

# SOPHOS

## SafeGuard Enterprise® 5.50

### Ayuda del usuario

Fecha del documento: Agosto 2010



# Contenido

1	SafeGuard Enterprise en los PC de los usuarios .....	2
2	POA (power-on authentication).....	4
3	POA (power-on authentication) en Windows Vista .....	25
4	Conexión a Windows Vista .....	37
5	Autenticación con el Lector de huellas digitales de Lenovo.....	39
6	Opciones de recuperación.....	48
7	Recuperación mediante Local Self Help .....	49
8	Recuperación mediante el procedimiento de desafío/respuesta .....	59
9	Icono de la bandeja del sistema e información sobre herramientas .....	70
10	Extensiones del explorador de SafeGuard .....	73
11	Cifrado de datos .....	76
12	SafeGuard Data Exchange.....	82
13	SafeGuard Configuration Protection .....	99
14	SafeGuard Enterprise y BitLocker .....	100
15	SafeGuard Enterprise y Lenovo Rescue and Recovery .....	103
16	Soporte técnico .....	111
17	Copyright .....	112

# 1 SafeGuard Enterprise en los PC de los usuarios

SafeGuard Enterprise es un conjunto modular de aplicaciones de seguridad que proporciona seguridad a los PC y dispositivos portátiles a través de directivas de seguridad que un administrador define y se aplican sobre varias plataformas. SafeGuard Enterprise es fácil de usar. La administración del sistema se realiza centralmente a través de SafeGuard Management Center.

Las funciones de protección centrales de SafeGuard Enterprise en un PC/portátil (cliente) de usuario son el cifrado de datos y la protección contra el acceso no autorizado al equipo a través de cualquier medio externo.

## 1.1 Módulos de SafeGuard Enterprise

### ■ SafeGuard Enterprise Cifrado para dispositivos

- POA (power-on authentication)
- El inicio de sesión del usuario se realiza inmediatamente después de encender el ordenador. Una vez que la POA (power-on authentication) se ha realizado correctamente, se conectará automáticamente al sistema operativo. También puede desactivar la POA, en cuyo caso, la autenticación del usuario se realiza a través del sistema operativo.
- Cifrado basado en volúmenes
- Compatibilidad con BitLocker

### ■ SafeGuard Data Exchange

- Intercambio de datos sencillo con medios extraíbles en todas las plataformas, sin tener que volver a cifrar.
- Cifrado basado en archivos
- Todos los medios grabables móviles, entre los que se incluyen los discos duros externos y los lápices de memoria, se cifran de forma transparente.

### ■ SafeGuard Configuration Protection

Con SafeGuard Configuration Protection, sólo puede permitir ciertas interfaces o dispositivos periféricos en determinados equipos. Esto evita que se introduzca código malicioso así como la exportación de datos a través de canales no deseados como WLAN. Este módulo también puede detectar y bloquear hardware dañino, como registradores de claves.

**Nota:** Tenga en cuenta que las características disponibles en su equipo dependen de la configuración definida en el SafeGuard Management Center. El responsable de seguridad especifica centralmente esta configuración en el SafeGuard Management Center mediante directivas y las distribuye a los equipos de los usuarios. Por consiguiente, es posible que no todas las características que se describen en este manual estén disponibles en su equipo.

## 2 POA (power-on authentication)

Con POA (power-on authentication), los usuarios tienen que autenticarse en la fase previa al arranque del equipo, es decir, antes de que se inicie el sistema operativo del PC. Cuando el usuario se haya autenticado correctamente en la POA, el sistema operativo real (Windows) se inicia y el usuario se conecta automáticamente a Windows. El procedimiento es el mismo cuando el equipo se vuelve a activar tras estar en hibernación (Suspendir en disco).



### 2.1 Aspecto visual y operativo de POA

El aspecto visual y operativo de la POA (power-on authentication) se puede personalizar de acuerdo con las necesidades de la empresa en cuestión. El responsable de seguridad de SafeGuard Enterprise realizará los ajustes correspondientes a través de la configuración de directivas de SafeGuard Management Center.

Se pueden realizar los siguientes ajustes:

- **Imagen de la conexión**

La imagen predeterminada de la conexión que aparece en la POA es un diseño de SafeGuard. Se puede personalizar esta pantalla mediante una directiva, lo que hace posible mostrar una imagen gráfica, como el logotipo de su empresa.

- **Texto de los cuadros de diálogo**

Todo el texto que se muestra en POA aparece en el idioma predeterminado que esté configurado en la Configuración regional y de idioma de Windows del equipo del usuario al instalar SafeGuard Enterprise.

Puede establecer cuál es el idioma predeterminado si selecciona **Inicio > Configuración > Panel de control > Configuración regional y de idioma > Opciones avanzadas**. Por ejemplo, si el valor predeterminado es "Alemán", el texto de todos los cuadros de diálogo de la POA aparecerá en alemán.

## 2.2 Primera conexión después de la instalación de SafeGuard Enterprise

Si se ha instalado SafeGuard Enterprise con POA (power-on authentication), el procedimiento de arranque es diferente durante el primer inicio del sistema tras haber instalado SafeGuard Enterprise en un equipo. Aparecen una serie de nuevos mensajes de inicio (como por ejemplo, la pantalla de conexión automática), debido a que SafeGuard Enterprise se ha incorporado al procedimiento de arranque del sistema. Después, se iniciará el sistema operativo Windows.

SafeGuard Enterprise utiliza credenciales basadas en certificados para conectarse. Los usuarios necesitan claves y certificados para conectarse correctamente a la POA (power-on authentication). Sin embargo, las claves y los certificados específicos del usuario sólo se crean después de conectarse correctamente a Windows. Únicamente los usuarios que se hayan conectado correctamente y accedido a Windows en un sistema que sea capaz de comunicarse con el servidor SGN se podrán autenticar también en la POA.

Por consiguiente, la primera vez que se conecte a Windows después de la instalación, primero debe acceder a Windows de la manera habitual. Posteriormente, se le registrará como usuario de SafeGuard Enterprise. Este proceso de registro es necesario para asegurarse de que la POA reconozca sus credenciales la próxima vez que el sistema se inicie.

**Nota:** Tras registrarse correctamente y recibir todos los datos necesarios, aparecerá una información sobre herramientas en el equipo que lo confirmará.

Cuando reinicie el equipo, se activará la POA. A partir de ese momento, debe especificar sus credenciales de Windows en la POA, tras lo que se conectará a Windows automáticamente sin tener que escribir ninguna contraseña (si está activada la conexión automática a Windows).

Puede conectarse a la POA (power-on authentication) a través de:

- nombre de usuario y contraseña
- token/tarjeta inteligente y PIN

Para ver los últimos dispositivos disponibles, consulte el archivo léame.

**Nota:** La configuración de los equipos de los usuarios en los que está instalado SafeGuard Enterprise la define el security officer de SafeGuard Enterprise y se distribuye a los usuarios a través de archivos de directivas.

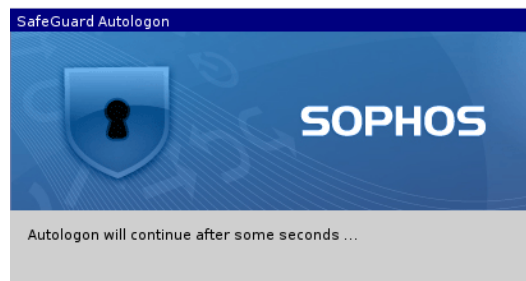
### 2.2.1 Procedimiento para la primera conexión

El procedimiento de la primera conexión sólo corresponderá al descrito aquí si la POA se ha instalado y activado en su equipo.

Según sea la configuración del sistema, se le pedirá que pulse **Ctrl+Alt+Supr.** Hecho esto, el procedimiento de conexión seguirá su curso.

### 2.2.2 Conexión automática a SafeGuard

Arranca el equipo y aparece la conexión automática a SafeGuard Enterprise.



#### ¿Qué sucede?

1. Hay un usuario automático conectado.
2. El equipo se registra automáticamente en el servidor de SafeGuard Enterprise, siempre que exista alguna conexión con éste.
3. La clave del equipo se envía al servidor de SafeGuard Enterprise y se almacena en la base de datos de SafeGuard Enterprise.
4. Las directivas de equipo se enviarán al ordenador.

### 2.2.3 Conexión a Windows

Aparecerá el cuadro de diálogo de conexión de Windows.

Especifique sus credenciales de usuario de Windows de la forma habitual.

**Nota:** Si está usando una **tarjeta inteligente** o un **token**, indique el PIN.

#### ¿Qué sucede?

1. Se enviarán al servidor el Id. de usuario y un hash de las credenciales del usuario.
2. Las directivas, los certificados y las claves del usuario se crearán y se enviarán al equipo de dicho usuario.

Los datos de usuario sólo estarán disponibles en la POA (power-on authentication) después de que todos los datos de usuario mencionados anteriormente se hayan sincronizado correctamente entre el servidor de SafeGuard Enterprise y el equipo del usuario.

**Nota:** Tras registrarse correctamente y recibir todos los datos necesarios, aparecerá una información sobre herramientas en el equipo que confirmará el proceso.

Lo que significa que la próxima vez que se inicie el sistema, sólo tiene que especificar sus credenciales de Windows (nombre de usuario y contraseña) en POA y se conectará automáticamente.

Para activar la POA, es necesario reiniciar el sistema. Tras el reinicio, la POA protege el ordenador contra el acceso no autorizado.

### 2.2.4 Conexión a la POA (power-on authentication) tras el reinicio

Tras reiniciar el ordenador, aparece el cuadro de diálogo de conexión de POA.



**Introduzca su nombre de usuario y contraseña.**

**¿Qué sucede?**

1. Se evaluarán sus credenciales. Tanto los certificados como las claves se ponen a disposición y se conectará automáticamente a Windows.

La conexión automática a Windows se puede desactivar mediante la configuración de una directiva. En tal caso, se mostrará el cuadro de diálogo de conexión a Windows y tendrá que especificar sus credenciales.

## 2.3 Conexión en la POA (power-on authentication)

Tras la correcta activación de la POA, se conecta especificando sus credenciales de usuario de Windows en el cuadro de diálogo de conexión de POA. Se conectará a Windows automáticamente.

**Nota:** Puede desactivar la conexión automática a Windows pulsando el botón **Opciones >>** en el cuadro de diálogo de conexión y desactivando la opción **Conexión automática a Windows**.

**Nota:** Por ejemplo, es necesario desactivar la conexión automática para permitir que otros usuarios utilicen la POA en el equipo pertinente (véase [Importación de otros usuarios](#), página 10).

### 2.3.1 Retraso en la conexión al producirse un error en el intento de conexión

Si se produce un error en la conexión de la POA, por ejemplo, a causa de una contraseña incorrecta, se mostrará un mensaje de error y se impondrá un retraso en el próximo intento de conexión. El período de retraso aumentará cada vez que tenga lugar un intento de conexión fallido. Los intentos de conexión fallidos quedan registrados.

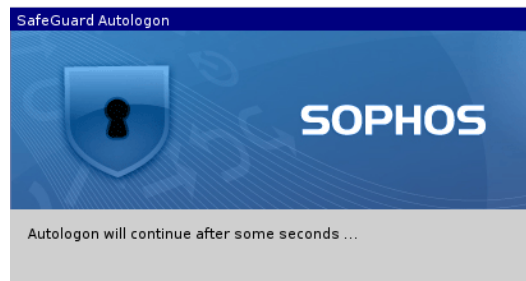
### 2.3.2 Bloqueo del equipo

De acuerdo con la configuración de directivas, es posible que su equipo quede bloqueado tras un número predeterminado de intentos de conexión fallidos. Para desbloquearlo, inicie un procedimiento de desafío/respuesta, véase [Recuperación mediante el procedimiento de desafío/respuesta](#), página 59.

### 2.3.3 Ejemplo de conexión de usuario a la POA

1. Usuario 1 (Alice) enciende el cliente XP.

Aparece el cuadro de diálogo Conexión automática en POA.



2. Aparece el cuadro de diálogo de conexión de Windows. Alice se conecta a Windows.

A partir de este momento, Alice recibe el nombre de "propietario". Hay un propietario por PC. En la configuración predeterminada, el primer usuario que se conecta es el propietario.

3. Si tanto las directivas del usuario como su certificado y su clave están en el cliente, se crea una entrada para Alice en el núcleo del sistema de SafeGuard Enterprise.

4. Cuando el equipo se haya reiniciado, Alice puede conectarse a la POA.



**Nota:** Si se aplica la configuración predeterminada, el primer usuario en conectarse a Windows se registrará automáticamente como "propietario" de este equipo. Dependiendo de la directiva, el propietario de un ordenador es el único que puede permitir a otros usuarios conectarse en la POA. En nuestro ejemplo, Alice es la única que puede conectarse en la POA.

**Nota:** Si otros usuarios pretenden conectarse a la POA, el propietario del equipo tiene que habilitarlos (véase [Importación de otros usuarios](#), página 10).

**Nota:** El security officer define en las directivas relevantes si la conexión automática a Windows se activa o se desactiva, y si se le permite que usted cambie dicha configuración en el cuadro de diálogo de conexión.

## 2.4 Importación de otros usuarios

Además de Alice, hay otro usuario de Windows (Bob) que desea conectarse al equipo.

1. Bob enciende el ordenador y aparece la POA.

Bob no puede conectarse en la POA, ya que no tiene las claves y los certificados necesarios.

2. Para que pueda conectarse en la POA, el propietario del equipo (Alice en este caso) debe darle permiso.

La configuración predeterminada estipula que el primer usuario que se conecte después de la instalación se registrará como el propietario del equipo.

**Nota:** El security officer también puede definir el propietario de un ordenador a través de una configuración de directiva.

3. Antes de conectarse en la POA, Alice desactiva la **Conexión automática a Windows**.

Aparece el cuadro de diálogo de conexión a Windows, que le solicita a Bob que se conecte.

4. Bob introduce sus credenciales de Windows.

5. Si tanto las directivas de Bob como su certificado y su clave están disponibles en el equipo (como resulta evidente por la información de las herramientas con forma de globo), se crea una entrada para Bob en el núcleo del sistema de SafeGuard Enterprise.

La próxima vez que se inicie el equipo, Bob podrá conectarse en la POA.

**Nota:** Si los usuarios ya se han conectado a través de la POA en otro ordenador del mismo entorno, un responsable de seguridad puede utilizar el Management Center para asignar usuarios a la POA de un equipo nuevo. Los usuarios asignados de esta forma también se pueden conectar en estos equipos en la POA.

## 2.5 Contraseña temporal de la POA

SafeGuard Enterprise le permite cambiar temporalmente la contraseña en la POA. Puede ser aconsejable cambiar la contraseña de la POA temporalmente si sospecha que alguien ha observado cómo escribía su contraseña.

**Ejemplo:** ha iniciado su portátil en un lugar público, por ejemplo, en el aeropuerto. Cree que alguien le ha visto escribir su contraseña en la POA. Como no está conectado a Active Directory (AD), no puede cambiar su contraseña de Windows.

**Solución:** puede cambiar temporalmente la contraseña de la POA, asegurándose así que ninguna persona sin autorización conozca su contraseña. Tan pronto como se conecte de nuevo a AD, se le pedirá automáticamente que cambie la contraseña temporal.

Para cambiar la contraseña de la POA temporalmente:

1. En el cuadro de diálogo de conexión de POA, escriba la contraseña ya existente.
2. Pulse **F8**.

Si no especifica la contraseña existente antes de pulsar **F8**, el sistema lo interpreta como una conexión fallida y muestra un mensaje de error.

3. En el cuadro de diálogo, escriba la contraseña nueva y confirmela.

El sistema le recordará que el cambio de contraseña es sólo temporal.

4. Haga clic en **Aceptar**.

Si cancela este diálogo, se conectará con su contraseña anterior.

Aparecerá el cuadro de diálogo de conexión de Windows.

**Nota:** La conexión no se pasará automáticamente a Windows, aunque el sistema esté configurado de esta forma. Escriba aquí la "contraseña anterior". La contraseña temporal sólo es válida para conectarse en la POA.

5. Haga clic en **Aceptar**.

Ya está conectado a Windows.

Para conectarse en la POA, ahora sólo puede usar la contraseña definida temporalmente. La contraseña temporal será válida hasta que la contraseña se cambie en la conexión a Windows. Sólo después de hacer esto se podrá pasar la conexión desde POA a Windows de nuevo.

### **Cambio de la contraseña temporal**

La contraseña cambiada temporalmente en la POA tiene que volver a cambiarse después, para que las contraseñas vuelvan a estar sincronizadas.

Cuando se conecte a Windows, SafeGuard Enterprise le indicará que cambie automáticamente la contraseña tan pronto como esté conectado de nuevo a Active Directory.

El cuadro de diálogo que le indica que cambie la contraseña puede cancelarse sin cambiar realmente la contraseña. En este caso, el cuadro de diálogo se mostrará cada vez que se conecte hasta que la cambie.

**Nota:** La contraseña de la POA se puede cambiar también temporalmente mientras esté conectado a Active Directory. En este caso, el cuadro de diálogo para cambiar la contraseña se mostrará inmediatamente después de cambiar la contraseña temporalmente de la POA. Sin embargo, puede cancelarse y la "contraseña anterior" se podrá usar para conectarse. Después, podrá cambiar la contraseña.

## **2.6 Conexión en la POA (power-on authentication) utilizando tarjetas inteligentes o tokens**

Hay dos tipos posibles de conexión utilizando tarjetas inteligentes o tokens:

- La conexión sólo se permite utilizando tarjetas inteligentes o tokens.
- La conexión se permite a través del nombre de usuario y la contraseña o a través de la tarjeta inteligente o token.

El security officer define el tipo de conexión permitido centralmente a través de una directiva.

El responsable de seguridad generará su tarjeta inteligente/token y se la dará, o bien usted mismo incluirá sus credenciales de usuario de Windows en su tarjeta inteligente/token.

**Nota:** Desde la perspectiva de SafeGuard Enterprise, las tarjetas inteligentes y los tokens se tratan de la misma forma. Por tanto, los términos "token" y "tarjeta inteligente" se consideran sinónimos tanto en el producto como en el manual.

**Nota:** Las siguientes secciones utilizan el término "token".

### 2.6.1 Primera conexión con token después de la instalación

El procedimiento que se utiliza para realizar la primera conexión con un token es el mismo que el que se ha descrito para conectarse sin él.

Si hay disponible un token generado, puede utilizarlo para conectarse a Windows mediante el número PIN del mismo.

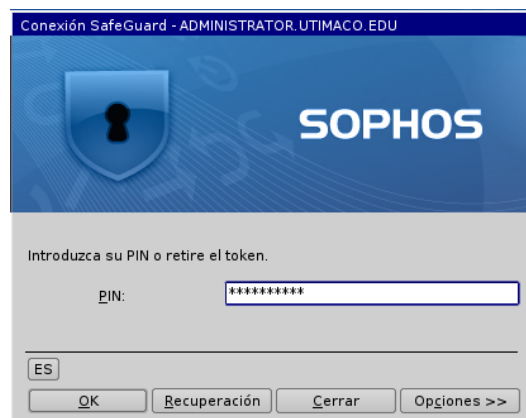
**Nota:** Se recomienda que configure su token con las credenciales de Windows (véase [Almacenamiento de la información de usuario de Windows en el token](#), página 15) antes de reiniciar el equipo. Las directivas de seguridad que se le aplican pueden exigir que utilice un token en la POA. Si el token no contiene información de usuario, no podrá conectarse en la POA.

### 2.6.2 Conexión en la POA con token

Asegúrese de que en la BIOS esté activada la compatibilidad con USB. Debe inicializarse la compatibilidad con el token para que se pueda generar.

Cómo conectarse en la POA con un token:

1. Conecte el token.
2. Encienda el equipo y espere hasta que aparezca el cuadro de diálogo para la conexión con el token.



**Nota:** Si la directiva le permite conectarse con sus credenciales de usuario y desconecta el token, se le pedirá que especifique sus credenciales de usuario para conectarse. Si el cuadro de diálogo para conectarse utilizando el Id. de usuario y la contraseña no aparece, solamente puede conectarse utilizando un token en la POA.

3. Especifique el número PIN del token.

Está conectado a la POA y a Windows (si la opción **Conexión automática a Windows** está activada en el cuadro de diálogo de conexión).

### 2.6.3 Cambio de número PIN

El número PIN del token se puede cambiar cuando aparece el cuadro de diálogo de conexión de Windows.

Si la opción **Conexión automática a Windows** está activada en la POA (power-on authentication), generalmente no se mostrará el cuadro de diálogo de conexión de Windows. Para que se muestre el cuadro de diálogo de conexión a Windows, tendrá que desactivar esta opción durante la conexión en la POA.

**Nota:** Si el security officer ha definido reglas que requieran un cambio de número PIN (por ejemplo, a intervalos de tiempo concretos), se le solicitará automáticamente que cambie el número PIN.

Cómo cambiar el número PIN del token:

1. En el cuadro de diálogo PIN que se emplea para conectarse a Windows, active la opción **Cambiar PIN**.



2. Especifique el número PIN del token y haga clic en **Aceptar**.

Aparecerá el cuadro de diálogo Cambiar PIN.



3. Especifique el número PIN nuevo y confírmelo.

4. Haga clic en **Aceptar**.

El número PIN del token se cambia y continúa la conexión a Windows.

#### 2.6.4 Almacenamiento de la información de usuario de Windows en el token

Si el token no tiene almacenada información de usuario de Windows, puede incluirla usted mismo.

**Nota:** Le recomendamos que configure su token durante la primera conexión.

**Nota:** Las directivas de seguridad que se le aplican pueden exigir que utilice un token en la POA. Si el token no contiene información de usuario, no podrá conectarse en la POA.

1. Durante la primera conexión después de la instalación, conecte el token al sistema cuando aparezca el cuadro de diálogo de conexión de Windows.
2. Si el sistema detecta un token vacío, mostrará automáticamente el cuadro de diálogo para generar tokens.



3. Introduzca su nombre de usuario de Windows y la contraseña.
4. Confirme la contraseña.
5. Seleccione o especifique el dominio y haga clic en **Aceptar**.

El sistema intentará conectarle a Windows utilizando los datos especificados. Si la conexión es correcta, los datos se escriben en el token.

Ya está conectado a Windows.

Si la conexión al token se define como opcional para el usuario (ya se ha conectado una vez en la POA con su nombre de usuario y contraseña), también puede generar posteriormente el token.

Para hacerlo, desactive la opción **Conexión automática a Windows (Opciones > Conexión automática a Windows)** en el cuadro de diálogo de conexión de la POA. Se mostrará el cuadro de diálogo de conexión de Windows y podrá almacenar los datos en el token como se ha descrito anteriormente.

