

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy Ayuda de usuario

Versión: 5.60

Edición: abril de 2011



Contenido

- 1 Acerca de Sophos SafeGuard.....3
- 2 Copia de seguridad de la clave para la recuperación.....4
- 3 POA (power-on authentication).....5
- 4 POA (power-on authentication) en Windows Vista y Windows 7.....16
- 5 Inicio de sesión en Windows Vista y Windows 7.....18
- 6 Conexión con el Lector de huellas digitales de Lenovo.....19
- 7 Opciones de recuperación.....25
- 8 Recuperación mediante Local Self Help.....26
- 9 Recuperación mediante el procedimiento de desafío/respuesta.....34
- 10 Icono de la bandeja del sistema e información de ayuda.....37
- 11 Acceder a funciones desde el Explorador de Windows.....40
- 12 Cifrado de datos.....41
- 13 SafeGuard Data Exchange.....44
- 14 Sophos SafeGuard y unidades autocifradas compatibles con Opal.....55
- 15 Sophos SafeGuard y Lenovo Rescue and Recovery.....56
- 16 Soporte técnico.....61
- 17 Aviso legal.....61

1 Acerca de Sophos SafeGuard

Sophos SafeGuard emplea directivas de cifrado para proteger la información en las estaciones. Las principales funciones de seguridad son el cifrado de datos y la protección contra el acceso sin autorización. Para el usuario, Sophos SafeGuard resulta muy fácil de utilizar. El sistema de autenticación de Sophos SafeGuard, la POA (power-on authentication), proporciona una potente protección para el acceso y ofrece un sistema de asistencia sencillo para recuperar las credenciales.

La administración se lleva a cabo mediante un editor de políticas, SafeGuard Policy Editor, que se utiliza para crear y gestionar directivas de seguridad y para prestar funciones de recuperación. Un equipo protegido con Sophos SafeGuard recibe las directivas a través de un paquete de configuración creado desde el editor de políticas. El paquete de configuración se puede distribuir a través de los mecanismos de distribución de software de la empresa o de forma manual.

Nota: Sophos SafeGuard está disponible con distintos paquetes de productos: SGE (SafeGuard Easy) y ESDP (Endpoint Security and Data Protection). Desde la versión 5.50, SGE es el nuevo nombre de producto para SafeGuard Enterprise Standalone. Para cada paquete hay disponibles distintos módulos y funciones. Los módulos y las funciones que no están disponibles para ESDP están marcadas con notas en esta ayuda.

Los módulos siguientes están disponibles para los equipos protegidos con Sophos SafeGuard:

■ SafeGuard Device Encryption

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 iniciará la sesión automáticamente en el sistema operativo. La POA (power-on authentication) también se puede desactivar, en cuyo caso, la autenticación del usuario se realiza a través del sistema operativo.

Cifrado de volúmenes

Todos los datos en los volúmenes (incluidos los archivos de arranque, archivos de intercambio, archivos en hibernación o sin uso, archivos temporales, información sobre directorios, etc.) se cifran de forma transparente sin que el usuario tenga que cambiar el procedimiento de trabajo normal o tenga que tomar en cuenta la seguridad.

■ SafeGuard Data Exchange

Nota:

SafeGuard Data Exchange y SafeGuard Portable no están disponibles con ESDP.

SafeGuard Data Exchange facilita el intercambio de datos mediante unidades extraíbles en todas las plataformas, sin tener que volver a cifrar.

Cifrado de 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.

Nota:

Puede que no todas las características que se describen en esta ayuda estén disponibles en su equipo. Esto se debe a que el responsable de seguridad define las funciones disponibles.

