se desinstala utilizando el proceso estándar de desinstalación del software Windows. Antes de desinstalar, se debe guardar los datos protegidos específicos del usuario. Sin guardarlos, los datos se perderán. El paso final de la desinstalación es la desactivación del chip.

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
2. Tan pronto como aparezca el comando **Presione cualquier tecla para ingresar la Configuración TPM**, presione una tecla.
3. Ingrese la contraseña del supervisor y presione **Intro**.
4. Presione **D** para desactivar el chip TPM.

   El chip está ahora desactivado.

Solución de Problemas

Mi Embedded Security no está funcionando. ¿Qué debo hacer?

1. Haga clic con el botón derecho en el icono **HP ProtectTools** en la bandeja del sistema; luego haga clic con el botón izquierdo en **Administrar Embedded Security**.
2. Haga clic en **Embedded Security > Información > Prueba Automática**.

También marque debajo de **Estado, Chip, Propietario y Usuario de Embedded Security**.

He restaurado mi sistema después de una falla general. ¿Qué debo hacer ahora?

PRECAUCIÓN: En la mayoría de los casos, el Administrador del Sistema de TI realiza este procedimiento. Se puede producir la pérdida de datos permanente, si el procedimiento no se realiza apropiadamente.

Para recuperar los datos después del reemplazo del chip de ProtectTools, debe tener lo siguiente:

- SPEmRecToken.xml-Clave de Señal de Recuperación de Emergencia
- SPEmRecArchive.xml-carpeta oculta, ubicación predeterminada: C:\Documents and Settings\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- Contraseñas de ProtectTools
  - Supervisor
  - Tomar Propiedad
  - Señal de Recuperación de Emergencia
  - Usuario Básico

1. Encienda o reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
2. Tan pronto como aparezca el indicador de comando **Presione cualquier tecla para ingresar la Configuración TPM**, presione una tecla.

3. Ingrese la contraseña del supervisor y presione **Intro**.
4. Presione **C** para borrar el chip TPM.
5. Presione **S** para confirmar.
6. Reinicie la computadora. Si está en Microsoft Windows, haga clic en **Inicio > Apagar > Reiniciar**.
7. Tan pronto como aparezca el comando **Presione cualquier tecla para ingresar la Configuración TPM**, presione una tecla.
8. Ingrese la contraseña del supervisor y presione **Intro**.
9. Presione **E** para activar el chip TPM.

   El chip está ahora activado.
10. Después de abrir Windows, haga clic con el botón derecho en el icono **HP ProtectTools Embedded Security** en la bandeja del sistema; luego haga clic con el botón izquierdo en **Inicialización de Embedded Security**.
11. Seleccione la casilla de verificación: **Deseo restaurar Embedded Security existente**, luego haga clic en **Siguiente**.
12. Escriba y confirme la contraseña original de Tomar Propiedad. Haga clic en **Siguiente**.
13. Haga clic en **No crear un archivo de recuperación**, luego haga clic en **Siguiente**.

PRECAUCIÓN: La creación de un nuevo archivo produce la pérdida total de datos al sobreescribir el archivo requerido para su restauración.

14. Haga clic en **Sí** para proceder sin crear un archivo de recuperación.
15. Haga clic en **Siguiente** para confirmar la configuración.
16. Haga clic en **Navegar** y ubique el archivo de emergencia; la ubicación predeterminada es: C:\Documents and Settings\ All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml.
17. Haga clic en **Abrir** y en **Siguiente**.

18. Haga click **Navegar** y ubique la señal de Recuperación creada durante la primera **Inicialización de HP ProtectTools Embedded Security**, haga clic en la señal y luego en **Abrir**.
19. Ingrese la contraseña de Señal y haga clic en **Siguiente**.
20. Seleccione el nombre de la máquina y haga clic en **Siguiente**.
21. Haga clic en **Siguiente** para confirmar la configuración.

    Si aparece un anuncio que indica fallas en la restauración, retorne al paso 1. Revise cuidadosamente las contraseñas, la ubicación y el nombre de la señal y la ubicación y nombre del archivo.
22. Si la cuenta de usuario se va a configurar ahora, asegúrese de haber seleccionado la casilla de verficación **Iniciar Asistente de Inicialización de Usuario de Embedded Security**. Haga clic en **Finalizar**.