## 2.6.5 Desbloqueo de tarjetas inteligentes o tokens

Si ha introducido su número PIN incorrectamente varias veces, el token se bloqueará. El security officer puede configurar SafeGuard Enterprise para que aparezca el cuadro de diálogo para desbloquear tokens bloqueados:



Para desbloquear el token, el security officer tiene que proporcionarle el número PIN del administrador definido para su token.

Siga estos pasos:

1. Especifique el número PIN del administrador.
2. Especifique un número PIN nuevo y confírmelo.

El número PIN que especifique estará sujeto a las reglas definidas para los números PIN (por ejemplo, es posible que se necesiten combinaciones de caracteres concretos, se puede prohibir que se vuelvan a utilizar los números PIN ya utilizados, etc).

3. Haga clic en **Aceptar**.

El token se desbloqueará y continuará el proceso de conexión.

**Nota:** Si esta función no está disponible en el equipo, puede volver a acceder al mismo a través de un procedimiento de desafío/respuesta.

**Nota:** A través del procedimiento de desafío/respuesta, puede volver a obtener acceso a su equipo. Sin embargo, no puede cambiar el PIN o sus credenciales de usuario mediante dicho procedimiento.

### 2.6.6 Conexión a Escritorio remoto

En Windows XP no es posible establecer una conexión a Escritorio remoto con un equipo si el usuario se ha conectado de forma local con un token.

La captura remota no es posible en este caso.

### 2.6.7 Tokens criptográficos - Kerberos

Cuando se usen tokens criptográficos, la autenticación en la POA se realizará mediante el certificado almacenado en el token.

Para este tipo de conexión, necesita un token completamente generado para su autenticación. El security officer o cualquier otra persona autorizada tiene que proporcionarle este token. Para conectarse al sistema, sólo tiene que especificar el PIN del token. Si este tipo de conexión es el único tipo válido para su equipo, no puede conectarse sin el token.

**Nota:** Al utilizar un token de este tipo, el procedimiento de desafío/respuesta no estará disponible en caso de problemas de conexión. Si surgen problemas de conexión, póngase en contacto con el security officer.

## 2.7 Conexión automática a POA con tarjeta inteligente o token

**Requisito previo:** Asegúrese de que en la BIOS esté activada la compatibilidad con USB. Debe inicializarse la compatibilidad con el token para que se pueda generar. La directiva correspondiente se ha asignado a su equipo.

Si se ha asignado a su equipo una directiva determinada con un PIN predeterminado definido, es posible que pueda conectarse automáticamente a la POA con un token. No tiene que escribir ninguna credencial ni introducir un número PIN durante la conexión, sino que funciona de manera automática en la POA. La conexión automática a Windows depende de la configuración de la directiva.

Cómo conectarse automáticamente en la POA con un token:

1. Conecte el token.
2. Encienda el equipo.

Ha iniciado sesión automáticamente en el proceso de POA. La conexión automática a Windows depende de la configuración de la directiva.

- Windows se iniciará si la conexión automática se ha realizado correctamente.
- Si la conexión automática ha fallado, se le pedirá que introduzca el número PIN del token. Ha iniciado sesión en el proceso de POA.

## 2.8 Teclado virtual

En la POA, puede mostrar/ocultar un teclado virtual en la pantalla y hacer clic en las teclas para introducir las credenciales, entre otras cosas.

**Requisito previo:** el security officer debe haber activado la opción de mostrar el teclado virtual en la directiva del tipo **Configuración específica del equipo** aplicable.

Para que el teclado virtual se muestre en la POA, haga clic en **Opciones >>** en el cuadro de diálogo de conexión de la POA y marque la casilla **Teclado virtual**.



El teclado virtual es compatible con varias distribuciones, que podrán cambiarse mediante las mismas opciones que se utilizan para cambiar la distribución del teclado físico en la POA (véase [Cambio de la distribución del teclado](#), página 20).

## 2.9 Distribución del teclado

La práctica mayoría de los países cuenta con su propia distribución del teclado, por lo que las teclas se asignan de forma diferente. La distribución del teclado de la POA es importante a la hora de introducir nombres de usuarios, contraseñas y códigos de respuesta.

De forma predeterminada, SafeGuard Enterprise adopta la distribución del teclado de la POA que está definida en la Configuración regional y de idioma de Windows en el momento en que se instala SafeGuard Enterprise. Si la distribución del teclado en Windows está definida para "Alemán", para el teclado de la POA se utilizará la distribución alemana.

El idioma de la distribución del teclado utilizada se muestra en la POA, p. ej., "EN" para English (inglés). Además de la distribución predeterminada del teclado, también cabe la posibilidad de utilizar la distribución US (Inglés, Estados Unidos) del teclado.

### 2.9.1 Cambio de la distribución del teclado

Tanto la distribución del teclado de la POA (power-on authentication) como la distribución del teclado virtual se pueden cambiar.

Para cambiar el idioma de la distribución del teclado.

1. Seleccione **Inicio > Panel de control > Configuración regional y de idioma > Opciones avanzadas**.
2. En la ficha **Opciones regionales**, seleccione el idioma deseado.
3. En la ficha **Opciones avanzadas**, en el apartado **Configuración de la cuenta de usuario predeterminado**, active la opción **Aplicar toda la configuración a la cuenta de usuario actual y al perfil de usuario predeterminado**.
4. Haga clic en **Aceptar**.

La POA recordará la distribución del teclado utilizada durante la última conexión correcta y la habilitará automáticamente la próxima vez que se conecte. Para esto es necesario reiniciar dos veces el equipo del usuario. Si se desactiva la anterior distribución del teclado mediante la **Configuración regional y de idioma**, se sigue manteniendo a no ser que seleccione una diferente.

**Nota:** Además, es necesaria para cambiar el idioma de la distribución del teclado para los programas que no sean compatibles con Unicode.

Si el idioma que desea no está disponible en su sistema, probablemente Windows le pida que lo instale. Después, debe reiniciar el equipo dos veces consecutivas de manera que, la primera vez, la POA reconozca la nueva distribución del teclado y, la segunda, la POA pueda configurar la nueva distribución.

Puede cambiar la distribución del teclado necesaria para la POA si utiliza el ratón o el teclado (**Alt+Mayús**).

Puede ver qué idiomas están instalados y disponibles en el sistema mediante **Inicio > Ejecutar > regedit: HKEY\_USERS\.DEFAULT\Keyboard Layout\Preload**.

## 2.10 Teclas aceleradoras y teclas de función admitidas en la POA (power-on authentication)

Ciertas funciones y configuraciones de hardware pueden causar problemas al arrancar los equipos de usuarios, provocando a su vez que se bloquee el sistema. La POA (power-on authentication) permite disponer de una serie de teclas aceleradoras para modificar estas configuraciones de hardware y desactivar funciones. Aún más: hay una lista gris con una serie de configuraciones y funcionalidades de hardware de las que se sabe que pueden causar estos problemas que está integrada en el archivo .msi instalado en el equipo.

Le recomendamos que instale una versión actualizada del archivo de configuración de POA antes de realizar cualquier implementación significativa de SafeGuard Enterprise. El archivo se actualiza de forma mensual y se puede descargar en la siguiente ubicación:

<ftp://POACFG:POACFG@ftp.ou.utimaco.de>

Puede personalizar este archivo para adaptarlo al hardware de un entorno específico.

**Nota:** Al definir un archivo personalizado, solo se podrá usar este en lugar del que está integrado en el archivo .msi. Sólo cuando no se haya definido ni encontrado un archivo de configuración de POA, se aplicará el archivo predeterminado.

Para instalar el archivo de configuración de POA, introduzca el siguiente comando:

```
MSIEXEC /i <Client MSI package> POACFG=<ruta del archivo de configuración de POA>
```

Para obtener más información, consulte el centro de conocimientos (knowledgebase):

<http://www.sophos.com/support/knowledgebase/article/65700.html>.

Además, la POA (power-on authentication) es compatible con un grupo de teclas de función.

## 2.10.1 Teclas aceleradoras

**Mayús-F3** = Compatibilidad con USB heredado (activar/desactivar)

**Mayús-F4** = Modo gráfico VESA (activar/desactivar)

**Mayús-F5** = Compatibilidad con USB 1.x y 2.0 (activar/desactivar)

**Mayús-F6** = Controladora ATA (activar/desactivar)

**Mayús-F7** = Compatibilidad sólo con USB 2.0 (activar/desactivar); la compatibilidad con USB 1.x se mantiene según lo establecido por **Mayús-F5**.

**Mayús-F9** = ACPI/APIC (activar/desactivar)

### Matriz de dependencias de las teclas aceleradoras

Mayús-F3	Mayús-F5	Mayús-F7	Heredado	USB 1.x	USB 2.0	Comentario
desactivado	desactivado	desactivado	activado	activado	activado	3.
activado	desactivado	desactivado	desactivado	activado	activado	Predeterminado
desactivado	activado	desactivado	activado	desactivado	desactivado	1., 2.
activado	activado	desactivado	activado	desactivado	desactivado	1., 2.
desactivado	desactivado	activado	activado	activado	desactivado	3.
activado	desactivado	activado	desactivado	activado	desactivado	
desactivado	activado	activado	activado	desactivado	desactivado	
activado	activado	activado	activado	desactivado	desactivado	2.

1. **Mayús-F5** Mayús F5 deshabilita tanto el USB 1.x como el USB 2.0.

**Nota:** Si se pulsa **Mayús-F5** durante el arranque, se reduce considerablemente el tiempo que lleva lanzar la POA. Sin embargo, tenga en cuenta que si su equipo utiliza un teclado o un ratón USB, es posible que se deshabiliten al pulsar **Mayús-F5**.

**Nota:** La POA puede utilizar el teclado USB mediante el BIOS SMM. Sin compatibilidad con el token USB

2. Si no hay ninguna opción de compatibilidad con USB activa, la POA intenta utilizar el BIOS SMM en lugar de realizar una copia de seguridad del controlador USB y restaurarlo. El modo Heredado puede funcionar en esa situación.
3. La compatibilidad con el modo Heredado y el USB están activos. La POA intenta realizar una copia de seguridad del controlador USB y restaurarlo. Dependiendo de la versión de BIOS utilizada, el sistema podría no responder.

**Nota:** Es posible que los cambios que se pueden ejecutar con las teclas aceleradoras se hayan especificado previamente durante la instalación del cliente de SafeGuard Enterprise con un archivo .mst.

Tras modificar la configuración de hardware con las teclas aceleradoras de la POA, se muestra un cuadro de diálogo en el que se le pide que guarde los cambios de la configuración. Este cuadro de diálogo muestra una descripción general de la configuración que va a guardarse. Para guardar los cambios, haga clic en **Sí**. Tras reiniciar el equipo, se activará la nueva configuración. Si hace clic en **No**, los cambios no se guardarán y permanecerá la configuración anterior una vez que se reinicie el equipo.

Si pulsa **F5** en cualquier cuadro de diálogo de la POA, abrirá un cuadro de diálogo en el que se indica la configuración de las teclas aceleradoras utilizada para iniciar la POA. Si se han cambiado las teclas aceleradoras durante el proceso de arranque, los estados de las teclas pertinentes se mostrarán en azul. El color azul significa que la tecla se ha utilizado con ese estado para iniciar la POA, pero que no se ha guardado aún. Los cambios sin guardar se mostrarán en negro. Para cerrar el cuadro de diálogo, pulse **F5** de nuevo o pulse **Intro**.

## 2.10.2 Teclas de función en el cuadro de diálogo de conexión

**Nota:** Las teclas de función son distintas de las teclas aceleradoras.

**F2** = cancela la conexión automática.

**F5** = muestra un cuadro de diálogo donde aparece la configuración de la tecla aceleradora utilizada para iniciar la POA.

**F8** = cambia la contraseña de la POA. Se debe utilizar en lugar de la tecla **Intro** para activar el cambio de contraseña en la POA tras la conexión.

**Alt+Mayús.** (teclas **Alt** y **Mayús.** situadas a la izquierda) = cambia la distribución del teclado de alemán a inglés (o al revés).

### Cancelar y preparar la POA para apagar

**Ctrl+Alt+Supr** = si ha fallado la autenticación pero es necesario apagar el PC de forma segura. Esta combinación de teclas tiene la misma función que el botón **Apagar**.

**Nota:** Si está activada la conexión mediante huella digital, puede utilizar la combinación **Ctrl+Alt+Supr** en el cuadro de diálogo de la POA de conexión mediante huella digital para cambiar y activar el cuadro de diálogo de POA de conexión con nombre de usuario y contraseña. Si desea obtener más información sobre la conexión mediante huella digital, véase [Autenticación con el Lector de huellas digitales de Lenovo](#), página 39.

## 2.11 Sincronización de la contraseña

SafeGuard Enterprise detecta automáticamente cuándo ha cambiado la contraseña de Windows y ya no se corresponde con la que hay almacenada en la base de datos de SafeGuard Enterprise. Esto puede pasar si la contraseña de Windows se cambia mediante una VPN, en otro equipo o en Active Directory.

Si SafeGuard Enterprise detecta la situación, se le solicitará que introduzca la contraseña anterior. Después, la contraseña almacenada por SafeGuard Enterprise se actualizará con la nueva contraseña de Windows.

La sincronización de la contraseña se producirá en dos situaciones:

- durante la conexión
- durante un procedimiento de bloqueo/desbloqueo de Windows

## 3 POA (power-on authentication) en Windows Vista

La POA (power-on authentication) en Windows Vista tiene el mismo aspecto y funciona igual que en Windows XP, (véase [POA \(power-on authentication\)](#), página 4). Solamente aparecen diferencias al conectarse al sistema operativo en sí mismo. Windows Vista presenta varios métodos de autenticación en paralelo para que el usuario se conecte.

**Nota:** Esta sección del manual sólo describe las diferencias relativas a Windows Vista. Si no se explicita la existencia de una diferencia, se deduce que los procedimientos y procesos descritos en la anterior sección acerca de la POA (power-on authentication) también se aplican a Vista.

### 3.1 Primera conexión tras la instalación de SafeGuard Enterprise en Windows Vista

Si se ha instalado SafeGuard Enterprise con POA (power-on authentication), el procedimiento de arranque es diferente durante el primer inicio del sistema tras haber instalado SafeGuard Enterprise en el equipo. Aparecen una serie de nuevos mensajes de inicio (como por ejemplo, la pantalla de conexión automática), debido a que SafeGuard Enterprise se ha incorporado al procedimiento de arranque del sistema. Después, se iniciará el sistema operativo Windows.

**Nota:** En Windows Vista, primero debe pulsar **Ctrl+Alt+Supr** para iniciar la conexión y la conexión automática. El administrador puede desactivar esta configuración en la consola MMC en el editor de objetos de directivas de grupo, en **Configuración de Windows > Configuración de seguridad > Directivas locales > Desactivar opciones de seguridad** (Conexión interactiva: **Ctrl+Alt+Supr** no es necesaria).

**Nota:** SafeGuard Enterprise utiliza una conexión basada en certificados. Los usuarios necesitan claves y certificados para conectarse correctamente en la POA. Sin embargo, solamente se crearán las claves y los certificados específicos para el usuario una vez que se haya conectado correctamente a Windows, lo que implica que únicamente es posible autenticarse en la POA si se ha accedido sin problemas a Windows.

Por consiguiente, la primera vez que se conecte a Windows después de la instalación, debe hacerlo utilizando sus credenciales habituales. Posteriormente, se le registrará como usuario de SafeGuard Enterprise. Este proceso de registro es necesario para asegurarse de que la POA reconozca sus credenciales la próxima vez que el sistema se inicie.

Tras registrarse correctamente y recibir todos los datos necesarios, aparecerá una información sobre herramientas en el equipo que se lo anunciará.

Cuando reinicie el equipo, se activará la POA. A partir de ese momento, debe especificar sus credenciales de Windows en la POA, tras lo que se conectará a Windows automáticamente sin tener que escribir ninguna contraseña (si está activada la conexión automática a Windows).

Puede conectarse a la POA mediante el nombre de usuario y la contraseña.

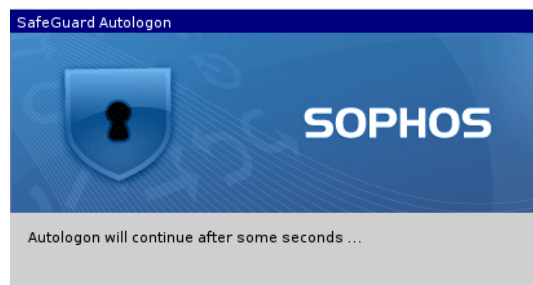
**Nota:** El security officer de SafeGuard Enterprise define centralmente la configuración de los PC del usuario en los que se instala SafeGuard Enterprise, que se distribuye a los equipos de usuarios a través de archivos de directivas.

### 3.1.1 Procedimiento para la primera conexión

Esta sección describe el procedimiento de la primera conexión a su equipo después de instalar SafeGuard Enterprise. El procedimiento de la primera conexión sólo corresponderá al descrito aquí si la POA se ha instalado y activado en su equipo.

### 3.1.2 Conexión automática a SafeGuard

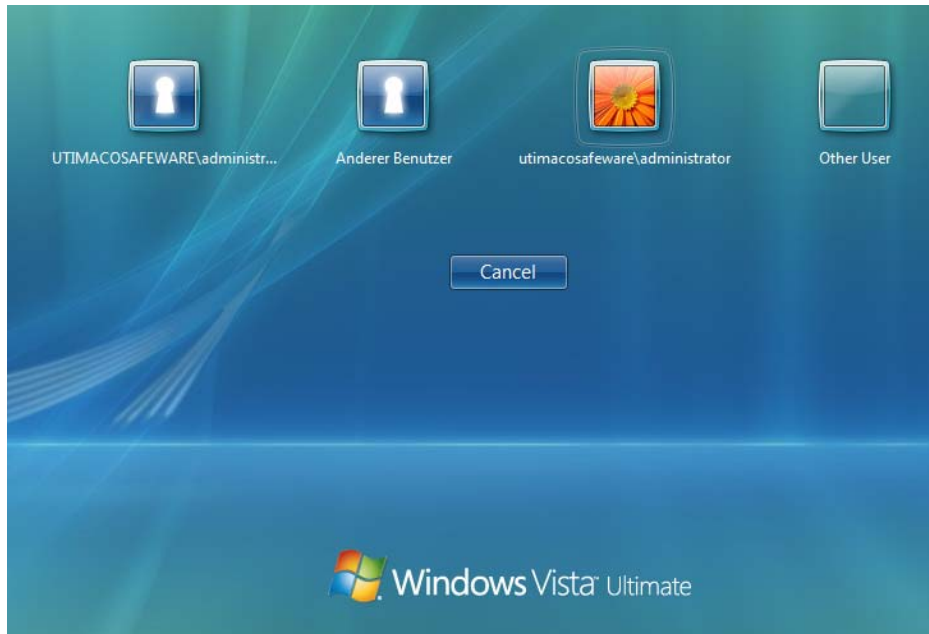
1. Se inicia el cliente y aparecerá el cuadro de diálogo de la conexión automática a SafeGuard Enterprise.



- Hay un usuario automático conectado.
- El equipo se registrará automáticamente en el servidor de SafeGuard Enterprise, siempre que exista alguna conexión con tal servidor de SafeGuard Enterprise.
- La clave del equipo se envía al servidor de SafeGuard Enterprise y se almacena en la base de datos de SafeGuard Enterprise.
- Las directivas de equipo se enviarán al ordenador.

### 3.1.3 Conexión a Windows Vista

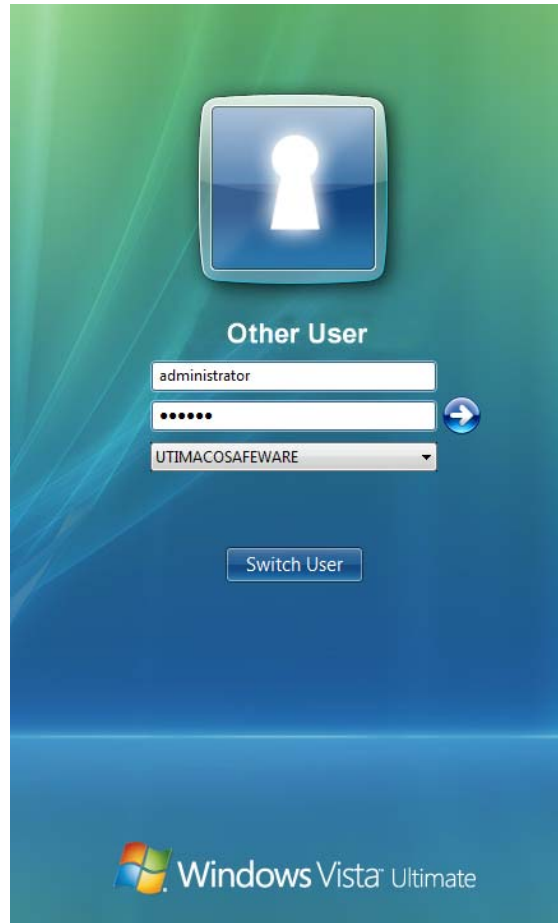
1. Aparece el cuadro de diálogo de conexión de Windows Vista.



En Windows Vista, SafeGuard Enterprise ofrece un método de autenticación adicional. El ejemplo muestra el método de autenticación de SafeGuard Enterprise y los iconos del método de autenticación de Vista.

2. Windows Vista cuenta con dos iconos para cada método de autenticación:
  - Si hace clic en **Otro usuario**, se abrirá un cuadro de diálogo para especificar las credenciales.
  - Al hacer clic en el segundo icono (ya se muestra un nombre de usuario debajo del icono), abre un cuadro de diálogo que contiene la información de usuario del último usuario conectado al sistema. Sólo hay que especificar la contraseña.

Si su nombre de usuario aparece debajo de un icono de SafeGuard Enterprise, seleccione dicho icono. Si éste no es el caso, seleccione el icono **Otro usuario** de SafeGuard Enterprise.



3. Especifique sus credenciales de usuario de Windows de la forma habitual.
  - El Id. de usuario y un hash de las credenciales del usuario se enviarán al servidor.
  - Las directivas, los certificados y las claves del usuario se crearán y se enviarán al cliente.

Los datos de usuario sólo están disponibles en la OA (power-on authentication) después de que todos los datos se hayan sincronizado correctamente entre el servidor de y el equipo.

Esto significa que **la próxima vez que se inicie el sistema**, sólo tendrá que especificar sus credenciales de usuario de Windows (nombre de usuario y contraseña) en la POA y se conectará automáticamente.