1.1 Funciones de Sophos SafeGuard

Sophos SafeGuard dispone de las siguientes funciones:

■ Opciones de recuperación en la POA (power-on authentication)

Para la recuperación (por ejemplo, si ha olvidado la contraseña), Sophos SafeGuard presenta estas opciones:

Si ha olvidado la contraseña, puede emplear **Local Self Help** para volver a acceder al equipo sin la asistencia del centro de ayuda. Para conectarse, no tiene más que responder una serie de preguntas predeterminadas en la POA (power-on authentication). Gracias a Local Self Help, puede volver a acceder a su equipo en situaciones donde ni el teléfono ni las conexiones de red están a su alcance (por ejemplo, si está viajando en avión). Para más información, [consulte el apartado *Recuperación mediante Local Self Help*](#) en la página 26.

El procedimiento desafío/respuesta es un sistema de recuperación seguro y eficaz que, con la asistencia del centro de ayuda, le permitirá acceder a su equipo o a datos cifrados. Para más información, [consulte el apartado *Recuperación mediante desafío/respuesta*](#) en la página 34.

■ Icono de la bandeja del sistema de Sophos SafeGuard

Puede acceder a las principales funciones de Sophos SafeGuard a través del icono de la bandeja del sistema. El icono de Sophos se encuentra en la barra de tareas de Windows. Para más información, [consulte el apartado *Icono de la bandeja del sistema*](#) en la página 37.

■ Extensiones de Sophos SafeGuard en el Explorador de Windows

Puede acceder a las funciones de cifrado desde el menú contextual del Explorador de Windows, [consulte *Acceder a funciones desde el Explorador de Windows*](#) en la página 40.

Nota:

Puede que no todas las características que se describen en esta ayuda estén disponibles en su equipo. Esto se debe a que el responsable de seguridad define las funciones disponibles.

2 Copia de seguridad de la clave para la recuperación

Para la recuperación del inicio de sesión, Sophos SafeGuard ofrece un procedimiento de desafío/respuesta ([consulte el apartado *Recuperación mediante el procedimiento desafío/respuesta*](#) en la página 34).

Para habilitar la recuperación mediante el procedimiento de desafío/respuesta, el centro de ayuda tendrá que disponer de los datos necesarios. Los datos que hacen falta para la recuperación se guardan en archivos específicos de recuperación de claves (archivos .XML).

Cuando se aplica la configuración de Sophos SafeGuard, el archivo de recuperación de clave se crea automáticamente. Si el responsable de seguridad no indica la ubicación del archivo, se le pedirá que lo guarde manualmente.

El responsable de seguridad puede especificar una ubicación para estos archivos de seguridad al crear el paquete de configuración. Normalmente, la ubicación de este archivo es una ruta compartida. El archivo de recuperación de la clave se creará automáticamente en esta ubicación.

Si no se puede acceder a la ubicación especificada para el archivo cuando Sophos SafeGuard intenta crearlo, se notificará al usuario, se creará una entrada en el registro de eventos del sistema y Sophos SafeGuard intentará guardar el archivo más adelante. Si el responsable de seguridad no ha indicado una ubicación para el archivo, aparecerá un cuadro de diálogo para poder guardar el archivo manualmente.

Si la ubicación especificada es una unidad de red a la que no dispone de acceso con sus credenciales de Windows, se le pedirá una cuenta de acceso. El responsable de seguridad le proporcionará el nombre de usuario y la contraseña correspondientes.

Nota: guarde el archivo cuando se le pida y asegúrese de que el centro de ayuda puede acceder al mismo. El archivo está cifrado y se puede guardar en cualquier medio externo para hacerlo llegar al servicio de asistencia. También se puede enviar por correo electrónico. Si no guarda el archivo, se le solicitará que lo haga cada vez que reinicie el equipo, hasta que lo guarde.

Puede crear en cualquier momento una nueva copia de seguridad de la clave desde el icono de la bandeja del sistema de Sophos SafeGuard. Crear un nuevo archivo de recuperación de la clave puede ser necesario, por ejemplo, si los archivos de clave existentes se han dañado o ya no están a disposición del centro de ayuda.