Pasos 23 para 35 la restauración de Claves de Usuario Básico. Estos pasos deben repetirse para cada usuario.

23. Si no está abierto el **Asistente de inicialización de Usuario de Embedded Security**, haga clic con el botón derecho en el icono de **HP ProtectTools Embedded Security** en la bandeja del sistema, luego haga clic con el botón izquierdo en **Restaurar Recursos de Embedded Security**.

    Aparecerá el **Asistente de Inicialización de Usuario de Embedded Security**.
24. Haga clic en **Siguiente**.
25. Haga clic en **Recuperar clave de usuario básico** y haga clic en **Siguiente**.
26. Seleccione un usuario, escriba la contraseña original de la Clave de Usuario Básico para ese usuario, luego haga clic en **Siguiente**.
27. Haga clic en **Siguiente** para confirmar la configuración y aceptar la ubicación del archivo de recuperación predeterminado.
28. Seleccione los Recursos de Seguridad apropiados y haga clic en **Siguiente**.
29. Haga clic en **Siguiente** para omitir archivos de ayuda.

30. Si existe más de un Certificado de Encriptación, haga clic en el certificado apropiado.

    Haga clic en **Siguiente** para aplicar el Certificado de Encriptación.

31. Haga clic en **Deseo cambiar la configuración de mi Personal Secure Drive** donde sea apropiado y haga clic en **Siguiente**.
32. Confirme los Recursos de Seguridad y haga clic en **Siguiente**.
33. Confirme la Configuración y haga clic en **Siguiente**.
34. Ingrese la contraseña de PSD y haga clic en **Aceptar**.
35. Haga clic en **Finalizar** y **Sí** para reiniciar.

PRECAUCIÓN: Protege la contraseña de Usuario Básico. No se puede obtener acceso a los datos encriptados, ni recuperarlos, sin la contraseña.

Glosario

Autoridad de Certificación (CA)—servicio que emite los certificados requeridos para ejecutar una infraestructura de claves públicas.

Criptografía—práctica y estudio de encriptación y desencriptación; codificación de datos, de modo que sólo puedan ser decodificados por individuos específicos. El sistema para encriptar y desencriptar datos es un criptosistema. Estos usualmente contienen un algoritmo que combina los datos originales ("texto común") con uno o más números "clave" o cadenas de caracteres conocidas sólo por el remitente y/o destinatario. El producto resultante es conocido como "texto cifrado."

Proveedor de Servicio Criptográfico (CSP)—proveedor o biblioteca de algoritmos criptográficos que pueden usarse en una interfaz bien definida para realizar funciones criptográficas particulares.

Desencriptación—cualquier procedimiento usado en criptografía para convertir texto cifrado (datos encriptados) en texto común.

Certificados Digitales—credenciales electrónicas que confirman la identidad de un individuo o una compañía al vincular la identidad del propietario del certificado digital a un par de claves electrónicas que se utilizan para firmar información digital.

Firma Digital—recurso utilizado para verificar la identidad del remitente de un documento digital y certificar que el contenido no sea modificado después de que el remitente haya firmado el documento.

Archivo de Recuperación de Emergencia—el archivo es un área de almacenamiento protegido que permite la reencriptación de claves de usuario básico de una clave de propietario de plataforma a otra.

Encriptación—por ejemplo, algoritmo, criptografía; cualquier procedimiento utilizado en criptografía para convertir texto común en texto cifrado con el fin de evitar que destinatarios no autorizados lean esos datos. Existen muchos tipos de encriptación de datos y éstos son la base de la seguridad de la red. Los tipos comunes incluyen Estándar de Encriptación de Datos y encriptación de claves públicas.

Sistema de Archivos de Encriptados (EFS)—sistema que encripta todos los archivos y subcarpetas dentro de la carpeta seleccionada.

Migración—tarea que permite la administración, restauración y transferencia de claves y certificados.

Personal Secure Drive - PSD—proporciona un área de almacenamiento protegida para datos confidenciales.

Infraestructura de Claves Públicas (PKI)—estándar que define las interfaces para la creación, utilización y administración de certificados y claves criptográficas.

Módulo de Plataforma Confiable - TPM)—proporciona seguridad de los datos a nivel de hardware. Integrado en el sistema, el chip de Embedded Security puede revisar la integridad del sistema y autenticar usuarios de terceros que accedan a la plataforma, mientras continúan bajo completo control de su usuario primario.