Para activar la POA (power-on authentication), es necesario reiniciar el sistema. Tras el reinicio, POA protege el equipo contra el acceso no autorizado.

### 3.1.4 Conexión a la POA (power-on authentication) tras el reinicio

1. Tras reiniciar el ordenador, aparecerá el cuadro de diálogo de conexión de POA.



Los certificados y las claves están disponibles y puede conectarse a POA con sus credenciales de Windows.

2. Especifique su nombre de usuario y contraseña y haga clic en **Aceptar**.

Se evaluarán sus credenciales. Cuando el sistema haya comprobado sus credenciales de usuario, se conectará automáticamente a Windows.

**Nota:** La conexión automática a Windows se puede desactivar mediante la configuración de una directiva. En tal caso, se mostrará el cuadro de diálogo de conexión a Windows y tendrá que especificar sus credenciales.

## 3.2 Conexión en la POA (power-on authentication) en Windows Vista

Tras la correcta activación de la POA (sincronización inicial y reinicio), conéctese especificando sus credenciales de usuario de Windows en el cuadro de diálogo de conexión de POA. Se conectará a Windows automáticamente.

**Nota:** Puede desactivar la conexión automática a Windows si pulsa el botón **Opciones >>** en el cuadro de diálogo de conexión y desactiva la opción **Conexión automática a Windows**. Por ejemplo, es necesario desactivar la conexión automática para permitir que otros usuarios utilicen la POA en el equipo pertinente. El security officer define en las directivas relevantes si la conexión automática a Windows se activa o se desactiva, y si se le permite que usted cambie dicha configuración en el cuadro de diálogo de conexión.

### 3.2.1 Retraso en la conexión al producirse un error en el intento de conexión

Si se produce un error en la conexión de la POA, por ejemplo, a causa de una contraseña incorrecta, se mostrará un mensaje de error y se impondrá un retraso en el próximo intento de conexión. El período de retraso aumentará cada vez que tenga lugar un intento de conexión fallido. Los intentos de conexión fallidos quedan registrados.

### 3.2.2 Bloqueo del equipo

De acuerdo con la configuración de directivas, es posible que su equipo quede bloqueado tras un número predeterminado de intentos de conexión fallidos. Para desbloquearlo, inicie un procedimiento de desafío/respuesta, véase [Recuperación mediante el procedimiento de desafío/respuesta](#), página 59.

## 3.3 Conexión en la POA utilizando tarjetas inteligentes o tokens en Windows Vista

Hay dos tipos posibles de conexión mediante tarjetas inteligentes o tokens:

- La conexión sólo se permite utilizando tarjetas inteligentes o tokens.
- La conexión se permite a través del nombre de usuario y la contraseña o a través de la tarjeta inteligente o token.

El security officer define el tipo de conexión permitido centralmente a través de una directiva.

El security officer generará su tarjeta inteligente/token y se la dará, o bien usted mismo incluirá sus credenciales de usuario de Windows en su tarjeta inteligente/token.

**Nota:** Desde la perspectiva de SafeGuard Enterprise, las tarjetas inteligentes y los tokens se tratan de la misma forma. Por tanto, los términos "token" y "tarjeta inteligente" se consideran sinónimos tanto en el producto como en el manual.

**Nota:** En las secciones siguientes, utilizaremos el término "token".

### 3.3.1 Primera conexión con token después de la instalación

El procedimiento que se utiliza para realizar la primera conexión con un token es el mismo que el que se ha descrito para conectarse sin él.

Si hay disponible un token generado en este momento, puede utilizarlo para conectarse a Windows mediante el número PIN del mismo.

**Nota:** Se recomienda que configure su token con las credenciales de Windows (véase [Almacenamiento de la información de usuario de Windows en el token](#), página 33) antes de reiniciar el equipo.

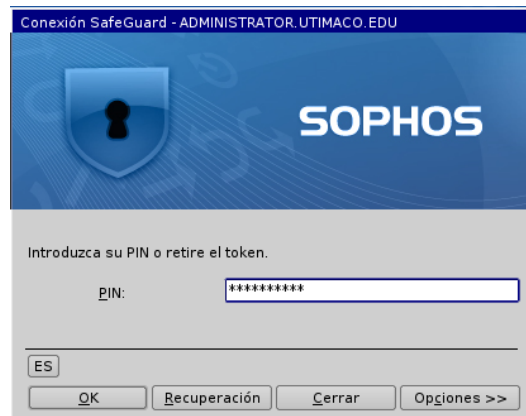
**Nota:** Las directivas de seguridad que se le aplican pueden exigir que utilice un token en la POA. Si el token no contiene información de usuario, no podrá conectarse en la POA.

### 3.3.2 Conexión en la POA con un token

**Requisito previo:** asegúrese de que en la BIOS esté activada la compatibilidad con USB. Debe inicializarse la compatibilidad con el token para que se pueda generar.

Cómo conectarse en la POA con un token:

1. Conecte el token.
2. Encienda el equipo y espere hasta que aparezca el cuadro de diálogo para la conexión con el token.



**Nota:** Si la directiva le permite conectarse con sus credenciales de usuario y desconecta el token, se le pedirá que especifique sus credenciales de usuario para conectarse. Si el cuadro de diálogo para conectarse utilizando el Id. de usuario y la contraseña no aparece, puede hacerlo utilizando un token en la POA.

3. Especifique el número PIN del token.

Está conectado a la POA y a Windows (si la opción "Conexión automática a Windows" está activada en el cuadro de diálogo de conexión).

### 3.3.3 Cambio de número PIN

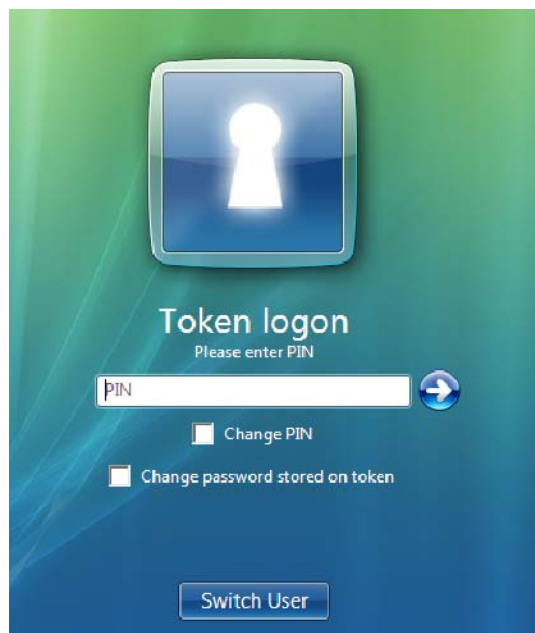
El número PIN del token se puede cambiar cuando aparece el cuadro de diálogo de conexión de Windows.

Si la opción **Conexión automática a Windows** está activada en la POA, generalmente no se mostrará el cuadro de diálogo de conexión de Windows. Para abrirlo, por ejemplo, para cambiar el número PIN, tiene que desactivar esta opción durante la conexión a la POA.

Si el security officer ha definido reglas que requieran un cambio de número PIN (por ejemplo, a intervalos de tiempo concretos), se le solicitará automáticamente que cambie el número PIN.

Cómo cambiar el número PIN del token:

1. En el cuadro de diálogo PIN que se muestra para conectarse a Windows, seleccione la opción **Cambiar PIN**.



2. Especifique el número PIN del token y haga clic en **Aceptar**.

Aparecerá el cuadro de diálogo Cambiar PIN.



3. Especifique el número PIN nuevo y confírmelo.
4. Haga clic en **Aceptar**.

El número PIN del token se cambia y continúa la conexión a Windows.

### 3.3.4 Almacenamiento de la información de usuario de Windows en el token

Si el token no tiene almacenada información de usuario de Windows, puede incluirla usted mismo.

**Nota:** Le recomendamos que configure su token durante la primera conexión. Las directivas de seguridad que se le apliquen pueden exigir que utilice un token en la POA. Si el token no contiene ninguna información de usuario, no podrá conectarse en la POA.

1. Durante la primera conexión después de la instalación, conecte el token al sistema cuando aparezca el cuadro de diálogo de conexión de Windows.

Si el sistema detecta un token vacío, mostrará automáticamente el cuadro de diálogo para generar tokens.



2. Introduzca su nombre de usuario de Windows y la contraseña.
3. Confirme la contraseña.
4. Seleccione o especifique el dominio y haga clic en **Aceptar**.

El sistema intentará conectarle a Windows utilizando los datos especificados. Si la conexión es correcta, los datos se escribirán en el token.

Ya está conectado a Windows.

Si la conexión al token se define como opcional para el usuario (ya se ha conectado una vez en la POA con su nombre de usuario y contraseña), también puede generar posteriormente el token.

Para ello, desactive esta opción (**Opciones > Conexión automática a Windows**) en el cuadro de diálogo de la POA. Se mostrará el cuadro de diálogo de conexión de Windows y podrá almacenar los datos en el token como se ha descrito anteriormente.

### 3.3.5 Desbloqueo de tarjetas inteligentes o tokens en Windows Vista

Si especifica un número PIN incorrecto varias veces, el token se bloqueará. El security officer puede configurar SafeGuard Enterprise para que aparezca el cuadro de diálogo para desbloquear tokens:



Para desbloquear el token, el security officer tiene que proporcionarle el número PIN del administrador definido para su token.

Para desbloquear un token:

1. Especifique el número PIN del administrador.
2. Especifique un número PIN nuevo y confírmelo.

El número PIN que especifique estará sujeto a las reglas definidas para los números PIN (por ejemplo, es posible que se necesiten combinaciones de caracteres concretos, se puede prohibir que se vuelvan a utilizar los números PIN ya utilizados, etc).

3. Haga clic en **Aceptar**.

El token se desbloqueará y continuará el proceso de conexión.

Si esta función no está disponible en el equipo, puede volver a acceder al mismo a través de un procedimiento de desafío/respuesta.

**Nota:** Si bien puede volver a acceder al equipo mediante un procedimiento de desafío/respuesta, esto no le permite cambiar el PIN ni las credenciales de usuario.

## 4 Conexión a Windows Vista

En Windows Vista, SafeGuard Enterprise ofrece un método de autenticación adicional.

Si desactiva la opción **Conexión automática a Windows** en el cuadro de diálogo de conexión de la POA, se mostrará el cuadro de diálogo de conexión a Windows Vista. En este cuadro de diálogo también puede seleccionar un método de autenticación distinto.

**Nota:** El uso de otro método de autenticación no supone que SafeGuard Enterprise esté inactivo en su equipo. En ese caso, la conexión a SafeGuard Enterprise no se realizará durante la conexión a Windows, sino después de la conexión de Windows Vista.

### 4.1 Conexión mediante SafeGuard Enterprise

Normalmente, se conectará automáticamente a Windows después de escribir su contraseña en la POA. Si desactiva la opción **Conexión automática a Windows** en el cuadro de diálogo de conexión de POA y utiliza el método de SafeGuard Enterprise para conectarse a Windows, SafeGuard Enterprise estará disponible con todo su ámbito de funcionalidad tras conectarse a Windows Vista.

Las claves necesarias estarán disponibles y todos los datos se cifrarán y descifrarán de acuerdo con las directivas definidas.

### 4.2 Conexión a través de un método de autenticación alternativo

En el cuadro de diálogo de conexión de Windows también puede seleccionar un método de autenticación alternativo para conectarse a Windows, en lugar del método de autenticación de SafeGuard Enterprise.

Si utiliza un método alternativo para conectarse al sistema operativo, la conexión a SafeGuard Enterprise se llevará a cabo después de la conexión al sistema operativo.

Después de conectarse a Windows Vista, la aplicación de autenticación de SafeGuard Enterprise se iniciará automáticamente.

En función de la configuración de conexión de la administración central, se mostrará un cuadro de diálogo para introducir las credenciales de usuario o un cuadro de diálogo para introducir el número PIN.

1. Especifique las credenciales o el número PIN y haga clic en **Aceptar**.

A partir de ese momento, la funcionalidad de SafeGuard Enterprise estará disponible y podrá, por ejemplo, acceder a los datos cifrados, siempre que tenga la clave necesaria.

## 4.3 Sincronización de la contraseña en Windows Vista

SafeGuard Enterprise detecta automáticamente si ha cambiado la contraseña de Windows y ya no se corresponde con la que hay almacenada. Esto puede pasar si la contraseña de Windows se cambia mediante una VPN, en otro equipo o en Active Directory.

Si SafeGuard Enterprise detecta la situación, se le informará y se le solicitará que introduzca la contraseña anterior. Después, la contraseña almacenada por SafeGuard Enterprise se actualizará con la nueva contraseña de Windows.

La sincronización de la contraseña se producirá en dos situaciones:

- durante la conexión
- durante un procedimiento de bloqueo/desbloqueo de Windows

## 5 Autenticación con el Lector de huellas digitales de Lenovo

Los usuarios deben recordar numerosas contraseñas y números PIN para acceder a sus ordenadores, aplicaciones y redes. Con un lector de huellas digitales, lo único que necesita para conectarse es pasar el dedo por el lector, en lugar de utilizar una contraseña o un token.

Asimismo, es imposible perder u olvidar sus credenciales, ni que personas no autorizadas adivinen esta información. Así, el uso de lectores de huellas digitales simplifica el proceso de conexión y aumenta la seguridad.

SafeGuard Enterprise permite la autenticación mediante huella digital en la POA y en la autenticación con Windows. Por ejemplo, para autenticarse en un portátil Lenovo, sólo tiene que pasar el dedo sobre el lector integrado. El resto del proceso de autenticación será automático. También puede bloquear y desbloquear el escritorio de Windows pasando el dedo por el lector de huellas digitales.

Determinados portátiles Lenovo llevan integrado un lector de huellas digitales. No obstante, también se puede usar un teclado USB externo para la conexión mediante huella digital.

- Un ordenador sólo puede tener conectado un lector de huellas digitales a la vez.
- No es posible combinar en un mismo equipo procedimientos de conexión mediante token y huella digital.
- No se admite la conexión remota mediante huella digital.

### 5.1 Requisitos

Es necesario satisfacer los requisitos enunciados a continuación para emplear la conexión mediante huella digital:

#### 5.1.1 Requisitos generales

- Hardware de Lenovo
- Lector de huellas digitales de Lenovo en el portátil o en un teclado USB con un lector de huellas digitales
- Se recomienda disponer de la BIOS más actualizada.
- SafeGuard Enterprise, versión 5.35 o posterior

- Antes que SafeGuard Enterprise debe estar instalada la versión recomendada de software específica del proveedor:
  - ThinkVantage Fingerprint para AuthenTec
  - o bien
  - ThinkVantage Fingerprint para UPEK
- El security officer debe haber configurado la opción de huella digital en la directiva de **Autenticación** relacionada.

### 5.1.2 Requisitos del sistema

- Windows XP, 32 bits
- Windows Vista, 32 bits, 64 bits
- Windows 7, 32 bits, 64 bits

### 5.1.3 Hardware compatible

- AuthenTec AES2810
- UPEK TCS3C/TCD42A

### 5.1.4 Software compatible

- Lenovo Fingerprint para AuthenTec Versión 3.2.0.166
- ThinkVantage Fingerprint para UPEK Versión 5.8.5.6014

## 5.2 Registro de huellas digitales

Para poder autenticarse en su portátil/PC mediante huella digital, primero deberá registrar una o más huellas mediante el software recomendado por el fabricante. El proceso de registro une el dedo registrado a sus credenciales (nombre de usuario y contraseña).

**Requisitos previos:** en el siguiente procedimiento se da por hecho que está instalado tanto el software recomendado por el fabricante como SafeGuard Enterprise.

Para registrar una huella digital:

1. Auténtíquese en la POA mediante el nombre de usuario y la contraseña.
2. Registre una o varias de sus huellas digitales mediante el software instalado, indicado por el fabricante. Este registro unirá su huella digital a sus credenciales de Windows.
  - a) Consulte la documentación del software ThinkVantage Fingerprint para ver cómo registrar una huella.
  - b) Habilite la opción **POA password in BIOS** (sólo en UPEK. para AuthenTec este paso no es necesario).
  - c) Para poder utilizar la conexión mediante huella digital en la POA, primero debe conectarse a Windows con la huella digital y transferir las credenciales al lector de huellas digitales. Para UPEK, sólo debe pasar un dedo registrado sobre el lector de huellas digitales. Para AuthenTec también deberá introducir su contraseña de Windows en la primera conexión.
3. Reinicie el PC/portátil.
4. Para probar la huella digital registrada, pase el dedo sobre el lector de huellas digitales tras reiniciar el ordenador.

Si la huella coincide con una de las registradas, se validará automáticamente contra Windows.

## 5.3 Conexión a POA mediante la huella digital

**Requisitos previos:**

- El security officer debe haber configurado la opción de huella digital en la directiva de **Autenticación** relacionada.
- Debe haber registrado una o más huellas.

1. Reinicie el PC/portátil.

Se muestra el diálogo de POA para conectarse con una huella digital.



2. Pase uno de los dedos registrados sobre el lector.

Si el software reconoce correctamente la huella, la POA leerá las credenciales y las enviará a Windows.

**Nota:** El procedimiento de conexión utiliza iconos con mensajes cortos de texto, como solicitudes, notificaciones y advertencias (véase [Iconos utilizados en el proceso de conexión](#), página 43).

Se conectará automáticamente a Windows sin que se le pidan más datos.

- Si el proceso de registro en Windows no se ha completado correctamente (por ejemplo, en el caso de que tras haber registrado las huellas digitales, no se haya desconectado y se haya vuelto a conectar en Windows), se encontrará una coincidencia de las huellas digitales registradas en la POA.

No obstante, no habrá ninguna credencial. En este caso, se mostrará un mensaje de error, en el que se le solicitará que se conecte con el nombre de usuario y contraseña, pero sin conexión automática a Windows. Sus credenciales se transferirán al lector de huellas digitales.

- El security officer especifica en las directivas que le afectan si se habilita la conexión automática a Windows y si se le permite cambiar esta opción en el cuadro de diálogo de POA para conectarse con un nombre de usuario y contraseña (véase [Conexión con nombre de usuario y contraseña](#), página 45).

### 5.3.1 Iconos utilizados en el proceso de conexión

Cuando se inicia sesión en POA con huella digital, el sistema utiliza iconos como instrucciones, notificaciones y advertencias. Estos iconos se muestran durante el proceso de conexión junto a un mensaje corto de texto.



Le solicita que pase el dedo sobre el lector de huellas digitales.



Indica que la conexión mediante huella digital no está activada en esos momentos. Esto puede suceder, por ejemplo, si el módulo de conexión mediante huella digital todavía no se ha iniciado.



Indica que el lector de huellas digitales está funcionando y está ocupado.



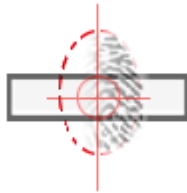
Indica que la huella se ha leído correctamente y se ha encontrado una coincidencia.



Indica que la huella se ha leído correctamente, pero no se ha encontrado ninguna coincidencia.



Indica que no se ha podido leer la huella digital. Vuelva a pasar el dedo por el lector de huellas digitales.



Indica que ha colocado el dedo demasiado hacia la izquierda (o demasiado hacia la derecha). Mueva el dedo al centro del lector de huellas digitales.



Indica que ha pasado el dedo demasiado sesgado. Vuelva a pasar el dedo por el lector de huellas digitales.



Indica que ha movido el dedo demasiado rápido. Vuelva a pasar el dedo por el lector de huellas digitales.



Indica que no ha dejado el dedo en el lector tiempo suficiente. Vuelva a pasar el dedo por el lector de huellas digitales.

### 5.3.2 Intentos de conexión fallidos

Si el sistema no puede leer la huella digital tras cinco intentos, lo considera como un intento fallido de conexión y lo registra como evento. En este caso, se aplica un período de retraso en la conexión.

Si el sistema puede leer la huella digital sin errores, pero no encuentra una coincidencia con la huella registrada tras cinco intentos, lo considera como un intento fallido de conexión y lo registra como evento. En este caso, también se aplica un período de retraso en la conexión.

El período de retraso en la conexión aumenta con cada intento de conexión fallido.

### 5.3.3 Conexión con nombre de usuario y contraseña

Aunque la conexión mediante huella digital esté habilitada, puede seguir iniciando sesión en la POA con su nombre de usuario y contraseña, por ejemplo, en el caso de que no pueda conectarse con la huella digital porque el lector esté dañado.

Para autenticarse con sus datos de conexión de usuario:

1. Pulse la tecla **Esc** o bien **Ctrl+Alt+Supr** en el cuadro de diálogo de la POA destinado a la conexión mediante huella digital.

Aparecerá el diálogo de POA para conectarse con el nombre de usuario y la contraseña.



**Nota:** Si pulsa **Ctrl+Alt+Supr** en el cuadro de diálogo de POA para conectarse con el nombre de usuario y la contraseña, el equipo se apagará. En este cuadro de diálogo, la combinación de las teclas **Ctrl+Alt+Supr** se corresponde con el botón **Apagar**.

El cuadro de diálogo de POA para la conexión con nombre de usuario y contraseña también aparece automáticamente si el lector de huellas digitales no está disponible o si el sistema no encuentra los datos de usuario del lector de huellas digitales.

**Nota:** La conexión con un nombre de usuario y contraseña también se habilita automáticamente si la caché local está dañada. Si ocurriese tal cosa, el equipo se bloqueará y tendrá que conectarse mediante un procedimiento de desafío/respuesta (véase [Inicio de un procedimiento de desafío/respuesta al conectarse mediante huella digital](#), página 47).

2. También puede optar por pulsar **Esc** de nuevo para volver al cuadro de diálogo de POA y conectarse mediante la huella digital.

Si ha pulsado **Esc** para activar el cuadro de diálogo de POA para conectarse con el nombre de usuario y la contraseña, podrá conectarse pasando el dedo por el lector de huellas digitales sin tener que volver primero al cuadro de diálogo de POA para la conexión mediante huella digital.

## 5.4 Cambio de contraseña

1. Si está habilitada la conexión mediante huella digital en la POA, puede modificar la contraseña de Windows pulsando **Ctrl+Alt+Supr**.

Cuando cambia la contraseña, el sistema le solicita que pase el dedo por el lector de huellas digitales para transferir la contraseña nueva al lector.

**Nota:** Siempre que cambie la contraseña, el cambio se aplicará a todos los dedos registrados.

### 5.4.1 Sincronización de la contraseña

Si la contraseña de Windows ya no coincide con la contraseña almacenada en el lector de huellas digitales, por ejemplo, cuando haya cambiado de contraseña, pero la contraseña nueva no se haya transferido al lector, puede sincronizarla realizando los siguientes pasos.