3 POA (power-on authentication)

Con la POA, los usuarios tienen que autenticarse en la fase previa al inicio del sistema operativo. A continuación, se iniciará la sesión en Windows de forma automática. El procedimiento es el mismo cuando el equipo se vuelve a activar tras estar en hibernación (suspenden en disco).



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 realiza esta configuración desde el editor de políticas de SafeGuard.

Se pueden realizar los siguientes ajustes:

■ Imagen de inicio de sesión

La imagen predeterminada que aparece en la POA es un diseño de SafeGuard. Puede modificar la directiva para, por ejemplo, mostrar el logotipo de su empresa.

■ Texto de los cuadros de diálogo

El texto que se muestra en la POA aparece en el idioma predeterminado Windows. Para cambiar el idioma, utilice la función Configuración regional y de idioma de Windows. El responsable de seguridad también puede especificar el texto.

3.1 Primer inicio de sesión tras instalar Sophos SafeGuard

Si Sophos SafeGuard se ha instalado con POA (power-on authentication), el procedimiento de inicio será diferente en el arranque del sistema. Aparecen una serie de nuevos mensajes de inicio (como por ejemplo, la pantalla de inicio de sesión automático), debido a que Sophos SafeGuard se ha incorporado al procedimiento de arranque del sistema. Después, se iniciará el sistema operativo Windows.

La primera vez que inicie la sesión tras la instalación, debe hacerlo en Windows con sus credenciales habituales. Posteriormente, se le registrará como usuario de Sophos SafeGuard. 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, aparecerá en el equipo una información sobre herramientas que le confirmará que todo funciona sin problemas.

Cuando reinicie el equipo, se activará la POA. A partir de ese momento, debe especificar sus credenciales de Windows en la POA (power-on authentication), tras lo que se iniciará la sesión en Windows automáticamente sin tener que escribir ninguna contraseña (si está activado el inicio de sesión automático en Windows).

Podrá iniciar la sesión en la POA mediante el nombre de usuario y la contraseña de Windows.

Nota: el responsable de seguridad define la configuración de Sophos SafeGuard de forma centralizada y la aplica a las estaciones en modo de directivas.

3.2 Inicio de sesión desde la POA (power-on authentication)

Tras la correcta activación de la POA, puede iniciar la sesión mediante las credenciales de Windows desde el cuadro de la POA. La sesión de Windows se inicia automáticamente.

Nota:

Puede desactivar el inicio de sesión automático en Windows pulsando el botón **Opciones >>** en el cuadro de inicio de sesión y desactivando la opción **Inicio de sesión automático en Windows**. Puede que sea necesario desactivar el inicio de sesión automático, por ejemplo, para permitir que otros usuarios utilicen la POA en el mismo equipo ([consulte el apartado *Importar otros usuarios*](#) en la página 7). El responsable de seguridad define en las directivas relevantes si se utiliza el inicio de sesión automático en Windows y si se permite que el usuario pueda modificar las opciones del cuadro de inicio de sesión.

La POA distingue entre mayúsculas y minúsculas.

Retraso en el inicio de sesión tras un intento fallido

Si se produce un fallo en el inicio de sesión 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 inicio de sesión. El período de retraso aumentará cada vez que tenga lugar un intento de inicio de sesión fallido. Los intentos fallidos quedan registrados.

Bloqueo del equipo

De acuerdo con la configuración de directivas, es posible que su equipo quede bloqueado tras un número determinado de intentos de inicio de sesión fallidos. Para desbloquearlo, inicie un procedimiento de desafío/respuesta, [consulte el apartado Recuperación mediante el procedimiento de desafío/respuesta](#) en la página 34.

3.2.1 Ejemplo de inicio de sesión en la POA por primera vez

El procedimiento de inicio de sesión sólo corresponderá al descrito aquí si la POA ya se encuentra instalada y activada.

Según sea la configuración del sistema, se le pedirá que pulse **Ctrl+Alt+Supr.** Continuará el proceso de inicio de sesión.

1. Encienda el equipo.

Aparece el cuadro de autoinicio de sesión de la POA.

2. Aparece el cuadro de inicio de sesión de Windows. Inicie la sesión en Windows.

Ahora se ha convertido en el "propietario" del equipo. Sólo existe un propietario en cada equipo. Por defecto, el primer usuario que inicie la sesión es el propietario.

3. Si tanto las directivas del usuario como su certificado y su clave están en el equipo, Sophos SafeGuard guarda los datos del usuario.
4. Al reiniciar el equipo podrá iniciar la sesión en la POA.

Nota: por defecto, el primer usuario en iniciar la sesión en Windows se registrará como "propietario" del equipo. Según directiva aplicada, el propietario del ordenador es el único que puede permitir a otros usuarios iniciar la sesión en la POA (power-on authentication).

Si desea que otros usuarios inicien la sesión en la POA, el propietario del equipo tiene que permitirlo ([consulte el apartado Importación de otros usuarios](#) en la página 7).

El responsable de seguridad define en las directivas relevantes si se utiliza el inicio de sesión automático en Windows y si se permite que el usuario pueda modificar las opciones del cuadro de inicio de sesión.

3.3 Importar otros usuarios

Para permitir que otros usuarios de Windows puedan iniciar la sesión:

1. Encienda el equipo.

Aparecerá el cuadro de inicio de sesión de la POA. El segundo usuario de Windows en el equipo no puede iniciar la sesión en la POA ya que no tiene las claves y los certificados necesarios.

2. El propietario del equipo debe permitir a otros usuarios iniciar la sesión en la POA.

Nota: la configuración predeterminada estipula que el primer usuario que inicie la sesión tras la instalación se registrará como el propietario del equipo. El responsable de seguridad también puede definir el propietario de un ordenador mediante una directiva.

3. En el cuadro de inicio de sesión de la POA, haga clic en **Opciones** y desactive la opción **Inicio de sesión automático en Windows**.

En el cuadro de inicio de sesión de Windows, el segundo usuario puede iniciar la sesión.

4. Introduzca las credenciales de Windows del segundo usuario.
5. Sophos SafeGuard almacena los datos del segundo usuario del sistema.

La próxima vez que se inicie el equipo, el segundo usuario podrá iniciar la sesión en la POA .

3.4 Contraseña temporal de la POA

Sophos SafeGuard permite cambiar temporalmente la contraseña en la POA. Puede ser aconsejable cambiar la contraseña 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 para evitar el acceso no autorizado al sistema. Cuando se conecte de nuevo a AD, se le pedirá que cambie la contraseña temporal.

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

Nota: si no especifica la contraseña existente antes de pulsar **F8**, el sistema lo interpreta como un intento fallido de inicio de sesión y muestra un mensaje de error.

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

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

4. Haga clic en **Aceptar**.

Nota: Si cancela este diálogo, se iniciará la sesión con la contraseña anterior.

Aparecerá el cuadro de diálogo de inicio de sesión de Windows.

Nota:

La sesión no se inicia automáticamente en Windows, aunque el sistema esté configurado de esta forma. Escriba aquí la "contraseña anterior". La contraseña temporal sólo es válida para iniciar la sesión en la POA.

5. Haga clic en **Aceptar**.

Se inicia la sesión en Windows.

Para iniciar la sesión en la POA, ahora sólo puede usar la contraseña definida temporalmente. La contraseña temporal será válida hasta que la contraseña se cambie en Windows. La sesión de Windows no se iniciará de forma automática desde la POA hasta que no realice este paso.

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 inicie la sesión en Windows, Sophos SafeGuard le pedirá que cambie la contraseña tan pronto como se conecte a Active Directory.