1. Reinicie el ordenador.
2. Pulse la tecla **Esc** o bien **Ctrl+Alt+Supr** en el cuadro de diálogo de POA para la conexión mediante huella digital, con el fin de cambiar al cuadro de diálogo de POA para la conexión con un nombre de usuario y contraseña.
3. Haga clic en **Opciones** y desactive la **Conexión automática a Windows**.  
El security officer especifica en las directivas que le afectan si se habilita la conexión automática a Windows y si se le permite cambiar esta opción en el diálogo de POA para conectarse con un nombre de usuario y contraseña.
4. Conéctese con su contraseña.
5. Aparecerá el cuadro de diálogo de conexión de Windows. Pase uno de los dedos registrados sobre el lector de huellas digitales.
6. El sistema reconocerá la huella digital, pero Windows rechazará de todos modos la contraseña asociada a la huella. Sin embargo, no se considera como un intento fallido de conexión, por lo que se no se aplica un retraso en la conexión.
7. En su lugar, se mostrará un mensaje que indica que se ha cambiado la contraseña y el sistema le solicitará que introduzca la contraseña actual de Windows. Introduzca la contraseña actual de Windows.

Si introduce aquí una contraseña incorrecta de Windows, se registrará como intento fallido de conexión y se aplicará el retraso en la conexión. Si cierra el cuadro sin introducir una contraseña, también se registrará como intento fallido de conexión y se aplicará un retraso en la conexión.

Al transferir correctamente la contraseña, se completará el proceso de sincronización y podrá usarla para conectarse.

## 5.5 Inicio de un procedimiento de desafío/respuesta al conectarse mediante huella digital

Para recuperar la conexión, puede llevar a cabo un procedimiento de desafío/respuesta. Esto puede ser necesario, por ejemplo, si la conexión mediante huella digital no funciona y se le ha olvidado la contraseña necesaria para conectarse. El procedimiento de desafío/respuesta de SafeGuard Enterprise representa un método muy seguro y eficaz para intercambiar información de forma confidencial.

Para iniciar un procedimiento de desafío/respuesta cuando esté habilitada la conexión mediante huella digital:

1. Pulse la tecla **Esc** en el cuadro de diálogo para conectarse mediante huella digital.

Aparecerá el diálogo para conectarse con el nombre de usuario y la contraseña.

2. Haga clic en **Recuperación** para iniciar el procedimiento de desafío/respuesta.

Debido a este procedimiento, puede que se le ofrezca la posibilidad de cambiar la contraseña cuando inicie el ordenador, por ejemplo, para permitir la recuperación en el caso de que no la recuerde. En este caso, el sistema también le ofrecerá la posibilidad de actualizar las credenciales de la huella digital.

Si quiere ver una descripción detallada del procedimiento de desafío/respuesta, véase [Recuperación mediante el procedimiento de desafío/respuesta](#), página 59.

## 6 Opciones de recuperación

Para las recuperaciones (por ejemplo, si ha olvidado la contraseña), SafeGuard Enterprise presenta varias opciones adaptadas a distintos escenarios de recuperación:

### ■ Recuperación de la conexión mediante Local Self Help

Si ha olvidado la contraseña, Local Self Help le permite acceder al equipo sin la asistencia del centro de ayuda. Incluso en situaciones en que no disponga ni de teléfono ni de conexión a la red (por ejemplo, viajando en un avión), puede recuperar el acceso a su equipo. Para conectarse, no tiene más que responder una serie de preguntas predeterminadas en la POA (power-on authentication).

Si desea ver más detalles, véase [Recuperación mediante Local Self Help](#), página 49.

### ■ Recuperación mediante el procedimiento de desafío/respuesta

El mecanismo desafío/respuesta es un sistema de recuperación seguro y eficaz que le ayudará si no puede conectarse a su equipo o acceder a datos cifrados. Durante el procedimiento de desafío/respuesta, tendrá que proporcionarle un código de desafío generado en el equipo a la persona responsable del centro de ayuda, quien a su vez generará un código de respuesta con el que obtendrá autorización para realizar una acción determinada en el ordenador.

Si desea ver más detalles, véase [Recuperación mediante el procedimiento de desafío/respuesta](#), página 59.

Es el security officer quien, mediante directivas, activa ambas opciones de recuperación para su uso en el equipo.

## 7 Recuperación mediante Local Self Help

Si ha olvidado su contraseña y no le es posible ponerse en contacto con el centro de ayuda para conseguir asistencia, SafeGuard Enterprise pone Local Self Help a su disposición.

Al utilizar Local Self Help, puede volver a tener acceso a su portátil en situaciones en las que no le es posible utilizar un procedimiento de desafío/respuesta porque no puede acceder a un teléfono o conectarse a Internet (por ejemplo, durante un vuelo). Puede iniciar sesión en su equipo respondiendo a un número específico de preguntas predefinidas en la POA (power-on authentication).

El security officer puede definir las preguntas que se deban responder centralmente y distribuir las a los equipos de los usuarios. También puede definir sus propias preguntas, siempre y cuando la directiva aplicable le permita hacerlo. SafeGuard Enterprise pone a su disposición el asistente de Local Self Help para proporcionar las respuestas iniciales y para modificar las preguntas. Puede abrir el asistente de Local Self Help haciendo clic en el icono de la bandeja del sistema de SafeGuard Enterprise que se encuentra en la barra de tareas de Windows.

### 7.1 Requisitos previos

Antes de usar Local Self Help para recuperar una conexión, hay que cumplir con los siguientes requisitos:

- El security officer ha habilitado Local Self Help en la directiva aplicable y efectiva del tipo **Configuración general** y ha definido la configuración de esta función (p. ej., los permisos necesarios para definir sus propias preguntas).
- Ha activado Local Self Help en su equipo (véase [Activación de Local Self Help](#), página 49).

### 7.2 Activación de Local Self Help

Una vez que la directiva que le permite utilizar Local Self Help se haya hecho efectiva, tiene que activar la función respondiendo a las preguntas predefinidas recibidas o definiendo y respondiendo sus propias preguntas.

Local Self Help sólo se activará en su equipo cuando haya respondido y guardado al menos diez preguntas.

De acuerdo con la configuración de las directivas, éstos son los posibles escenarios:

- **Ha recibido preguntas predefinidas y no dispone de los permisos necesarios para definir sus propias preguntas.**

Responda y guarde al menos diez de las preguntas predefinidas recibidas.

- **Ha recibido preguntas predefinidas y dispone de los permisos necesarios para definir sus propias preguntas.**

Responda y guarde al menos diez de las preguntas (predefinidas, sus propias preguntas definidas o una combinación de ambas).

- **No ha recibido preguntas predefinidas y dispone de los permisos necesarios para definir sus propias preguntas.**

Defina, responda y guarde al menos diez preguntas.

**Nota:** Para conectarse en la POA mediante Local Self Help, debe responder a cinco preguntas seleccionadas aleatoriamente de entre las diez preguntas respondidas.

**Requisito previo:** tras recibir la directiva, la información de herramientas le indica la existencia de preguntas de Local Self Help sin responder. Reinicie el equipo para agregar el comando **Local Self Help** al menú contextual del icono de la bandeja del sistema que se encuentra en la barra de tareas de Windows.

Para activar Local Self Help:

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de SafeGuard Enterprise, que se encuentra en la barra de tareas de Windows.
2. Seleccione **Local Self Help**.

Aparecerá el cuadro de diálogo de bienvenida al asistente de Local Self Help.

Por razones de seguridad, se le pedirá que introduzca su contraseña.

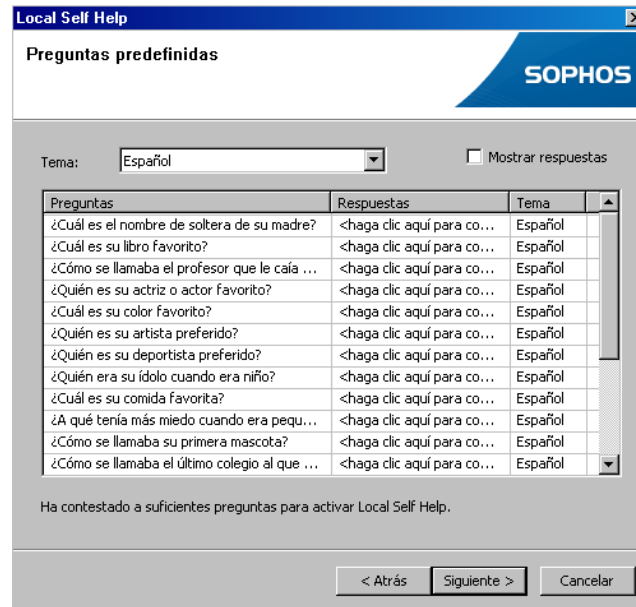
3. Especifique la contraseña y haga clic en **Siguiente**.

Se mostrará el cuadro de diálogo Descripción del estado.

Este cuadro de diálogo proporciona una instrucción breve sobre cómo activar Local Self Help. Además, muestra información de estado (p. ej., el número de preguntas respondidas definidas por el usuario, el número de preguntas predefinidas respondidas, etc).

4. Haga clic en **Siguiente**.

Si ha recibido preguntas predefinidas con la directiva efectiva, se mostrará el cuadro de diálogo Preguntas predefinidas.



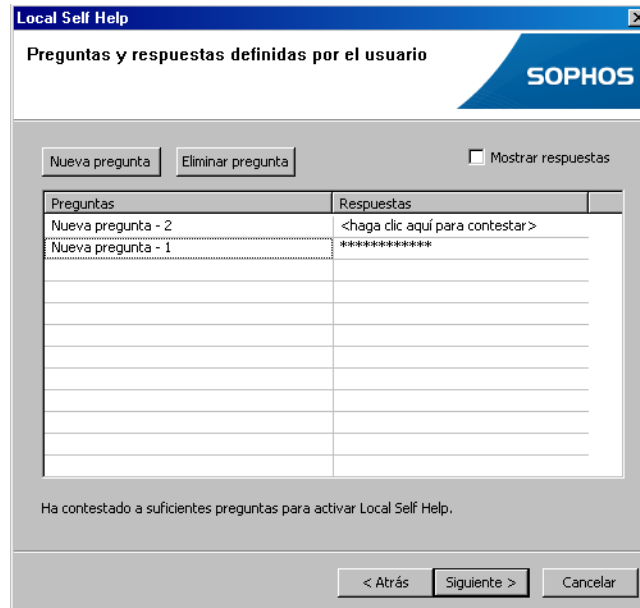
- Si ha recibido varios temas de preguntas diferentes, puede elegir entre ellos los que desea mostrar en la lista desplegable del campo **Tema**.
- Para que aparezcan todos los temas en una lista continua, seleccione la opción **Todos los temas** (predeterminada) de la lista desplegable.
- Para responder a las preguntas, haga clic en la pregunta correspondiente y escriba la respuesta en la columna **Respuestas**.
- Tras escribir la respuesta, el texto introducido se ocultará. Para que se muestre el texto, seleccione **Mostrar respuestas**.

**Nota:** Si responde a las preguntas durante el proceso de recuperación en la POA, deberá escribir las respuestas de la misma manera en que las escribió en el asistente de Local Self Help. Por ejemplo, las respuestas distinguen entre mayúsculas y minúsculas en Local Self Help.

**Nota:** Si va a escribir las respuestas en japonés, debe utilizar los caracteres Romaji (romanos). De lo contrario, las respuestas no coincidirán cuando responda a las preguntas en la POA.

5. Una vez que haya terminado de responder a las preguntas predefinidas, haga clic en **Siguiete**.

6. Si dispone de los permisos necesarios para definir sus propias preguntas, aparecerá el cuadro de diálogo Preguntas y respuestas definidas por el usuario.



- a) Para agregar una nueva pregunta, haga clic en **Nueva pregunta**.

Se añadirá una nueva línea a la lista de preguntas.

- b) Escriba la pregunta en la columna **Preguntas** y la respuesta en la columna **Respuestas**.

Tras escribir la respuesta, el texto introducido se ocultará.

- c) Para que se muestre el texto, seleccione **Mostrar respuestas**.

**Nota:** Si responde a las preguntas durante el proceso de recuperación en la POA, deberá escribir las respuestas de la misma manera en que las escribió en el asistente de Local Self Help.

Por ejemplo, las respuestas distinguen entre mayúsculas y minúsculas en Local Self Help.

**Nota:** Si va a escribir las respuestas en japonés, debe utilizar los caracteres Romaji (romanos).

De lo contrario, las respuestas no coincidirán cuando responda a las preguntas en la POA.

7. Una vez que haya terminado de definir y responder a sus propias preguntas, haga clic en **Siguiente**.

El último cuadro de diálogo del asistente de Local Self Help muestra la nueva información de estado tras responder a las preguntas. Un mensaje le indica si se cumplen los requisitos previos para la activación de Local Self Help.

8. Haga clic en **Finalizar**.

Se guardarán tanto las preguntas como las respuestas. Se mostrará un mensaje en el que se indica que Local Self Help se ha activado correctamente.

9. Haga clic en **Aceptar**.

Local Self Help estará activo en su equipo. Puede utilizar Local Self Help para la recuperación de inicio de sesión en la POA.

**Nota:** Si Local Self Help está activo en su equipo y debe restablecer la contraseña mediante el procedimiento de desafío/respuesta, las respuestas de Local Self Help almacenadas ya no tendrán validez. Local Self Help ya no estará activo en su equipo. Para volver a activar Local Self Help, responda de nuevo a las preguntas.

## 7.3 Edición de preguntas

Tras activar Local Self Help en su equipo, podrá editar las preguntas en cualquier momento:

- En cuanto a las preguntas predefinidas, puede modificar las respuestas que se proporcionaron al responder a las preguntas inicialmente. Sin embargo, las preguntas predefinidas no pueden eliminarse.
- Con respecto a las preguntas definidas por el usuario, puede modificar las respuestas que se proporcionaron la primera vez que se respondieron las preguntas, eliminar preguntas o agregar otras nuevas.

Cómo editar preguntas en el asistente de Local Self Help:

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de SafeGuard Enterprise, que se encuentra en la barra de tareas de Windows.
2. Seleccione **Local Self Help**.

Aparece el cuadro de diálogo de bienvenida al asistente de Local Self Help, Local Self Help Wizard Welcome.

Por razones de seguridad, se le pedirá que introduzca su contraseña.

3. Especifique la contraseña y haga clic en **Siguiente**.

Se muestra el cuadro de diálogo Descripción del estado.

Este cuadro de diálogo proporciona una instrucción breve sobre cómo activar Local Self Help. Además, muestra información de estado (p. ej., el número de preguntas respondidas definidas por el usuario, el número de preguntas predefinidas respondidas, etc).

4. Haga clic en **Siguiente**.

- a) Si ha recibido y respondido varias preguntas predefinidas, aparecerá el cuadro de diálogo de preguntas predefinidas, en el que se muestran las preguntas contestadas.
- b) Si ha recibido varios temas de preguntas diferentes, puede elegir entre ellos los que desea mostrar en la lista desplegable del campo **Tema**.
- c) Para que aparezcan todos los temas en una lista continua, seleccione la opción **Todos los temas** (predeterminada) de la lista desplegable.

De forma predeterminada, las respuestas introducidas no se muestran como texto.

- d) Para que se muestre el texto introducido, marque la casilla **Mostrar respuestas**.
- e) Para cambiar las respuestas, haga clic en las preguntas pertinentes y escriba la nueva respuesta en la columna **Respuestas**.

5. Tras realizar los cambios, haga clic en **Siguiente**.

Si dispone de los permisos necesarios para definir sus propias preguntas, aparecerá el cuadro de diálogo Preguntas y respuestas definidas por el usuario. De forma predeterminada, las respuestas introducidas no se muestran como texto.

6. Para que se muestre el texto introducido, marque la casilla **Mostrar respuestas**.

- a) Para cambiar las respuestas existentes, haga clic en la preguntas pertinente y escriba la nueva respuesta en la columna **Respuestas**.
- b) Para agregar una nueva pregunta, haga clic en **Nueva pregunta**.

Se añadirá una nueva línea a la lista de preguntas. Escriba la pregunta en la columna **Preguntas** y la respuesta en la columna **Respuestas**.

- c) Para eliminar una pregunta, haga clic en la pregunta correspondiente y, a continuación, en **Eliminar pregunta**.

Aparecerá un mensaje en el que se le pide que confirme si desea eliminar la pregunta. Haga clic en **Sí**.

7. Tras realizar los cambios, haga clic en **Siguiente**.

El último cuadro de diálogo del asistente de Local Self Help muestra la nueva información de estado tras modificar las preguntas. Un mensaje le indica si se cumplen los requisitos previos necesarios para que Local Self Help permanezca activo.

8. Haga clic en **Finalizar**.

Se guardarán tanto las preguntas como las respuestas. Se mostrará un mensaje en el que se indica que el procedimiento de edición se ha realizado correctamente y que Local Self Help permanecerá activo.

9. Haga clic en **Aceptar**.

Las modificaciones entran en vigor

La próxima vez que inicie Local Self Help en la POA, las preguntas nuevas o modificadas se podrán seleccionar y visualizar de forma aleatoria. Se aplicarán las preguntas nuevas o modificadas.

**Nota:** Si el número de preguntas contestadas es inferior al número mínimo necesario como consecuencia de los cambios realizados, se mostrará un mensaje de advertencia en el último cuadro de diálogo del asistente de Local Self Help, en el que se indica que Local Self Help se desactivará una vez se haya cerrado el asistente.

**Nota:** Si no quiere que Local Self Help se desactive, puede volver a **Preguntas definidas por el usuario** y **Preguntas predefinidas** haciendo clic en el botón **Atrás**. A continuación, podrá agregar o responder nuevas preguntas. Si hace clic en **Finalizar** y el número de preguntas respondidas ha caído por debajo del mínimo necesario, aparecerá otro mensaje de advertencia en el que se indica que Local Self Help ya no está activo en su equipo. Sin embargo, en este caso, podrá reactivar Local Self Help (véase [Activación de Local Self Help](#), página 49).

## 7.4 Conexión en la POA mediante Local Self Help

Para conectarse en la POA mediante Local Self Help, debe responder a cinco preguntas seleccionadas aleatoriamente de entre las diez preguntas definidas.

Cómo conectarse a su equipo mediante Local Self Help en la POA:

1. Especifique el nombre de usuario en el cuadro de diálogo de conexión de la POA.

Se activará el botón **Recuperación**.

2. Haga clic en **Recuperación**.

- Si sólo se activa Local Self Help para la recuperación del inicio de sesión, se inicia Local Self Help.
- Si tanto el procedimiento de desafío/respuesta como Local Self Help están activados para la recuperación del inicio de sesión, aparecerá un cuadro de diálogo para seleccionar uno de los dos métodos de recuperación. Haga clic en **Local Self Help**.

Aparecerá el cuadro de diálogo de bienvenida Local Self Help Welcome.

Este cuadro de diálogo proporciona una breve descripción de los pasos siguientes.

3. Haga clic en **Siguiente** para comenzar a responder a las preguntas.

La primera pregunta aparecerá en el cuadro de diálogo Local Self Help - Pregunta 1 de 5.

4. Escriba la respuesta.

De forma predeterminada y por razones de seguridad, el texto introducido no aparece en el campo habilitado al efecto. Para que se muestre la respuesta, desactive la casilla **Ocultar respuesta**.



5. Tras responder a la pregunta, haga clic en **Siguiente**.

Solamente podrá hacer clic en **Siguiente** y continuar con la próxima pregunta tras haber escrito una respuesta.

6. A continuación, responda las otras cuatro preguntas. Cuando responda a la última, haga clic en **Aceptar**.

El siguiente cuadro de diálogo mostrará su contraseña actual.

7. Para visualizar la contraseña, pulse **Intro** o la **barra espaciadora**, o bien haga clic en el cuadro azul.

NO haga clic en **Aceptar**. Después de hacer clic en **Aceptar**, el proceso de arranque continuará SIN mostrar la contraseña.



La contraseña sólo se mostrará durante un máximo de cinco segundos. Después, el proceso de arranque continuará automáticamente.

**Nota:** Asegúrese por todos los medios de que ninguna persona no autorizada pueda ver el contenido de la pantalla (casualmente o a propósito). Puede ocultar inmediatamente la contraseña pulsando la barra espaciadora, Intro o haciendo clic en el cuadro azul.

8. Puede leer la contraseña y usarla para la conexión en la POA y de nuevo en Windows.
9. Tras leer la contraseña, haga clic en **Aceptar**. De lo contrario, el proceso de arranque continuará automáticamente transcurridos cinco segundos desde que aparezca la contraseña.

Ahora está conectado a la POA y a Windows.

## 7.5 Intentos de conexión fallidos

Si escribe una respuesta incorrecta en una o en varias preguntas, se produce un fallo en la conexión. En ese caso, aparece un mensaje en el que se indica que se ha producido un fallo en la conexión. Por razones de seguridad, Local Self Help no indica cuáles son las preguntas que se han respondido de manera incorrecta.

Un procedimiento de recuperación de Local Self Help fallido se considera como un intento de conexión fallido y se registra como evento. En este caso, se aplica un período de retraso en la conexión. El período de retraso en la conexión aumenta con cada intento de conexión fallido.

Si reinicia el equipo tras haberse producido un intento de conexión fallido y selecciona de nuevo la recuperación de inicio de sesión mediante Local Self Help, se volverán a seleccionar aleatoriamente cinco preguntas.

## 7.6 Reactivación de las preguntas y respuestas tras modificaciones en la contraseña en varios equipos

Si utiliza distintos equipos con Local Self Help activado y cambia su contraseña de Windows en uno de ellos, las preguntas y respuestas de Local Self Help ya no estarán activas en los otros equipos una vez que se haga efectivo el cambio de contraseña. Sin embargo, las preguntas y respuestas seguirán disponibles en el asistente de Local Self Help. Para utilizar el mismo conjunto de preguntas de nuevo en un segundo equipo, confírmelo mediante el asistente de Local Self Help.

Siga estos pasos:

1. Tras cambiar la contraseña en un equipo, conéctese al otro.

Una información sobre herramientas le indicará que hay preguntas de Local Self Help sin responder.

2. Haga clic con el botón derecho en el icono de la bandeja del sistema de SafeGuard Enterprise, que se encuentra en la barra de tareas de Windows y seleccione **Local Self Help**.

Aparecerá el cuadro de diálogo de bienvenida al asistente de Local Self Help.

3. Especifique la contraseña y haga clic en **Siguiente**.
4. Confirme todas las páginas del cuadro de diálogo del asistente de Local Self Help que se muestren a continuación con **Siguiente** y haga clic en **Finalizar** en la última.

Las preguntas y respuestas almacenadas anteriormente en el equipo están activas de nuevo y se utilizan al conectarse a la POA a través de Local Self Help.

## 8 Recuperación mediante el procedimiento de desafío/respuesta

Para la recuperación, SafeGuard Enterprise le ofrece un **procedimiento de desafío/respuesta** para intercambiar información de forma confidencial. El procedimiento de desafío/respuesta es muy seguro y eficaz:

Si utiliza SafeGuard Enterprise y, por poner un ejemplo, ha olvidado la contraseña, puede conseguir acceder de nuevo a su equipo con toda rapidez con la colaboración de un centro de ayuda.

**Nota:** Recomendamos usar principalmente Local Self Help para recuperar una contraseña olvidada. Al recuperarla mediante Local Self Help, se le puede mostrar la contraseña actual de forma confidencial en Power-on Authentication y puede seguir usando esta contraseña. Esto evitará que se tenga que restablecer la contraseña y también la necesidad de obtener asistencia del centro de ayuda.

Durante el procedimiento de desafío/respuesta, se genera un código de desafío (una cadena de caracteres ASCII) que debe proporcionar al personal del centro de ayuda. En función del código de desafío proporcionado, el responsable del centro de ayuda genera un código de respuesta que le autoriza a realizar una acción específica en el equipo.

## 8.1 Situaciones habituales en las que puede necesitar la asistencia del centro de ayuda

- Ha olvidado la contraseña.
- Ha escrito la contraseña de forma incorrecta demasiadas veces en el nivel de POA y el equipo se ha bloqueado.
- Ha olvidado o perdido el token/la tarjeta inteligente.
- La caché local de la POA (power-on authentication) está parcialmente dañada.
- Otro usuario tiene que arrancar el equipo protegido con SafeGuard Enterprise.
- Otro usuario tiene que arrancar el equipo protegido con SafeGuard Enterprise desde un medio externo.

## 8.2 Procedimientos para los que se puede solicitar una respuesta y situaciones pertinentes

- **Inicio del cliente de SafeGuard Enterprise sin conexión del usuario:** arrancar el equipo sin conexión del usuario puede ayudar si ha escrito incorrectamente la contraseña (por ejemplo, debido a errores de escritura, a que la tecla Bloq Mayús estaba activada, etc.) y, sin embargo, conoce la contraseña correcta. El procedimiento de desafío/respuesta le conectará a su ordenador sin restablecer la contraseña.

Si ha escrito varias veces la contraseña incorrecta, el centro de ayuda generará automáticamente un código de respuesta para arrancar el cliente sin la conexión del usuario (la situación se incluye en el desafío). Después, podrá volver a conectarse con su nombre de usuario y contraseña.

- **Inicio del cliente de SafeGuard Enterprise con conexión del usuario:** si ha olvidado la contraseña, solicite un desafío sin intentar especificar antes la contraseña. El centro de ayuda generará una respuesta para conectarse con o sin nombre de usuario. Al conectarse con su nombre de usuario, pida al centro de ayuda que se muestre su antigua contraseña durante el procedimiento de desafío/respuesta. Esto evitará que tenga que restablecer la contraseña. De lo contrario, si se conecta con su nombre de usuario, debe restablecer la contraseña para la conexión de Windows durante el procedimiento de desafío/respuesta.

**Nota:** Para los usuarios que trabajan sin conexión, es decir, sin estar conectados al controlador de dominio, hay que tener en cuenta algunas consideraciones especiales (véase [Desafío/respuesta para usuarios sin conexión](#), página 65).

■ **Restauración de la caché de directivas de SafeGuard Enterprise:**

Si la caché de directivas de SafeGuard sufre daños, este procedimiento es necesario. La caché local almacena todas las claves, directivas, certificados de usuario y archivos de auditoría. La recuperación de la conexión se desactiva, de forma predeterminada, cuando la memoria caché local presenta daños; esto es, se restaurará automáticamente a partir de la copia de seguridad. En este caso, no es necesario iniciar un procedimiento de desafío/respuesta para reparar la caché local. Sin embargo, la recuperación de la conexión se puede activar a través de una directiva, si es que la memoria caché local tiene que repararse explícitamente mediante un procedimiento de desafío/respuesta. En tal caso, se le solicitará automáticamente que inicie un procedimiento de desafío/respuesta si la caché local está dañada.

■ **Arranque desde un medio externo o disquete:** el procedimiento de desafío/respuesta también se puede usar para permitir que el equipo arranque desde un medio externo. Para ello, seleccione la opción **Continuar inicio desde: disquete/medio externo** en el cuadro de diálogo de conexión de la POA e inicie el procedimiento de desafío/respuesta. Ahora, el centro de ayuda podrá generar una respuesta para las acciones siguientes:

- Iniciar el cliente SGN con conexión del usuario
- Iniciar el cliente SGN sin conexión del usuario
- Permitir el procedimiento de arranque desde medios externos

## 8.3 Procedimiento de desafío/respuesta

1. Se inicia la POA (power-on authentication).

A partir de la generación del desafío, hay disponible un período de tiempo de 30 minutos para especificar correctamente la respuesta que ha generado el centro de ayuda en un procedimiento de desafío/respuesta. A los 30 minutos, el código de respuesta dejará de ser válido y no se podrá utilizar.

2. Solicitud de un desafío:

El usuario abre el cuadro de diálogo de desafío/respuesta en la POA. Se generará y aparecerá un código de desafío en forma de cadena de caracteres ASCII.

3. Póngase en contacto con el centro de ayuda.

Transmítale sus datos de usuario (Id. de usuario, Id. de equipo, etc.) tal como se muestra en el cuadro de diálogo de Desafío, así como el código de desafío.

4. El centro de ayuda generará un código de respuesta a través de SafeGuard Management Center

5. El centro de ayuda le proporciona el código de respuesta mediante una llamada de teléfono o un mensaje SMS.

6. Escriba el código de respuesta en la POA.

Ahora puede llevar a cabo la acción para la cual está autorizado. Por ejemplo, restablecer la contraseña.

Ya puede retomar el trabajo.

## 8.4 Solicitud de un desafío

1. En el cuadro de diálogo de la conexión en la POA, haga clic en **Recuperación**.

El botón **Recuperación** sólo se activará al especificar un nombre de usuario o, al menos, un carácter en el cuadro de diálogo del número PIN.

**Nota:** Si ha especificado una contraseña o número PIN incorrectos demasiadas veces, o bien si la caché de directivas tiene daños, SafeGuard Enterprise le informará automáticamente y se ofrecerá para solucionar el problema mediante un procedimiento de desafío/respuesta.

Aparecerán sus datos de usuario y un código de desafío generado aleatoriamente. Para facilitar su lectura, el código de desafío se divide en bloques de cinco caracteres.

Desafío/Respuesta - Paso 2 de 3

**SOPHOS**

Si ha olvidado la contraseña, puede llamar al servicio de soporte para recibir una contraseña de uso único.

Dominio del usuario: MY\_COMPANY

ID del usuario:

Dominio del ordenador: MY\_COMPANY.EDU

ID del ordenador: XP\_ES

Desafío: JA7K3 WFIDC AS1S6 LLUNF U2PEI ULJRY

Este desafío caducará en: 14:46 minuto

Anterior Próximo Cancelar Deletrear

2. Póngase en contacto con el centro de ayuda de SafeGuard Enterprise y proporcione sus datos de usuario, así como el código de desafío a la persona responsable.

Para facilitar el proceso de indicación del código de desafío, puede visualizar una ayuda para deletrearlo haciendo clic en **Ayuda a la ortografía**.

El responsable del centro de ayuda podrá identificar la situación para la que desea el código de respuesta del código de desafío.

3. Haga clic en **Siguiente**.

## 8.5 Introducción de la respuesta

1. Especifique en el cuadro de diálogo de respuesta el código de respuesta que le ha proporcionado el responsable del centro de ayuda y confírmelo haciendo clic en **Aceptar**. Si introduce incorrectamente el código de respuesta, se resaltará en color rojo el grupo de caracteres que contenga el error.
2. Ha iniciado sesión en la POA.

Si es necesario, SafeGuard Enterprise le solicitará que cambie las credenciales de usuario de Windows.

## 8.6 Prácticas recomendadas

### 8.6.1 Ha escrito una contraseña incorrecta demasiadas veces

1. Ha especificado una contraseña incorrecta demasiadas veces en la POA (power-on authentication) (por ejemplo, porque la ha escrito mal, ha activado la tecla **Bloq mayús**, etc.), sin embargo sí conoce la contraseña correcta. Está conectado al dominio.
2. El PC está bloqueado y se le solicita que inicie un procedimiento de desafío/respuesta para desbloquearlo.
3. El responsable del centro de ayuda genera una respuesta para arrancar sin conexión del usuario.
4. Arrancar sin conexión del usuario significa que no tiene que cambiar la contraseña para conectarse a Windows. Aparecerá el cuadro de diálogo de conexión de Windows. Escriba la contraseña de Windows aquí y se conectará al sistema.
5. El contador del número máximo de intentos de introducción de contraseña permitidos se pone a cero.

También puede solicitar una respuesta con conexión de usuario. En ese caso, se le solicitará que cambie las credenciales de Windows antes de conectarse a Windows.

## 8.6.2 Ha olvidado la contraseña

Le recomendamos usar principalmente los siguientes métodos para recuperar una contraseña olvidada a fin de evitar que se tenga que restablecer la contraseña centralmente:

- Use Local Self Help. Con la recuperación mediante Local Self Help, se le puede mostrar la contraseña actual y puede seguir usando esta contraseña sin tener que restablecerla y sin necesidad de obtener asistencia del centro de ayuda. Para obtener más información, consulte [Recuperación mediante Local Self Help](#), página 49.
- Al usar el procedimiento de desafío/respuesta: Pida al centro de ayuda que genere una respuesta con conexión de usuario y que se muestre su antigua contraseña durante el procedimiento de desafío/respuesta. Esto evitará que tenga que restablecerla. Puede seguir trabajando con la antigua contraseña y modificarla de forma local posteriormente, si lo desea.

Si no se pueden aplicar los métodos anteriores, proceda de la siguiente manera:

1. Si ha olvidado la contraseña, recibirá una respuesta para iniciar el equipo mediante la conexión de usuario. En ese caso, tendrá que cambiar la contraseña al conectarse a Windows (siempre que se pueda acceder al dominio).
2. Después de cambiar la contraseña, utilice la contraseña nueva para conectarse en la POA (power-on authentication).

## 8.6.3 Ha olvidado o perdido el token

En este caso, se tiene que llevar a cabo el procedimiento de desafío/respuesta con conexión del usuario.

1. Durante el procedimiento de desafío/respuesta, se le solicitará que cambie la contraseña. El cuadro de diálogo para cambiar la contraseña se mostrará solamente si se establece una conexión con el controlador de dominio.
2. Si es obligatoria la conexión con un token y un PIN; puede decidir si desea cambiar la contraseña o bien omitir el cambio de contraseña haciendo clic en **Cancelar**.
  - **Ha olvidado el token**

Seguir el método de omitir el cambio de la contraseña mediante un clic en **Cancelar** en el cuadro de diálogo solamente tiene sentido si ha olvidado su token pero sí dispondrá de él para conexiones futuras. Tras hacer clic en **Cancelar**, se conectará al sistema y podrá seguir usando el equipo.

Sin token, sólo puede conectarse a través de la opción Desafío/respuesta de la POA. Una vez que vuelva a tener su token, podrá conectarse con él a la POA.

- **Ha perdido el token**

Si ha perdido el token, especifique una contraseña nueva en el cuadro de diálogo para cambiar la contraseña. Se conectará a Windows con esta contraseña. Si las directivas del equipo se lo permiten (no es obligatoria la conexión de token a la POA), también puede conectarse en la POA usando esta contraseña.

Así puede descartar que alguien encuentre el token y lo utilice sin autorización. Los usuarios sin autorización no podrán utilizar el token para conectar, incluso aunque sepan el número PIN, ya que su contraseña habrá cambiado.

#### **8.6.4 Ha olvidado el número PIN**

1. Si ha olvidado el número PIN del token, solicite una respuesta y especifique una contraseña nueva. Se conectará a Windows con esta contraseña, que también puede utilizar para conectarse en la POA, siempre que tenga la autorización necesaria para conectarse utilizando contraseña.
2. Un responsable de seguridad tiene que asignar un número PIN nuevo al token y almacenar los nuevos datos de conexión en él. Después, puede utilizarlo para volver a conectarse.

#### **8.6.5 Ya no puede acceder a su equipo**

Si ya no le es posible acceder al equipo, tal vez se deba a que la POA esté dañada. Incluso en esta situación tan preocupante, SafeGuard Enterprise le ofrece un procedimiento de desafío/respuesta con la colaboración del centro de ayuda, que le permitirá volver a acceder a sus unidades cifradas. El procedimiento de desafío/respuesta en este caso se realiza a través de un entorno WinPE. Si se encuentra en una situación de cariz tan preocupante, le recomendamos que se ponga en contacto con su centro de ayuda de SafeGuard Enterprise. La persona responsable del centro de ayuda le proporcionará los archivos necesarios y le guiará por los pasos necesarios para conseguir acceder de nuevo a su equipo.

### **8.7 Desafío/respuesta para usuarios sin conexión**

Hay algunos detalles relevantes a la hora de utilizar el procedimiento de desafío/respuesta por parte de los usuarios sin conexión. Los usuarios sin conexión (es decir, los que no están conectados al controlador del dominio) no pueden iniciar un cambio de contraseña durante el procedimiento de desafío/respuesta.

### 8.7.1 Desafío/respuesta para usuarios sin conexión con modo de conexión con nombre de usuario/contraseña

#### Ejemplo:

Está trabajando sin conexión (es decir, no está conectado al controlador de dominio) y ha olvidado la contraseña. A través del procedimiento de desafío/respuesta puede volver a obtener acceso rápida y fácilmente a su equipo.

SafeGuard Enterprise también le puede conectar a Windows automáticamente durante el procedimiento de desafío/respuesta. Sin embargo, como después de este procedimiento no conocería la contraseña, tendría que repetirlo cada vez que iniciase el equipo. Además, no podría desbloquear el equipo si se bloqueara (p.ej. en el caso de que quedase bloqueado al activarse el protector de pantalla). En ese caso, tendría que reiniciar el equipo, lo que supondría el peligro de pérdida de datos (y volver a iniciar un procedimiento de desafío/respuesta).

**Nota:** Éste es el motivo por el que SafeGuard Enterprise ofrece la posibilidad de mostrar la contraseña durante un procedimiento de desafío/respuesta. Los usuarios sin conexión deberían visualizar siempre su contraseña durante los procedimientos de desafío/respuesta. Indique al responsable del centro de ayuda que le gustaría ver su contraseña. El responsable del centro de ayuda tiene que activar explícitamente la visualización de la contraseña antes de generar el código de respuesta.

Proceda de la siguiente forma:

1. Inicie el procedimiento de desafío/respuesta, para lo que debe hacer clic en **Recuperación** en el cuadro de diálogo de conexión de POA.
2. Llame al centro de ayuda y comunique su desafío.
3. Indique al responsable que le gustaría arrancar el equipo con la conexión de usuario y que desea ver su contraseña.
4. Haga clic en **Siguiente** en el cuadro de diálogo de desafío/respuesta y especifique la respuesta.
5. Haga clic en **Aceptar**.

6. Se le preguntará si la contraseña antigua debe aparecer en pantalla.



7. Responda **Sí** y haga clic en **Aceptar**.
8. El siguiente cuadro de diálogo le informa de que la contraseña se mostrará cuando pulse **Intro** o la **barra espaciadora** del teclado, o bien cuando haga clic en el texto.

**No** haga clic en **Aceptar**. Después de hacer clic en **Aceptar**, el proceso de arranque continuará SIN mostrar la contraseña.

La contraseña se mostrará durante cinco segundos. Después, el proceso de arranque continuará automáticamente.

9. Pulse **Intro** o la **barra espaciadora** del teclado, o bien haga clic en el texto.

Se mostrará la contraseña.

**Nota:** Asegúrese por todos los medios de que ninguna persona no autorizada pueda ver el contenido de la pantalla (casualmente o a propósito). Puede ocultar inmediatamente la contraseña pulsando la **barra espaciadora**, **Intro** o haciendo clic con el ratón. La contraseña sólo se mostrará durante un máximo de cinco segundos.



10. Puede leer la contraseña y usarla para la conexión en la POA o y en Windows.

Ya puede volver a trabajar con el equipo.

### 8.7.2 Desafío/respuesta para usuarios sin conexión con modo de conexión con "Sólo token"

En este caso, si ha olvidado el número PIN o ha olvidado o perdido el token, el procedimiento que se va a utilizar dependerá de si conoce las credenciales de Windows.

#### ■ Conoce las credenciales de Windows

a) Si conoce las credenciales de Windows, inicie el procedimiento de desafío/respuesta tal como se ha descrito. Se conectará automáticamente a Windows y podrá utilizar su equipo.

El modo de conexión "Sólo token" se restablecerá durante todo el tiempo que dure la sesión de trabajo después del procedimiento de desafío/respuesta. Por consiguiente, también podrá conectarse a Windows con el nombre de usuario y la contraseña.

En el caso de que deba bloquearse el equipo, podrá desbloquearlo especificando la contraseña de Windows. Sin embargo, la conexión en la POA sólo será posible a través del procedimiento de desafío/respuesta.

#### ■ No conoce las credenciales de Windows

a) Aunque no conozca las credenciales de Windows y haya olvidado el número PIN, también puede iniciar un procedimiento de desafío/respuesta en el que se muestre su contraseña.

b) Indique al responsable del centro de ayuda que la contraseña debería mostrarse.

Como el modo de conexión "Sólo token" se desactivará, también podrá desbloquear el equipo en caso de se bloquee usando esta contraseña.

Sin embargo, la conexión en la POA sólo será posible a través del procedimiento de desafío/respuesta.

## 9 Icono de la bandeja del sistema e información sobre herramientas

Puede acceder fácilmente a todas las funciones importantes del cliente de SafeGuard Enterprise en su equipo. El icono de la bandeja del sistema de SafeGuard Enterprise se coloca en la barra de tareas de Windows para permitir el acceso a estas funciones.

**Nota:** El security officer define el comportamiento del icono de la bandeja del sistema en el equipo. El security officer especifica en una directiva si el icono aparece en el equipo. También se puede establecer en modo "silencioso". En ese caso, en el equipo no se mostrará la información sobre herramientas en forma de globo.

A través del icono de la bandeja del sistema puede visualizar información o realizar acciones concretas. Al hacer clic en el icono con el botón derecho del ratón, hará que se muestre un menú con las siguientes entradas:

- **Mostrar:**

- **Juego de claves:** muestra todas las claves que tiene a su disposición.
- **Certificado:** muestra la información relativa a su certificado.

- **Crear nueva clave:** abre un cuadro de diálogo para crear una clave nueva para su uso en el intercambio de datos mediante un medio extraíble (véase [SafeGuard Data Exchange](#), página 82).

- **Local Self Help**

Si se ha activado Local Self Help para su equipo mediante la directiva correspondiente, el comando Local Self Help aparece en el menú contextual del icono de la bandeja del sistema. Puede iniciar el asistente de Local Self Help mediante este comando. Local Self Help es un método de recuperación del inicio de sesión que no precisa la ayuda del servicio de asistencia. Para obtener más información acerca de Local Self Help, véase [Recuperación mediante Local Self Help](#), página 49.

- **Cambiar contraseña de acceso al medio:** abre un cuadro de diálogo para crear una clave nueva para su uso en el intercambio de datos mediante un medio extraíble (véase [SafeGuard Data Exchange](#), página 82).
- **Sincronizar:** inicia la sincronización de datos con el servidor de SafeGuard Enterprise. La información sobre herramientas muestra el progreso y el resultado de la sincronización de datos.

**Nota:** La sincronización también se puede iniciar haciendo doble clic en el icono de la bandeja del sistema.

- **Estado:** proporciona un cuadro de diálogo que ofrece información sobre el estado actual del equipo protegido con SafeGuard Enterprise:

Campo	Información
<b>Última directiva recibida</b>	Muestra la fecha y la hora en que el equipo recibió una directiva nueva por última vez.
<b>Última clave recibida</b>	Muestra la fecha y la hora en que el equipo recibió una clave nueva por última vez.
<b>Último certificado recibido</b>	Muestra la fecha y la hora en que el equipo recibió un certificado nuevo por última vez.
<b>Último contacto con el servidor</b>	Muestra la fecha y la hora del último contacto con el servidor.
<b>Estado de usuario de SGN</b>	<p>Muestra el estado del usuario que está conectado al equipo (conexión con Windows):</p> <ul style="list-style-type: none"> <li>■ <b>Pendiente</b> La replicación del usuario en la POA está pendiente; es decir: aún no ha finalizado la sincronización inicial del usuario. Esta información es especialmente importante después de la primera conexión a SafeGuard Enterprise, ya que sólo puede conectarse a la POA después de que se haya completado la sincronización inicial del usuario.</li> <li>■ <b>Usuario SGN</b> Se ha asignado el usuario a la instalación de SafeGuard Enterprise como un usuario de SafeGuard Enterprise.</li> <li>■ <b>Invitado de SGN</b> El usuario que está conectado a Windows es un usuario invitado de SafeGuard Enterprise. Al usuario se le permite que se conecte a Windows sin asignarlo a este equipo protegido con SafeGuard Enterprise en calidad de usuario de SafeGuard Enterprise.</li> <li>■ <b>Invitado de SGN (cuenta de servicio)</b> El usuario conectado a Windows es un usuario invitado de SafeGuard Enterprise que se ha conectado mediante una cuenta de servicio para tareas de administración.</li> <li>■ <b>Desconocido</b> Indica que no se ha podido determinar el estado del usuario.</li> </ul>

Campo	Información
<b>Estado de la memoria caché de la directiva Paquetes de datos preparados para la transmisión</b>	Indica si hay algún paquete que enviar al servidor de SafeGuard Enterprise.
<b>Estado de Local Self Help (LSH) Habilitado Activo</b>	Indica si Local Self Help se ha habilitado mediante una directiva y si el usuario lo ha activado en el equipo. Para obtener más información acerca de Local Self Help, véase <a href="#">Recuperación mediante Local Self Help</a> , página 49.

- **Ayuda:** abre la ayuda en línea de SafeGuard Enterprise.
- **Acerca de SafeGuard Enterprise:** muestra información acerca de la versión de SafeGuard Enterprise.

## 10 Extensiones del explorador de SafeGuard

Puede acceder a funciones relativas al cifrado mediante las correspondientes entradas en los menús contextuales del Explorador de Windows.

### 10.1 Extensiones del explorador para el cifrado basado en archivos

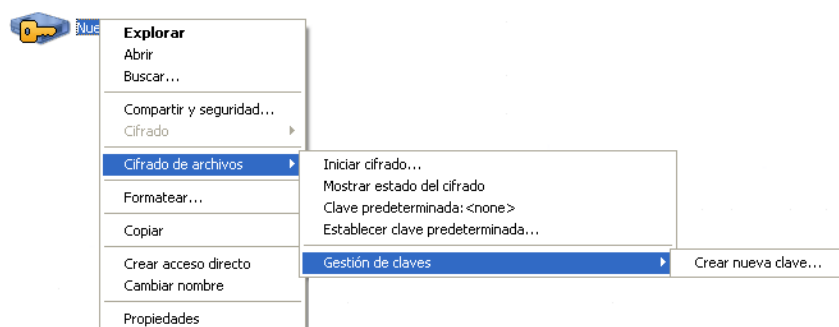
Para poder acceder a las funciones de cifrado basado en archivos, debe utilizar las entradas correspondientes de los menús contextuales del Explorador de Windows. Las funciones están disponibles en los menús contextuales de

- volúmenes
- medios extraíbles
- directorios
- archivos

La entrada **Cifrado de archivos** se agrega al menú contextual. Para acceder a las funciones individuales, utilice este menú.

Si ninguna de las directivas de cifrado basado en archivos es aplicable al volumen seleccionado, sólo es posible determinar el estado de cifrado y visualizar el cuadro de diálogo para generar claves desde el menú contextual.

Si alguna de las directivas de cifrado basado en archivos es aplicable al volumen, al medio extraíble, al directorio o al archivo seleccionado, se agregan las siguientes entradas al menú contextual:



**Nota:** Las funciones que se muestran dependen de la configuración definida en las directivas. Además, dependen de si la función pertinente está disponible para el volumen seleccionado. El ámbito de la función varía dependiendo de si en el volumen pertinente se ha utilizado cifrado basado en archivos o basado en volúmenes.

Están disponibles las siguientes funciones:

- **Iniciar cifrado:** si selecciona esta opción en el menú contextual de un volumen, todos los archivos se podrán cifrar o volver a cifrar.
- **Mostrar estado de cifrado:** indica si se ha cifrado un volumen, medio extraíble o archivo, qué clave se ha utilizado, si la clave está incluida en su juego de claves y si tiene acceso a este archivo.
- **Descifrar:** descifra el volumen o archivo seleccionado.
- **Clave predeterminada:** muestra la clave actualmente usada para los archivos nuevos agregados al volumen (al guardar, copiar o mover). La clave estándar de cada volumen individual o medio extraíble se puede definir por separado.
- **Establecer clave predeterminada:** abre un cuadro de diálogo para seleccionar una clave predeterminada diferente.
- **Gestión de claves: Crear nueva clave:** abre un cuadro de diálogo para crear claves locales definidas por el usuario.

## 10.2 Extensiones del explorador para el cifrado basado en volúmenes

La entrada **Cifrado** se añade al menú contextual del Explorador de Windows.

Si el volumen está cifrado, aparece el símbolo de una llave junto a la entrada del menú. Si se muestra el símbolo de una llave verde, significa que tiene las claves necesarias y puede acceder al volumen.

**Nota: Cifrado de > Mostrar estado de cifrado** muestra el estado de cifrado de los archivos en el volumen desde el punto de vista del cifrado basado en archivos. Los archivos de un volumen cifrado también se pueden cifrar de forma que se basen en archivos. En ese caso, aparecerá el cuadro de diálogo correspondiente.

### 10.2.1 Agregar o quitar claves

Es posible agregar claves al volumen cifrado (o quitárselas), siempre que la configuración especificada en las directivas correspondientes así lo permita. Al hacerlo, los propietarios de la clave pertinente tendrán acceso a los datos cifrados de este volumen.

Puede asignar claves al volumen mediante el cuadro de diálogo **Propiedades** del volumen. Este cuadro de diálogo incluye la ficha Cifrado (hacer clic con el botón derecho en **Volumen > Propiedades > Cifrado**).

Seleccione una clave en la lista inferior y haga clic en **Agregar clave**. El archivo se desplazará hacia arriba en la lista de selección de claves. Está incluido en la lista de claves que se pueden utilizar para tener acceso al volumen cifrado.

Con la opción **Quitar clave** puede eliminar la clave de la lista de claves utilizadas para acceder a los medios.

## 11 Cifrado de datos

SafeGuard Enterprise cifra datos en un equipo, ya sea basándose en volúmenes o en archivos. En las directivas de seguridad, el security officer define los volúmenes (unidades) que deben cifrarse.

### 11.1 Cifrado inicial para el cifrado basado en archivos

Si una directiva que estipula el cifrado de archivos se aplica a una ubicación del equipo, en el Explorador de Windows aparecerá el símbolo de una llave amarilla al lado de los archivos correspondientes.

El símbolo de la llave amarilla por sí solo no indica necesariamente que ya se han cifrado todos los archivos de la unidad. Primero se tiene que realizar un cifrado inicial.

Si se estipula el cifrado de los archivos, el cifrado inicial se iniciará automáticamente, o bien tendrá que iniciar manualmente el proceso.

### 11.2 Cifrado transparente

Los archivos de las unidades cifradas se cifran de forma transparente. No verá ninguna solicitud ni mensaje sobre el cifrado o descifrado al abrir, editar y guardar archivos. Al abrir los archivos, se descifrarán y podrá editarlos. Al cerrar o guardar los archivos, se volverán a cifrar.

Si copia o mueve archivos (también a través de Guardar como) de una unidad cifrada a otra ubicación de archivos del equipo sin cifrado, se descifrarán. Los archivos se almacenarán en la nueva ubicación en forma de texto simple.

## 11.3 Restricciones para el cifrado inicial de equipos protegidos con SafeGuard Enterprise

La configuración inicial de los equipos protegidos con SafeGuard Enterprise puede implicar la creación de directivas de cifrado que puedan distribuirse dentro de un paquete de configuración a equipos.

Sin embargo, si el cliente de SafeGuard Enterprise no se conecta a un servidor de SafeGuard Enterprise inmediatamente después de instalar el paquete de configuración, sino que temporalmente está sin conexión, solamente las directivas de cifrado con esta configuración en concreto se activarán inmediatamente en el equipo protegido con SafeGuard Enterprise:

- Protección del dispositivo basada en volúmenes, utilizando la clave de equipo definida como clave de cifrado

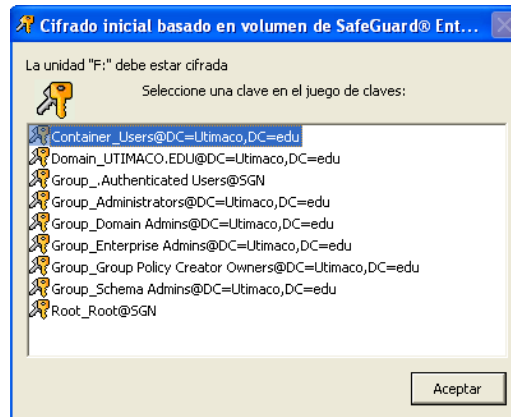
Para que se activen todas las demás directivas que impliquen cifrado con claves definidas por el usuario en el equipo protegido con SafeGuard Enterprise, también se deberá reasignar al equipo el paquete de configuración correspondiente. Entonces, las claves definidas por el usuario solamente se crearán una vez que el cliente de SafeGuard Enterprise se conecte de nuevo al servidor SafeGuard Enterprise.

Esto es así debido a que la clave de equipo definida se crea en el equipo protegido con SafeGuard Enterprise tras reiniciarlo por primera vez después de la instalación, mientras que las claves definidas por el usuario solamente se pueden crear en el equipo una vez que se ha registrado en el servidor SafeGuard Enterprise.

## 11.4 Cifrado basado en volúmenes

El cifrado basado en volúmenes de los discos del equipo protegido con SafeGuard Enterprise se inicia automáticamente, siempre que el security officer haya definido la directiva para que lo haga.

1. Aparecerá un cuadro de diálogo y se le solicitará que seleccione una clave que le permita acceder al volumen.



**Nota:** Todos los usuarios cuyo juego de claves incluya ésta podrán acceder a este volumen. El security officer define el ámbito de las claves que se ofrecen. Si el security officer ha definido una clave específica, no podrá seleccionar ninguna clave.

2. Al hacer clic en **Aceptar**, se iniciará el cifrado.

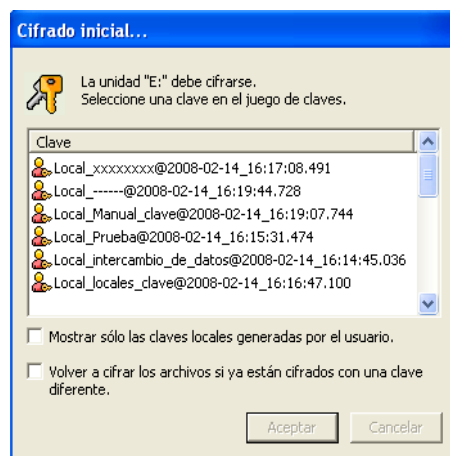
Durante el proceso de cifrado, un visor de cifrado muestra el progreso del cifrado. Dicho visor aparecerá minimizado en la barra de tareas de Windows. Para mostrar el visor de cifrado, no hay más que hacer clic en el icono. Si desea minimizar el visor de cifrado, puede solicitar una notificación de que el cifrado se ha completado si activa la opción **Mostrar notificación antes de cerrar**. El visor se cerrará automáticamente al finalizar el cifrado. El volumen cifrado se puede utilizar como cualquiera de los volúmenes no cifrados del equipo.

**Nota:** Para Windows 7 Professional, Enterprise y Ultimate, se ha creado una partición del sistema en los equipos de usuario sin una letra de unidad asignada. SafeGuard Enterprise no puede cifrar esta partición del sistema.

## 11.5 Cifrado basado en archivos

El cifrado de un volumen o bien se inicia automáticamente o tendrá usted que iniciar el proceso.

1. Si el cifrado no comienza de forma automática, seleccione **Cifrado de archivo > Iniciar cifrado**.
2. Si el security officer no ha definido ninguna clave específica, se mostrará un cuadro de diálogo en ambos casos, en el que se le solicitará que seleccione una clave que le permita acceder a este volumen.



**Nota:** Todos los usuarios cuyo juego de claves incluya ésta podrán acceder a este volumen. El security officer ámbito de las claves que se ofrecen. Si el security officer ha definido una clave específica, no podrá seleccionar ninguna clave.

**Nota:** Para intercambiar datos con los usuarios que tengan SafeGuard Enterprise instalado en su equipo, pero que no utilicen la misma clave, por lo general se requieren **claves locales generadas por el usuario**. Estas claves también son necesarias para proteger el intercambio de datos con usuarios que no utilicen SafeGuard Enterprise. Puede identificar las claves locales por su prefijo (Local\_).

**Nota:** Si la opción **Volver a cifrar los archivos si ya están cifrados con una clave diferente** está activada, los archivos cifrados, para los que existe una clave, se descifrarán y se volverán a cifrar usando la nueva clave.

3. Seleccione una clave y haga clic en **Aceptar**.

Se cifrarán todos los datos del volumen correspondiente.

### 11.5.1 Cómo definir una clave predeterminada

Mediante la definición de una clave predeterminada, especifica la clave que se va a utilizar para el cifrado durante el funcionamiento del sistema.

1. La clave predeterminada se puede definir a través del menú contextual de un archivo de un volumen, o bien a través del menú contextual del propio medio extraíble.
2. Para mostrar un cuadro de diálogo para la selección de claves, seleccione **Cifrado de archivos > Establecer clave predeterminada**.

La clave que seleccione se utilizará para todos los procesos de cifrado del volumen posteriores.

3. Si desea utilizar otra clave, defina una clave predeterminada nueva.

### 11.5.2 Estado del cifrado

En los volúmenes cifrados basados en archivos, los archivos individuales se marcan mediante símbolos de llaves de distintos colores. Los colores de las llaves indican el estado del cifrado.

- **Llave verde:** el archivo se cifra y se puede acceder a él.
- **Llave gris:** se aplica una directiva de cifrado al archivo. Sin embargo, aún no está cifrado.
- **Llave roja:** el archivo se cifra con una clave que no se incluye en su juego de claves. No tiene acceso a él.

El estado de cifrado de un archivo también se puede ver a través de su menú contextual. Al seleccionar **Cifrado de archivos > Mostrar estado de cifrado**, puede abrir una ventana mostrando el estado de cifrado.

Si selecciona **Cifrado de archivos > Estado de cifrado** en el menú contextual del propio volumen, se mostrará un cuadro de diálogo mostrando todos los archivos y sus estados de cifrado.

## 11.6 Restricciones de acceso a volúmenes

SafeGuard Enterprise impide acceder a los volúmenes en los casos siguientes:

### 11.6.1 Volúmenes con un cifrado fallido

Si existe una directiva que define que se debe cifrar un volumen o un tipo de volumen y se producen errores en el proceso de cifrado, se impedirá el acceso a ese volumen o volúmenes.

Cuando intente acceder al volumen, aparecerá un mensaje al respecto.

### **11.6.2 Objetos del sistema de archivos no identificados**

Los objetos del sistema de archivos no identificados son volúmenes que no se pueden identificar con claridad como archivos simples ni se pueden cifrar con SafeGuard Enterprise.

Si hay una directiva que defina que un volumen de este tipo se debe cifrar, se impedirá el acceso a este volumen. Cuando intente acceder al volumen, aparecerá un mensaje al respecto.

Si no hay ninguna directiva de cifrado para los objetos del sistema de archivos no identificados, será posible acceder al volumen.

## 12 SafeGuard Data Exchange

Con SafeGuard Data Exchange puede cifrar los datos almacenados en medios extraíbles conectados a su equipo e intercambiarlos con otros usuarios. Todos los procesos de cifrado y descifrado se ejecutan de forma transparente e implican una interacción mínima del usuario.

Sólo los usuarios que dispongan de las claves apropiadas podrán visualizar el contenido de los datos cifrados. Todos los procesos de cifrado posteriores se ejecutan de forma transparente. Cifrado transparente significa que los datos que se han cifrado y guardado los descifra automáticamente una aplicación al volver a acceder a ellos.

Al guardar el archivo pertinente, éste se volverá a cifrar automáticamente. En el trabajo del día a día, no notará que los datos están cifrados. Sin embargo, al desconectar los medios extraíbles, los datos permanecerán cifrados y estarán protegidos contra el acceso no autorizado. Los usuarios no autorizados pueden acceder a los archivos físicamente, pero no pueden leerlos sin SafeGuard Data Exchange y la clave pertinente.

**Nota:** El comportamiento de SafeGuard Data Exchange en su equipo lo define centralmente el security officer.

En la administración central, el security officer define cómo se tratan los datos de los medios extraíbles. Por ejemplo, el security officer puede definir que es obligatorio cifrar los archivos almacenados en los medios extraíbles. En este caso, todos los archivos sin cifrar presentes en el medio se cifran en principio. Además, se cifran todos los archivos nuevos guardados en medios extraíbles. Si los archivos existentes no se van a cifrar, el security officer puede decidir si se permite el acceso a los archivos no cifrados existentes. En ese caso, SafeGuard Data Exchange no procede a cifrar los archivos no cifrados presentes. Sin embargo, sí se cifran los archivos nuevos. Por tanto, puede leer y editar los archivos no cifrados existentes, pero se cifrarán en cuanto les cambie el nombre. Como alternativa, no se le permitirá acceder a los archivos sin cifrar y éstos seguirán estando sin cifrar.

Hay dos métodos posibles para intercambiar los archivos cifrados almacenados en los medios extraíbles:

- Se instala **SafeGuard Enterprise** en el equipo del destinatario: puede usar las claves disponibles para ambos (usted y el destinatario) o puede crear una nueva. Si genera una clave nueva, tiene que proporcionar el destinatario de los datos con la frase de contraseña para la clave.
- **SafeGuard Enterprise no** se instala en el equipo del destinatario: SafeGuard Enterprise le ofrece SafeGuard Portable. Esta utilidad se puede copiar automáticamente a los medios extraíbles, junto con los archivos cifrados. Mediante el empleo de SafeGuard Portable y la frase de contraseña pertinente, el destinatario puede descifrar los archivos cifrados y volver a cifrarlos sin necesidad de instalar SafeGuard Data Exchange en su equipo.

## 12.1 Una única contraseña de acceso al medio para todos los dispositivos extraíbles conectados al equipo

En SafeGuard Data Exchange es posible definir una única contraseña de acceso al medio para acceder a todos los dispositivos extraíbles conectados a su equipo. Esta característica es independiente de la clave utilizada para el cifrado de archivos individuales.

Si se especifica, se puede autorizar el acceso a los archivos cifrados indicando una única contraseña de acceso al medio para todos los medios. La contraseña de acceso al medio está vinculada a los equipos para los que tenga permiso de acceso. Esto significa que puede utilizar la misma contraseña en todos ellos.

La contraseña de acceso al medio se puede modificar y se sincronizará automáticamente en cada equipo en el que esté trabajando, desde el momento en que conecte un medio extraíble.

Es aconsejable especificar una contraseña de acceso al medio en las siguientes situaciones:

- Desea utilizar datos cifrados de medios extraíbles también en equipos en los que SafeGuard Enterprise no está instalado (SafeGuard Data Exchange en combinación con SafeGuard Portable).
- Desea intercambiar datos con usuarios externos: Si les proporciona la contraseña de acceso al medio, obtendrán acceso a todos los archivos de los medios extraíbles con una única contraseña de acceso, independientemente de la clave utilizada para el cifrado de los archivos individuales.

También puede restringir el acceso a todos los archivos proporcionando al usuario externo sólo la contraseña de acceso al medio de una clave determinada (denominada clave local, que puede crear un usuario de SafeGuard Data Exchange). En este caso, el usuario externo sólo tendrá acceso a los archivos cifrados con esta clave y no podrá visualizar los demás archivos.

**Nota:** No es necesario especificar una contraseña de acceso al medio si utiliza claves de grupo de SafeGuard Enterprise para intercambiar datos de medios extraíbles en un grupo de trabajo cuyos miembros comparten dicha clave.

**Nota:** En ese caso, si así lo establece el security officer, se podrá acceder sin ningún problema a los archivos cifrados de medios extraíbles. No es necesario especificar una contraseña o contraseña de acceso al medio.

**Nota:** Esto se debe a que las claves de grupo y las frases de contraseña para medios extraíbles se pueden utilizar simultáneamente. Ya que el sistema detecta de manera automática si hay una clave de grupo disponible, los usuarios que compartan dicha clave tendrán total acceso. Si no se detecta ninguna clave de grupo, SafeGuard Data Exchange mostrará un cuadro de diálogo y le solicitará al usuario que introduzca la contraseña de acceso al medio o la frase de contraseña de una clave local.

Si SafeGuard Data Exchange está instalado en su equipo, el security officer predefinirá cómo se tratarán los medios extraíbles. Un security officer puede definir la siguiente configuración del comportamiento para SafeGuard Data Exchange (también es posible una combinación de varias configuraciones):

- **Cifrado inicial de todos los archivos:** En este caso, el cifrado de todos los datos contenidos en el medio extraíble comenzará tan pronto como se conecte el dispositivo al equipo. Esta configuración asegura que los medios extraíbles sólo contienen datos cifrados. Al comenzar el cifrado, se le pedirá que seleccione una clave, o bien se usará una clave predefinida.
- **Se le permite cancelar el cifrado inicial:** cuando comience el cifrado inicial, se muestra un cuadro de diálogo que le permite cancelar el cifrado inicial.
- **No tendrá acceso a los datos sin cifrar:** en este caso, SafeGuard Data Exchange sólo aceptará datos cifrados en los medios extraíbles. Si hay datos sin cifrar en los medios extraíbles, el sistema no le permitirá tener acceso a ellos. Sólo después de cifrar los archivos, obtendrá acceso a los datos.
- **Se le permite descifrar los archivos:** en este caso, puede descifrar explícitamente los archivos en los medios extraíbles. Los archivos que se han descifrado explícitamente permanecen como texto simple en el medio extraíble; por ejemplo, si se transfieren a un tercero.
- **Se le permite definir una contraseña de acceso al medio para medios extraíbles:** se le pide que introduzca una contraseña de acceso al medio la primera vez que conecta un medio extraíble.
- **Carpeta de texto simple en medios extraíbles:** el security officer puede definir una carpeta de texto simple que se creará en todos los medios extraíbles. SafeGuard Data Exchange no cifrará los archivos incluidos en esta carpeta.

### 12.1.1 Medios compatibles

SafeGuard Data Exchange admite los siguientes medios extraíbles:

- Lápices ópticos
- Discos duros externos conectados a través de USB o FireWire
- Unidades CD RW (UDF)
- Unidades DVD RW (UDF)
- FireWire
- Tarjetas de memoria en lectores de tarjetas USB (incl. ZIP, JAZ)

## 12.2 Cifrado de medios extraíbles

### 12.2.1 Cifrado inicial

El cifrado de datos sin cifrar contenidos en los medios extraíbles o bien comienza automáticamente tan pronto como conecte los medios al sistema, o deberá iniciar el proceso manualmente.



1. Para iniciar el proceso de cifrado, seleccione **Cifrado de archivos > Iniciar cifrado** en el menú contextual del Explorador de Windows. Si no se ha definido ninguna clave específica, se mostrará un cuadro de diálogo para la selección de claves.



2. Seleccione una clave y haga clic en **Aceptar**. Se cifrarán todos los datos que contengan los medios extraíbles.
3. Se utiliza la clave predeterminada hasta que se defina como predeterminada otra clave distinta. Si modifica la clave predeterminada, la nueva se utilizará para el cifrado inicial de los dispositivos extraíbles que se conecten al equipo posteriormente.

**Nota:** Para intercambiar datos con los usuarios que tengan SafeGuard Enterprise instalado en sus equipos, pero que no utilicen la misma clave que usted, son necesarias claves locales generadas por el usuario o una frase de contraseña para los medios. Estas claves también son necesarias para proteger el intercambio de datos con usuarios que no utilizan SafeGuard Enterprise. Puede identificar las claves locales por su prefijo (Local\_).

Si está activada la opción **Volver a cifrar los archivos si ya están cifrados con una clave diferente**, los archivos cifrados para los que existe una clave se descifrarán y se volverán a cifrar con la clave nueva.

#### **Tiempo de espera del cifrado inicial**

Si el cifrado inicial está configurado para que se inicie automáticamente, posiblemente pueda cancelarlo. En este caso, el botón **Cancelar** estará activado, aparecerá el botón **Iniciar** y el proceso de cifrado comenzará con un período de retraso de 30 segundos. Si no hace clic en el botón **Cancelar** durante este intervalo de tiempo, el cifrado inicial comenzará automáticamente transcurridos 30 segundos. Si hace clic en **Iniciar**, el proceso de cifrado inicial comenzará inmediatamente.

#### **12.2.1.1 Cifrado inicial en caso de utilizar la contraseña de acceso al medio**

Si se ha especificado el uso de una frase de contraseña de acceso al medio mediante una directiva, se le pedirá que introduzca la contraseña de medios antes del cifrado inicial. La contraseña de acceso al medio es válida para todos sus medios extraíbles y está vinculada a su equipo o a todos los equipos para los que tenga permisos de acceso.

El cifrado inicial no comenzará a menos que haya introducido la frase de contraseña de acceso al medio. Una vez introducida, el cifrado inicial comienza automáticamente.

Cuando haya introducido una vez la contraseña de acceso al medio, el cifrado inicial comenzará automáticamente cuando conecte otro dispositivo distinto al equipo.

**Nota:** En los equipos en los que no esté configurada la frase de contraseña de acceso al medio, no se iniciará el cifrado inicial.

#### **12.2.2 Cifrado transparente**

Si la configuración definida para su equipo estipula que los archivos se deben cifrar en los medios extraíbles, todos los procesos de cifrado y descifrado se ejecutarán de forma transparente.

Los archivos se cifrarán cuando se escriban en medios extraíbles y se descifrarán cuando se copien o muevan desde medios extraíbles a otra ubicación de los archivos.

**Nota:** Los datos sólo se descifrarán si se copian o se mueven a una ubicación en la que no se aplique ninguna otra directiva de cifrado. En ese caso, los datos estarán disponibles en dicha ubicación en forma de texto simple. Si en la nueva ubicación de los archivos está vigente un directiva de cifrado distinta, los datos se cifrarán en consecuencia.

### 12.2.2.1 Frase de contraseña de acceso a medios

Si se ha definido en la directiva, se le pedirá que la introduzca cuando conecte por primera vez un dispositivo extraíble tras haber instalado SafeGuard Data Exchange.

Si se muestra un cuadro de diálogo, lea atentamente la información que aparece y especifique una frase de contraseña para los medios o soportes. Puede utilizar esta misma frase de contraseña para medios o soportes para acceder a todos los archivos cifrados de sus medios extraíbles, independientemente de la clave utilizada para cifrarlos.

La frase de contraseña para medios será válida para todos los dispositivos que conecte al equipo. La contraseña de acceso al medio o soporte también se puede utilizar con SafeGuard Portable y permite acceder a todos los archivos independientemente de la clave utilizada para cifrarlos.

### 12.2.2.2 Cambiar/restablecer la contraseña de acceso al medio

Puede modificar la contraseña de acceso al medio en cualquier momento mediante la opción **Cambiar contraseña de acceso al medio** del menú del icono de la bandeja del sistema. Aparecerá un cuadro de diálogo en el que deberá introducir tanto la contraseña de acceso al medio anterior como la nueva, y confirmar esta última.

Si ha olvidado la frase de contraseña de acceso al medio, en este cuadro de diálogo tiene la opción de restablecerla. Si activa la opción **Restablecer contraseña de acceso al medio** y hace clic en **Aceptar**, se le informará de que su contraseña de acceso al medio se restablecerá la próxima vez que se conecte.

Desconéctese y vuelva a conectarse inmediatamente. A continuación, seleccione **Cambiar contraseña de acceso al medio** en el menú del icono de la bandeja. Se le informará de que no hay ninguna contraseña de acceso al medio en su equipo y se le pedirá que introduzca una nueva.

### 12.2.2.3 Sincronización de la contraseña de acceso al medio

La contraseña de acceso al medio de sus dispositivos y de su equipo se sincronizarán automáticamente. Si cambia la contraseña de acceso al medio de su equipo y conecta un dispositivo que aún utiliza la contraseña anterior de acceso al medio, se le indicará que las frases de contraseña del soporte se han sincronizado. Esto será válido para todos los equipos en los que tenga permiso para conectarse.

**Nota:** Una vez que haya cambiado la contraseña de acceso al medio, debería conectar todos los medios extraíbles a su equipo. De esta manera, se garantiza que la nueva contraseña de acceso a medios se utilizará inmediatamente en todos los dispositivos (sincronización).

#### 12.2.2.4 Cómo definir una clave predeterminada

Mediante la definición de una clave predeterminada, se especifica la clave que se va a utilizar para el cifrado durante el funcionamiento normal.

La clave predeterminada se puede definir a través del menú contextual de un archivo de un medio extraíble, o bien a través del menú contextual del propio medio extraíble. Además, puede definir una clave como la predeterminada inmediatamente después de crear una nueva clave local en el cuadro de diálogo "Crear clave".

Seleccione **Cifrado de archivos > Establecer clave predeterminada** para abrir un cuadro de diálogo para la selección de claves.

La clave que seleccione en este cuadro de diálogo se utilizará para todos los procesos de cifrado posteriores del medio extraíble. Si desea utilizar otra diferente, podrá definir una nueva clave predeterminada en cualquier momento.

Mediante una directiva se puede especificar una clave predeterminada que se utilizará para el cifrado. Si no se define mediante la directiva, se le pedirá que indique una clave inicial predeterminada.

### 12.3 Intercambio de datos con SafeGuard Data Exchange

A continuación, encontrará ejemplos típicos de intercambio seguro de datos a través de SafeGuard Data Exchange:

- Intercambio de datos con usuarios de SafeGuard Enterprise que tienen al menos una clave que está incluida en su juego de claves.

En este caso, cifre los datos del medio extraíble con una clave que también esté incluida en el juego de claves del destinatario (p. ej., en su equipo portátil). El destinatario podrá utilizar la clave para acceder a los datos cifrados de forma transparente.

- Intercambio de datos con usuarios de SafeGuard Enterprise que no tienen las mismas claves que usted.

En este caso, cree una clave local y cifre los datos con ella. Las claves que se crean localmente se protegen mediante una frase de contraseña y SafeGuard Enterprise puede importarlas.

El destinatario de los datos se proporciona con la frase de contraseña. Con la frase de contraseña, el destinatario podrá importar la clave y acceder a los datos.

- Intercambio de datos con usuarios que no dispongan de SafeGuard Enterprise

Los usuarios que no tengan SafeGuard Enterprise instalado en sus equipos tienen SafeGuard Portable a su disposición. Para intercambiar datos con SafeGuard Portable también hay que utilizar claves locales, combinadas con una frase de contraseña.

Además, SafeGuard Portable se tiene que copiar al medio extraíble. También debe proporcionar la frase de contraseña pertinente al destinatario de los datos cifrados. Con la frase de contraseña y SafeGuard Portable, el usuario puede descifrar los archivos, editarlos y volver a guardarlos cifrados en el medio extraíble. Dado que SafeGuard Portable es una aplicación autosuficiente, no hay que instalar ningún software adicional en el sistema host para acceder a los datos cifrados.

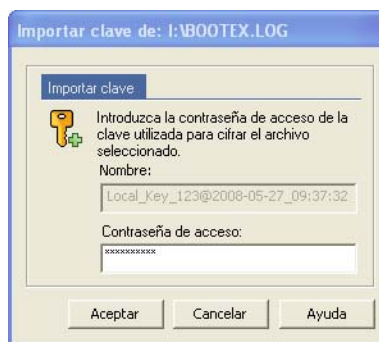
**Nota:** El security officer determinará si SafeGuard Portable se copia al medio extraíble a través de la directiva de seguridad que se le aplique a usted.

### 12.3.1 Importación de claves desde un archivo

Si ha recibido medios extraíbles que contienen datos cifrados que se han cifrado usando claves locales definidas por el usuario, puede importar la clave requerida para el descifrado en su juego de claves privado.

Para hacerlo, necesita la frase de contraseña pertinente. La persona que haya cifrado los datos tiene que proporcionarle la frase de contraseña.

Seleccione el archivo pertinente en el dispositivo extraíble y haga clic en **Cifrado de archivos > Gestión de claves > Importar clave**.

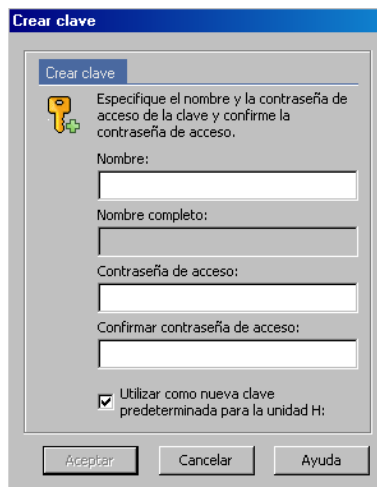


Especifique la frase de contraseña en el cuadro de diálogo que aparece. La clave se importará y tendrá acceso al archivo.

## 12.3.2 Creación de claves locales para el intercambio de datos de SafeGuard

Para crear una clave local definida por el usuario:

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de SafeGuard Enterprise, que se encuentra en la barra de tareas de Windows.
2. Haga clic en **Crear nueva clave**.



3. En el cuadro de diálogo Crear clave, escriba un **Nombre** y una **Contraseña de acceso** para la clave.

El nombre completo de la clave aparece en el campo de debajo.

4. Confirme la frase de contraseña.

Si especifica una frase de contraseña que no sea segura, aparecerá un mensaje de advertencia. Para aumentar el nivel de seguridad, es aconsejable que use frases de contraseña complejas. A pesar del mensaje de advertencia, puede utilizar la frase de contraseña si lo desea. La frase de contraseña también tiene que corresponder con las directivas definidas de la empresa. De lo contrario, se mostrará un mensaje de advertencia.

5. Con la opción **Utilizar como nueva clave predeterminada para la unidad c** podrá definir la clave nueva de manera inmediata como la clave predeterminada para la unidad en cuestión.

La clave predeterminada que especifique en este cuadro de diálogo es la que se va a utilizar para el cifrado durante el funcionamiento normal. Esta clave se utilizará hasta que se defina otra diferente.

6. Haga clic en **Aceptar**.

La clave se crea y estará disponible en cuanto los datos se hayan sincronizado correctamente con el servidor de SafeGuard Enterprise.

Si define esta clave como la predeterminada, todos los datos que se copien al medio extraíble a partir de ese momento se cifrarán con esta clave.

Para que el destinatario pueda descifrar todos los datos que contiene un medio extraíble, es posible que tenga que volver a cifrar los datos del medio extraíble con la clave creada localmente. Para ello, seleccione **Cifrado de archivos > Iniciar cifrado** en el menú contextual del medio en el Explorador de Windows. Seleccione la clave local necesaria y cifre los datos. Esto no será necesario si utiliza una contraseña de acceso al medio.

## 12.4 Grabación de archivos en un CD o DVD mediante el Asistente para grabación de CD de Windows

**Nota:** Con Windows XP, sólo puede grabar archivos en un CD mediante el Asistente para grabación de CD de Windows. Windows XP no es compatible con la grabación de archivos en DVD con el Asistente para grabación de CD.

SafeGuard Data Exchange permite grabar archivos cifrados en CD con el Asistente para grabación de CD.

Para ello, debe especificarse una regla de cifrado para la unidad de grabación de CD. SafeGuard Data Exchange agrega un cuadro de diálogo a los del Asistente para grabación de CD. En él, puede especificar la forma en que se grabarán los archivos en el CD (cifrados o como texto simple).

**Nota:** Si no se ha especificado ninguna regla de cifrado para la unidad de grabación de CD, los archivos se grabarán siempre como archivos de texto simple. No se mostrará el cuadro de diálogo de SafeGuard Data Exchange, en el que se puede especificar el estado de cifrado de los archivos que se van a grabar en el CD.

Cuando haya escrito un nombre para el CD, aparecerá la Extensión de grabación de disco extraíble de SafeGuard.

En **Estadística** se muestra la siguiente información:

- cuántos archivos se han seleccionado para la grabación en CD
- cuántos de ellos están cifrados
- cuántos de ellos son archivos simples

En **Estado** aparecen las claves utilizadas para el cifrado de los archivos previamente cifrados.

Para cifrar archivos que se van a grabar en CD, siempre se utiliza la clave especificada en la regla de cifrado para la unidad de grabación de CD.

Los archivos que se van a grabar en CD pueden estar cifrados con distintas claves si se ha cambiado la regla de cifrado para la unidad de grabación de CD. Si la regla de cifrado se desactivó al agregar los archivos, los archivos simples relevantes se pueden encontrar en la carpeta donde se incluyen los archivos que se van a copiar en CD.

### 12.4.1 Cifrado de archivos para la grabación en CD

Si desea grabar archivos cifrados en un CD, haga clic en **(Volver a) Cifrar todos los archivos**.

Si es necesario, los archivos ya cifrados se volverán a cifrar y los archivos simples se cifrarán. En el CD, los archivos se cifran con la clave especificada en la regla de cifrado de la unidad de grabación de CD.

### 12.4.2 Grabación de archivos en CD con formato simple

Si selecciona **Descifrar todos los archivos**, los archivos se descifran en primer lugar y, a continuación, se graban en el CD.

### 12.4.3 Copia de SafeGuard Portable a un soporte óptico

Si selecciona esta opción, SafeGuard Portable también se copiará en el CD. Esto permite leer y modificar los archivos cifrados con SafeGuard Data Exchange sin la necesidad de tenerlo instalado.

### 12.4.4 Grabación en CD o DVD con Windows Vista

Windows Vista también tiene un Asistente para grabación de CD para CD y DVD.

La extensión de grabación de disco de SafeGuard del Asistente para grabación de CD sólo está disponible para la grabación de CD y DVD en formato **con registro de inicio maestro**. El asistente sólo se mostrará si los archivos que se van a grabar en CD/DVD tienen formato **con registro de inicio maestro**.

Con el sistema de archivos LFS, no es necesario utilizar ningún Asistente para grabación. En este caso, la unidad de grabación se utiliza al igual que cualquier soporte extraíble. Si se ha definido una regla de cifrado para la unidad de grabación, los archivos se cifrarán automáticamente al copiarse en el CD/DVD.

## 12.5 SafeGuard Portable

Con SafeGuard Portable puede intercambiar datos cifrados a través de medios extraíbles con destinatarios que no tengan SafeGuard Data Exchange instalado en sus equipos. Los datos cifrados a través de SafeGuard Data Exchange se pueden cifrar y descifrar con SafeGuard Portable. Esto se logra mediante un programa (SGPortable.exe) que se copia automáticamente a los medios extraíbles.

**Nota:** SafeGuard Portable sólo cifra o descifra archivos cifrados con AES 256.

Con SafeGuard Portable en combinación con la contraseña de acceso al medio relevante se obtendrá acceso a todos los archivos cifrados, independientemente de la clave que se haya utilizado para cifrarlos. O bien, puede utilizar la contraseña de una clave local, que le proporcionará acceso a los archivos que se hayan cifrado con esta clave determinada. El destinatario puede descifrar los datos cifrados y volverlos a cifrar de nuevo.

**Nota:** La contraseña de acceso al medio o la frase de contraseña de una clave local deben comunicarse por adelantado al destinatario.

El destinatario puede utilizar las claves existentes creadas con SafeGuard Data Exchange para el cifrado, o bien crear una clave nueva con SafeGuard Portable (por ejemplo, para los archivos nuevos).

No es necesario que SafeGuard Portable se instale o se copie en el equipo de la otra parte integrante en la comunicación. Permanece en el medio extraíble.

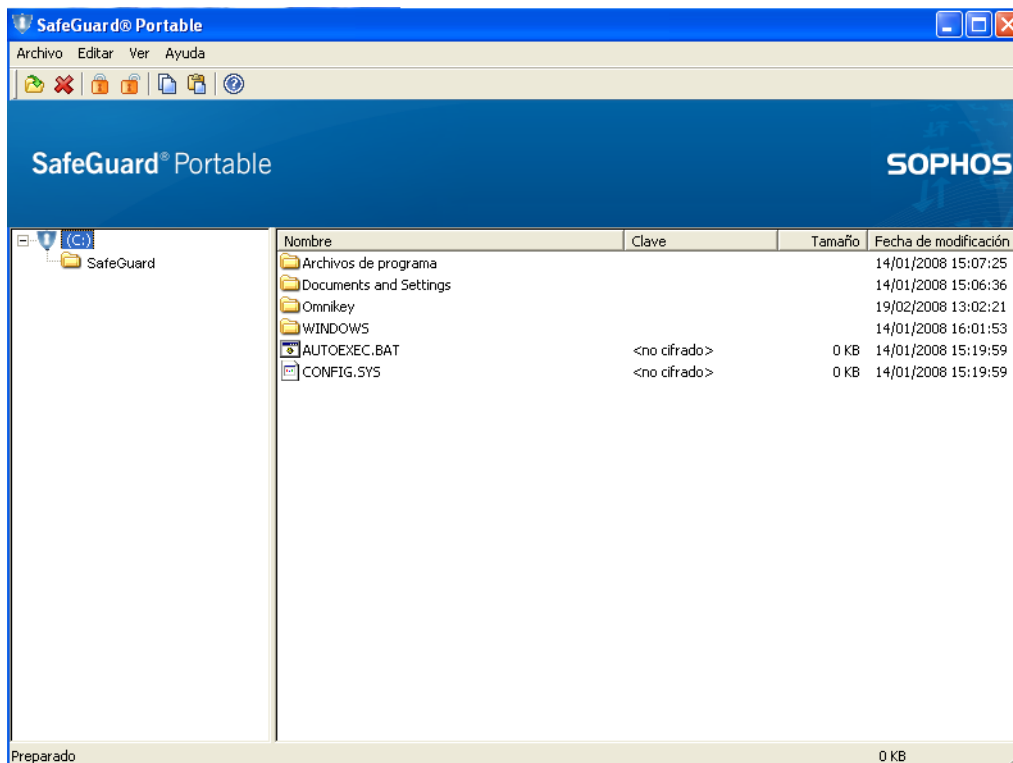
**Nota:** Los usuarios de SafeGuard Enterprise no suelen necesitar SafeGuard Portable. La descripción que se facilita a continuación asume que los usuarios no tienen SafeGuard Enterprise instalado en sus equipos y que, por lo tanto, deben utilizar SafeGuard Portable para editar los datos cifrados.

## 12.5.1 Edición de archivos con SafeGuard Portable

Ha recibido un medio extraíble que contiene archivos cifrados con SafeGuard Data Exchange, así como una carpeta llamada `SGPortable`. Esta carpeta contiene el archivo `SGPortable.exe`.

1. Haga doble clic en `SGPortable.exe` para iniciar SafeGuard Portable.

Con SafeGuard Portable puede descifrar los datos cifrados que contiene el medio extraíble y después volver a cifrarlos. SafeGuard Portable le ofrece una funcionalidad parecida a la del Explorador de Windows.



Además de los detalles de los archivos que el Explorador de Windows presenta (nombre, tamaño, etc.), SafeGuard Portable muestra la columna **Clave**. Esta columna indica si los datos pertinentes están cifrados. Si un archivo está cifrado, aparece el nombre de la clave que se ha utilizado para cifrarlo.

**Nota:** Sólo se pueden descifrar aquellos archivos de los que se conozca la frase de contraseña correspondiente a la clave utilizada.

2. Para editar archivos en el medio extraíble, seleccione el archivo haciendo clic en él y elija el comando relevante en el menú contextual (haciendo clic con el botón derecho), o bien desde el menú **Archivo**.

En el menú contextual están disponibles estos comandos:

<b>Establecer clave de cifrado</b>	Abre el cuadro de diálogo Clave. En este cuadro de diálogo, podrá generar una clave de cifrado con SafeGuard Portable.
<b>Cifrar</b>	Cifra el archivo activado en el medio extraíble. Para el cifrado se empleará la última clave que se haya usado.
<b>Descifrar</b>	Abre el cuadro de diálogo Especificar contraseña de acceso al medio. En este cuadro de diálogo se especifica la frase de contraseña necesaria para descifrar el archivo seleccionado.
<b>Estado de cifrado</b>	Muestra un cuadro de diálogo y el estado del cifrado del archivo.
<b>Copiar a</b>	Copia el archivo a la carpeta que elija y lo descifra.
<b>Suprimir</b>	Elimina el archivo activado del medio extraíble.

También puede seleccionar los comandos **Abrir**, **Suprimir**, **Cifrar**, **Descifrar** y **Copiar** mediante los iconos de la barra de herramientas.

### 12.5.1.1 Establecimiento de claves de cifrado

Para cifrar un archivo de un medio extraíble y crear una clave de cifrado:

1. En el menú contextual, o bien desde el menú **Archivo**, seleccione **Establecer clave de cifrado**. Aparecerá el cuadro de diálogo Clave.
2. Especifique un **Nombre** y una **Contraseña de acceso** para la clave. Tendrá que **Confirmar** la contraseña de acceso y hacer clic en **Aceptar**.

La contraseña de acceso tiene que corresponderse con las directivas que estén definidas por la empresa. De lo contrario, se mostrará un mensaje de advertencia.

La clave se crea y, a partir de ese momento, se utilizará para el cifrado.

### 12.5.1.2 Cifrado

Para cifrar un archivo en un medio extraíble:

1. En el explorador de SafeGuard Portable, seleccione el archivo y, a continuación, elija la opción **Cifrar** en el menú contextual.

El archivo se cifrará con la última clave utilizada por SafeGuard Portable.

Al guardar archivos nuevos en medios extraíbles con el procedimiento de arrastrar y soltar en el explorador de SafeGuard Portable, se le preguntará si desea cifrarlos.

Si es así y no se ha realizado antes ningún cifrado con SafeGuard Portable, se abrirá un cuadro de diálogo para establecer la clave. En este cuadro de diálogo tiene que escribir el nombre de la clave y la contraseña de acceso (que tendrá que confirmar). Haga clic en **Aceptar**.

2. Seleccione el archivo que desea cifrar con la clave que acaba de establecer y elija la opción **Cifrar** del menú contextual incluido en el menú **Archivo**.

El archivo se cifrará y cuando el proceso finalice aparecerá un mensaje.

**Nota:** La última clave que SafeGuard Portable haya utilizado y establecido se usará para todos los procesos de cifrado posteriores que realice con SafeGuard Portable, a menos que establezca una clave nueva.

### 12.5.1.3 Descifrado

Para descifrar un archivo en un medio extraíble:

1. Seleccione el archivo en el explorador de SafeGuard Portable y, en el menú contextual, elija **Descifrar**.

Aparecerá el cuadro de diálogo en el que debe introducir la contraseña de acceso al medio o la frase de contraseña de una clave local.

2. Especifique la contraseña de acceso al medio pertinente (el remitente tiene que proporcionarle esta frase de contraseña) y haga clic en **Aceptar**.

El archivo se descifrá.

La contraseña de acceso al medio le da acceso a todos los archivos cifrados en medios extraíbles, sin que importe qué clave se utilizó para cifrarlos. Si sólo dispone de la contraseña de acceso al medio de una clave local, sólo tendrá acceso a los archivos cifrados con esta clave.

Al descifrar un archivo que se haya cifrado con una clave que se ha generado en SafeGuard Portable, este archivo se descifrá automáticamente.

Después de descifrar los archivos en los medios extraíbles y de escribir la contraseña de acceso de la clave, no es necesario especificarla de nuevo la siguiente vez que cifre o descifre los archivos que se han cifrado con la misma clave.

SafeGuard Portable guarda la contraseña de acceso al medio mientras la aplicación se esté ejecutando. Para el cifrado se utilizará la última clave que empleó SafeGuard.

Tras descifrar los archivos, estarán disponibles en forma de texto simple en el medio extraíble. Los archivos que se hayan descifrado se cifrarán automáticamente al cerrar SafeGuard Portable.

#### 12.5.1.4 Cifrado de archivos nuevos con SafeGuard Portable

Con SafeGuard Portable también puede copiar sus propios archivos cifrados en medios extraíbles.

Para ello:

1. No tiene más arrastrar y soltar los archivos que desee copiar para llevarlos al explorador de SafeGuard Portable.

El sistema le pregunta si desea cifrar el archivo pertinente.

2. Si lo confirma, el archivo se cifrará con la última clave utilizada y se copiará en el medio extraíble.

#### 12.5.1.5 Estado del cifrado

Para determinar el estado de cifrado de un archivo:

1. Seleccione el archivo y elija la opción **Estado de cifrado** en el menú contextual del menú **Archivo**.

El estado de cifrado también se indicará en la columna **Clave**, junto al nombre del archivo, en el explorador de SafeGuard Portable.

## 12.5.2 Otras operaciones con SafeGuard Portable

Están disponibles las siguientes funciones:

- **Abrir:** el comando de menú sólo está disponible con el menú Archivo de SafeGuard Portable.

Después de abrir un archivo cifrado mediante este menú de comando, se le pedirá que introduzca su frase de contraseña de acceso. Escríbala y haga clic en **Aceptar**. El archivo se cifrará y se abrirá.

- **Suprimir:** elimina el archivo seleccionado.

- **Copiar a:** este comando de menú sólo está disponible en el menú contextual que puede visualizar utilizando el botón derecho del ratón en el explorador de SafeGuard Portable.

Con este comando, puede copiar los archivos de los medios extraíbles a otra unidad del equipo.

- **Salir:** este comando de menú sólo está disponible en el menú Archivo de SafeGuard Portable.

**Salir** cierra SafeGuard Portable.

## 13 SafeGuard Configuration Protection

Con SafeGuard Configuration Protection, podrá definir las interfaces y los dispositivos permitidos en los equipos de los usuarios. Esto evita que se introduzca código malicioso así como la exportación de datos a través de canales no deseados como WLAN. Este módulo también puede detectar y bloquear hardware dañino, como registradores de claves.

En general, se pueden permitir o bloquear los puertos o dispositivos en el equipo usando directivas. Asimismo, se puede restringir el uso de determinados dispositivos.

Es posible establecer restricciones para ciertos dispositivos en los siguientes tipos de puertos:

- USB
- PCMCIA
- Firewire

Para estos puertos, se pueden definir con exactitud los dispositivos permitidos y no permitidos.

El security officer define centralmente los puertos y los dispositivos que se pueden usar.

Si un puerto específico no se permite en general, se muestra un mensaje de notificación una vez después de la recepción de la directiva que contiene esta información. El puerto no se puede utilizar.

El mensaje de notificación se muestra como una información de herramientas del icono de protección de configuración independiente en la barra de tareas de Windows.

Si se han definido para el equipo restricciones de uso del puerto o del medio de almacenamiento, la información sobre herramientas le avisa tan pronto como intente usar puertos o medios de almacenamiento que no estén permitidos.

## 14 SafeGuard Enterprise y BitLocker

El cifrado de unidad BitLocker es una completa función de cifrado de discos con autenticación en la fase previa al arranque del equipo, incluida en los sistemas operativos Windows Vista y Windows 7 de Microsoft. Está pensada para proteger los datos, ya que proporciona cifrado al volumen de arranque.

### 14.1 Directivas de cifrado para BitLocker

El security officer puede crear una directiva para el cifrado (inicial) en SafeGuard Management Center y distribuirla a los equipos de los usuarios de BitLocker donde se ejecuta.

Ya que los clientes de BitLocker se administran de forma transparente en el Management Center, el responsable de seguridad no tiene que preparar ninguna configuración especial de BitLocker para el cifrado. SafeGuard Enterprise conoce cuál es el estado de los clientes y selecciona el cifrado de BitLocker de acuerdo con tales datos. Cuando se instala un cliente de BitLocker con SafeGuard Enterprise y se activa el cifrado de volúmenes, BitLocker cifra los volúmenes.

### 14.2 Cifrado inicial en el equipo protegido con BitLocker

Cuando se envíe la directiva de cifrado al equipo protegido con BitLocker y antes de que el equipo dé comienzo al cifrado inicial, BitLocker genera las claves de cifrado. Se le preguntará dónde desea almacenar la clave de cifrado de BitLocker. Una copia de seguridad de esta clave se almacena adicionalmente en la base de datos SafeGuard Enterprise para su recuperación.

Cuando se instala SafeGuard Enterprise en su equipo, el icono del producto SafeGuard Enterprise se muestra en la bandeja del sistema de la barra de tareas del PC. Podrá acceder centralmente a todas las funciones importantes ofrecidas por SafeGuard Enterprise en su equipo. Tenga en cuenta que las funciones disponibles dependen de la configuración definida en SafeGuard Management Center. El security officer especifica centralmente esta configuración en SafeGuard Management Center y la distribuye a los equipos de los usuarios.



**Nota:** Si un disco duro cifrado de BitLocker en un equipo se sustituye por un nuevo disco duro cifrado por BitLocker y a éste se le asigna la misma letra de unidad que el anterior, SafeGuard Enterprise sólo guarda la clave de recuperación del nuevo disco duro.

**Nota:** En caso de que un volumen ya esté cifrado con BitLocker, antes de instalar la compatibilidad de BitLocker con SafeGuard Enterprise, debe realizar una copia de seguridad de las claves del volumen anteriormente cifrado usando los mecanismos de copia de seguridad ofrecidos por Microsoft.

## 14.3 Descifrado con BitLocker

Los equipos de usuarios cifrados con BitLocker no se pueden descifrar automáticamente. El descifrado debe realizarse usando la herramienta "Manage-bde" de Microsoft.

## 14.4 Autenticación con BitLocker

BitLocker ofrece toda una gama de opciones de autenticación. Los usuarios de BitLocker pueden autenticarse a través del Módulo de plataforma segura (TPM) o de un lápiz de memoria, mediante una combinación de ambos métodos.

El security officer puede establecer los diversos modos de conexión en una directiva en el SafeGuard Management Center y distribuirla a los equipos de los usuarios de BitLocker.

Los usuarios de BitLocker de SafeGuard Enterprise tienen a su disposición los siguientes modos de conexión:

- Sólo TPM
- TPM + PIN
- TPM + lápiz de memoria
- Sólo lápiz de memoria (sin TPM)

### 14.4.1 Módulo de plataforma segura (TPM)

El TPM es un módulo similar a una tarjeta inteligente en la placa base que ejecuta funciones criptográficas y operaciones de firma digital. Puede crear, almacenar y gestionar claves de usuario. Está protegido contra ataques.

### 14.4.2 Lápices ópticos

Las claves externas se pueden almacenar en un lápiz de memoria no protegido.

### **14.4.3 Autenticación en el equipo BitLocker**

Durante el preinicio del equipo BitLocker, se le pedirá que inserte el PIN de TPM o el lápiz de memoria para su autenticación.

## 15 SafeGuard Enterprise y Lenovo Rescue and Recovery

Para obtener información sobre las versiones de Lenovo Rescue and Recovery (RnR) compatibles con SafeGuard Enterprise, consulte el siguiente artículo del centro de conocimientos (Knowledge Base): <http://www.sophos.com/support/knowledgebase/article/108383.html>

Es posible restaurar copias de seguridad completas del sistema operativo en una partición cifrada sin tener que descifrar primero el disco duro. Esto ahorra mucho tiempo al realizar una recuperación tras un desastre. SafeGuard Enterprise ha recibido el certificado oficial de Lenovo para esta funcionalidad.

La función principal de Lenovo Rescue and Recovery es restaurar datos con tan solo pulsar una tecla. Incluso si el sistema operativo principal está dañado y ya no arranca, Rescue and Recovery guarda los datos mediante un entorno de emergencia (WinPE). Puede acceder a las herramientas de rescate desde el escritorio de Microsoft Windows o pulsando la tecla "ThinkVantage" de color azul integrada en los sistemas de Lenovo.

Lenovo Rescue and Recovery resulta especialmente útil para los usuarios que no dispongan de la ayuda de un administrador. Por ejemplo, en medio de un viaje de negocios, podrán utilizar esta funcionalidad para restaurar el equipo.

### 15.1 Descripción general

SafeGuard Enterprise se integra con la función Rescue and Recovery y es compatible con funciones de Lenovo como el botón azul "ThinkVantage" presente en el teclado de los portátiles Lenovo o el botón azul "Intro" de los teclados para PC.

Esta función integrada le permite aunar este eficaz método de copia de seguridad y recuperación junto con las particiones del sistema operativo cifradas mediante SafeGuard Enterprise. Las copias de seguridad de los sistemas cifrados de SafeGuard Enterprise se pueden guardar en cualquier unidad de disco que utilice RnR. Por tanto, en caso de emergencia, se puede restaurar un sistema cargando la copia de seguridad desde una partición virtual o de servicio, o bien, desde un dispositivo extraíble, como puede ser un CD/DVD o un disco duro USB.

SafeGuard Enterprise no se ve afectado por la restauración del sistema y conserva toda la configuración de cifrado para que no sea necesario volver a instalar ningún programa de software. No tiene que reiniciar el cifrado.

En un entorno de SafeGuard Enterprise, Rescue and Recovery se basa en la recuperación de WinPE. WinPE se puede iniciar desde diferentes entornos:

- desde una partición virtual o de servicio
- desde un dispositivo extraíble como puede ser un CD/DVD o un disco duro USB.

## 15.2 Requisitos

- BIOS más reciente para el PC/portátil
- Si desea obtener información sobre la compatibilidad de las versiones de Rescue and Recovery con las versiones de SafeGuard Enterprise, consulte: <http://www.sophos.com/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery se puede utilizar para recuperar volúmenes cifrados de SafeGuard Enterprise. Debe estar instalado el paquete de instalación `SGNClient.msi`.
- En el caso de los volúmenes para Rescue and Recovery, éstos deben estar cifrados con la clave del equipo definida. Rescue and Recovery no es compatible con volúmenes cifrados con cualquier otra clave.

## 15.3 Instalación

Cuando el software Rescue and Recovery se instala en un disco duro que no tiene una partición de servicio, se aplica lo siguiente:

El entorno de Rescue and Recovery se instala en una partición virtual de la unidad "C:" del disco duro del equipo (partición principal del disco duro maestro).

En las secciones que figuran a continuación, fíjese en la secuencia de instalación de Rescue and Recovery y SafeGuard Enterprise. Le recomendamos que instale la función Rescue and Recovery de Lenovo en primer lugar y después SafeGuard Enterprise.

### 15.3.1 Instalación de Rescue and Recovery y SafeGuard Enterprise

Le recomendamos que siga la secuencia de instalación que ahora describimos:

1. Instale la versión más reciente de Rescue and Recovery.
2. Instale la versión más reciente del módulo SafeGuard Enterprise Device Encryption (`SGNClient.msi`).

SafeGuard Enterprise comprueba si está instalado Rescue and Recovery y agrega sus propios archivos y configuraciones al entorno de recuperación de Lenovo.

3. Compruebe que está activada la POA, de forma que no sea posible restaurar copias de seguridad no autorizadas.

La POA se activa durante la instalación de SafeGuard Enterprise.

### 15.3.2 SafeGuard Enterprise Device Encryption ya está instalado

Los pasos de instalación necesarios de Rescue and Recovery dependen del lugar en el se ubique el entorno WinPE de RnR.

- Si el entorno WinPE de RnR está ubicado en el primer disco duro de una partición virtual o de servicio

En este caso, no se realiza la configuración automática de SafeGuard Enterprise para el entorno WinPE de RnR. Debe iniciar una herramienta de SafeGuard Enterprise llamada `SetupWinPE.exe` para configurar el entorno WinPE de RnR, con el fin de usarlo con SafeGuard Enterprise. Esta herramienta realizará todas las modificaciones necesarias para el entorno WinPE.

**Nota:** `SetupWinPE.exe` también se puede utilizar si actualiza la versión actualmente instalada de RnR con una versión nueva. En el caso de una actualización de RnR, le recomendamos que vuelva a iniciar `SetupWinPE.exe` para asegurarse de que se realicen todas las modificaciones necesarias de WinPE.

**Nota:** Observe que esta herramienta solo se puede usar para un entorno WinPE de RnR ubicado en un disco duro local.

- a) Instale Rescue and Recovery en el disco duro local.
- b) Inicie la siguiente herramienta:  
`SetupWinPE.exe -r`
- c) Reinicie el sistema operativo Windows.

- Si el entorno WinPE de RnR se encuentra en un CD-ROM o un disco duro externo

Cuando la función Crear medios de Rescue and Recovery de RnR crea WinPE, ya se han realizado todas las modificaciones necesarias para el entorno WinPE de RnR.

- a) Instale Rescue and Recovery.
- b) Reinicie el sistema operativo Windows.

### 15.3.3 Si Rescue and Recovery ya está instalado

Si el entorno WinPE de RnR está ubicado en el primer disco duro de una partición virtual o de servicio

En este caso se copian todos los controladores y archivos necesarios en sus ubicaciones correspondientes del entorno WinPE de RnR y se agregan las entradas de registro necesarias a los archivos de registro de WinPE.

Instale la versión más reciente del módulo SafeGuard Enterprise Device Encryption (`SGNClient.msi`).

SafeGuard Enterprise comprueba si está instalado Rescue and Recovery y agrega sus propios archivos y configuraciones al entorno de recuperación de Lenovo (WinPE).

## 15.4 Actualización

Actualizar significa que SafeGuard Enterprise y Rescue and Recovery ya están instalados y desea actualizar uno de ellos o ambos a una versión más reciente.

### 15.4.1 Actualización de SafeGuard Enterprise

Si actualiza SafeGuard Enterprise, se actualiza todo el sistema, por lo que no deberá realizar más configuraciones adicionales.

### 15.4.2 Actualización de Rescue and Recovery

Si actualiza Rescue and Recovery, ejecute `SetupWinPE.exe` antes de reiniciar el equipo tras la actualización.

## 15.5 Desinstalación

Al desinstalar productos de software:

- Le recomendamos que desinstale SafeGuard Enterprise en primer lugar y, a continuación, la función Rescue and Recovery. Si se desinstala SafeGuard Enterprise mientras Rescue and Recovery sigue instalado, se eliminan del entorno WinPE de RnR todas las modificaciones específicas de SafeGuard Enterprise, como las entradas de registro, los archivos y las unidades agregadas.
- No desinstale SafeGuard Enterprise inmediatamente después de haber restaurado el sistema. Tras una restauración del sistema, reinicie el equipo una vez y, a continuación, desinstale SafeGuard Enterprise.
- Si se elimina Rescue and Recovery mientras SafeGuard Enterprise sigue instalado, se eliminarán las modificaciones de RnR del sector de arranque MBR y se restaurará el sector de arranque MBR original.

## 15.6 Opciones de recuperación y entorno de arranque

SafeGuard Enterprise le permite arrancar en el entorno de Rescue and Recovery tras haber iniciado sesión correctamente en la POA (power-on authentication).

### Desde el disco duro local

- La partición virtual en el disco duro local o la partición de servicio local
- Los volúmenes deben estar cifrados en SafeGuard Enterprise con la clave de equipo definida. Todos los controladores necesarios se han debido agregar al entorno WinPE de RnR. Entonces, la clave de equipo definida estará disponible en el entorno WinPE de RnR y se podrá acceder de nuevo a los volúmenes.

**Nota:** SafeGuard Enterprise no le permite arrancar en el entorno de Rescue and Recovery cuando arranca directamente desde BIOS.

### Desde un CD/DVD de arranque o desde cualquier medio extraíble de arranque

- En este caso, no se realiza ninguna autenticación en la Autenticación durante el encendido, ni hay claves disponibles, por lo que no se puede acceder a los volúmenes cifrados. Si se arranca Rescue and Recovery directamente desde BIOS, se restaurará el sistema operativo. SafeGuard Enterprise se eliminará durante el proceso de restauración. Para volver a proteger el sistema, se debe volver a instalar SafeGuard Enterprise.

## 15.7 Crear una copia de seguridad

En Windows, utiliza Rescue and Recovery para crear copias de seguridad. En equipos en los que Rescue and Recovery ya esté instalado y se instale SafeGuard Enterprise más adelante, se muestra un mensaje que pide al usuario que cree una copia de seguridad nueva del sistema.

Antes de crear una copia de seguridad de su sistema con Rescue and Recovery, lea la documentación proporcionada por Lenovo.

SafeGuard Enterprise sólo admite guardar copias de seguridad en:

- el disco duro local
- un segundo disco duro
- un disco duro USB
- una red
- un lápiz de memoria USB
- un CD/DVD

De forma predeterminada, las copias de seguridad se guardan en la carpeta C:\RRUbackups. Esta carpeta está protegida por Rescue and Recovery si se guarda en una partición local del disco duro principal. En tal caso, no se puede eliminar ni borrar.

## 15.8 Restaurar copias de seguridad de archivos

Rescue and Recovery puede restaurar archivos o carpetas desde copias de seguridad en las que esté instalado SafeGuard Enterprise. Sólo tiene que iniciar Windows, a continuación, Rescue and Recovery y restaurar los archivos seleccionados. No es necesario reiniciar el equipo cuando haya finalizado la restauración: puede trabajar con los archivos inmediatamente.

## 15.9 Restauración del sistema de SafeGuard Enterprise

Para restaurar una copia de seguridad del sistema que incluya SafeGuard Enterprise, arranque en el entorno de Rescue and Recovery. El entorno de RnR aparecerá en cuanto pulse una de las siguientes teclas durante el proceso de arranque:

- "Thinkvantage" (portátiles Lenovo)
- tecla "Intro azul" (equipos de sobremesa de Lenovo)
- **F11** en otros teclados

1. Si utiliza un equipo Lenovo:

- a) Inicie el entorno de Rescue and Recovery desde un disco duro local pulsando el botón "ThinkVantage" en el teclado de un portátil Lenovo o el botón "Intro" azul en el teclado de un PC Lenovo.

Se muestra la Autenticación durante el encendido.

- b) Introduzca las credenciales de SafeGuard Enterprise.

2. Si no utiliza un equipo Lenovo:

- a) Conéctese a la POA con sus credenciales de SafeGuard Enterprise.
- b) Mientras el equipo sigue iniciándose, pulse **F11** para iniciar el entorno de Rescue and Recovery.

Se mostrará la interfaz del usuario de Rescue and Recovery. Aparecerá la pantalla de bienvenida.

3. Haga clic en **Siguiente**.

4. En el menú situado a la izquierda, seleccione la opción **Restaurar copia de seguridad**.

Aparecerá un cuadro de diálogo que el que podrá seleccionar la copia de seguridad.

5. Selecciónela y restáurela.

## 15.10 Particiones de servicio y de recuperación de fábrica

Los equipos nuevos de Lenovo incluyen particiones especiales preinstaladas:

- **Partición de servicio de Lenovo:** contiene el entorno de arranque de Rescue and Recovery.
- **Partición de recuperación de fábrica:** contiene toda la información sobre la configuración y las funciones de recuperación incluidas de fábrica en el equipo.

Estas particiones están visibles en Windows con diferentes letras de unidades.

**Nota:** Cuando estas particiones estén disponibles en el equipo, nunca estarán cifradas incluso si se define una directiva de cifrado para, por ejemplo, cifrar todos los volúmenes.

Si en el equipo no existen estas particiones, pero desea crear una, hágalo antes de instalar SafeGuard Enterprise. Si desea obtener más información, consulte la documentación de Lenovo.

## **15.11 POA deshabilitada y Lenovo Rescue and Recovery**

Si la POA está deshabilitada en su equipo, la autenticación de Rescue and Recovery debe habilitarse para que sirva como método de protección frente a los accesos no autorizados a los archivos cifrados desde el entorno de Rescue and Recovery.

Para obtener información detallada sobre cómo activar la autenticación de Rescue and Recovery, consulte la documentación de Lenovo Rescue and Recovery.

## 16 Soporte técnico

Para obtener asistencia técnica sobre cualquier producto de Sophos, puede:

- Visitar el fórum SophosTalk en <http://community.sophos.com/> para consultar casos similares.
- Visitar la base de conocimiento de Sophos en <http://www.sophos.com/support/>
- Descargar la documentación correspondiente desde <http://www.sophos.com/support/docs/>
- Enviar un email a [support@sophos.com](mailto:support@sophos.com) indicando la versión del producto de Sophos, el sistema operativo y parches aplicados, y el texto exacto de cualquier mensaje de error.

## **17 Copyright**

Copyright © 1996 - 2010 Sophos Group y Utimaco Safeware AG. Todos los derechos reservados.

Ninguna parte de esta publicación puede ser reproducida, almacenada o transmitida de ninguna forma, ni por ningún medio, sea éste electrónico, mecánico, grabación, fotocopia o cualquier otro sin la correspondiente licencia del producto, bajo dichos términos, o sin la previa autorización escrita por parte del propietario.

Sophos es una marca registrada de Sophos Plc y Sophos Group. SafeGuard es una marca registrada de Utimaco Safeware AG - a member of the Sophos Group. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

Todos los productos SafeGuard están sujetos del derechos de autor de Utimaco Safeware AG - a member of the Sophos Group, o, si procede, de sus licenciantes. Todos los otros productos Sophos están sujetos del derechos de autor de Sophos plc., o, si procede, de sus licenciantes.

La información del copyright de proveedores terceros se encuentra en el archivo Disclaimer and Copyright for 3rd Party Software.rtf del directorio del producto.