El cuadro de diálogo que pide el cambio de contraseña puede cancelarse sin cambiar 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 de la POA. Sin embargo, puede cancelarse y la "contraseña anterior" se podrá usar para iniciar la sesión. Después, podrá cambiar la contraseña.

3.5 Inicio de sesión en la POA (power-on authentication) mediante tarjetas inteligentes o tokens

Nota:

Esta función no está disponible con ESDP (Endpoint Security and Data Protection).

Existen dos formas de iniciar la sesión utilizando tarjetas inteligentes o tokens:

- *Sólo con tarjeta inteligente o token.*
- *Con el nombre de usuario y la contraseña, o con la tarjeta inteligente o token.*

El responsable de seguridad define el tipo de inicio de sesión que se puede utilizar en las estaciones.

Nota: desde la perspectiva de Sophos SafeGuard, 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. En las secciones siguientes, utilizaremos el término "token".

3.5.1 Primer inicio de sesión con token

El primer inicio de sesión con token es igual que el inicio de sesión sin token.

Si ya dispone de un token, puede utilizarlo para iniciar la sesión en Windows.

Nota: se recomienda que configure su token con las credenciales de Windows (consulte [Almacenamiento de credenciales de Windows en el token](#) en la página 10) 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 las credenciales, no podrá iniciar la sesión en la POA (power-on authentication).

3.5.2 Almacenar las credenciales de Windows en el token

Si el token no contiene las credenciales de Windows, puede almacenarlas usted mismo.

Nota: se recomienda que configure su token en el primer inicio de sesión. Las directivas de seguridad que se le aplican pueden exigir que utilice un token en la POA. Si el token no contiene las credenciales, no podrá iniciar la sesión en la POA (power-on authentication).

1. En el primer inicio de sesión tras la instalación, conecte el token al sistema cuando aparezca el cuadro de inicio de sesión 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**.

Se intentará iniciar la sesión de Windows con los datos especificados. A continuación, los datos se transfieren al token.

Se inicia la sesión en Windows.

Si el inicio de sesión mediante token es opcional (ya ha iniciado la sesión en la POA con su nombre de usuario y contraseña), puede generar el token en cualquier otro momento.

Para hacerlo, en el cuadro de inicio de sesión de la POA, haga clic en **Opciones** y desactive la opción **Inicio de sesión automático en Windows**. Se mostrará el cuadro de inicio de sesión de Windows y podrá almacenar los datos en el token como se ha descrito anteriormente.

3.5.3 Inicio de sesión en la POA con token

Requisitos previos: Asegúrese de que en la BIOS esté activada la compatibilidad con USB. Debe inicializarse la compatibilidad con el token y se le debe proporcionar uno.

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

Se muestra el cuadro de inicio de sesión con 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 no aparece el cuadro para este tipo de inicio de sesión, sólo podrá hacerlo mediante el token.

3. Introduzca el número PIN del token.

Se inicia la sesión en la POA y en Windows (si tiene activada la opción **Inicio de sesión automático en Windows**).

3.5.4 Cambiar el número PIN

El número PIN del token se puede cambiar en el cuadro de inicio de sesión de Windows.

Si la opción **Inicio de sesión automático en Windows** está activada en la POA (power-on authentication), no se mostrará el cuadro de inicio de sesión de Windows. Para que se muestre el cuadro de inicio de sesión de Windows, tendrá que desactivar esta opción en la POA.

Nota: si el responsable de seguridad ha definido reglas que requieran un cambio de número PIN (por ejemplo, a intervalos de tiempo concretos), se le comunicará cuando sea necesario.

1. En el cuadro de diálogo **PIN** que se emplea para iniciar la sesión en 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**.

Se cambia el número PIN del token y se inicia al sesión en Windows.

3.5.5 Recuperación de inicio de sesión mediante token

Si ha olvidado el PIN, puede volver a tener acceso a su equipo de dos formas:

- Recuperación mediante Local Self Help, [consulte el apartado Recuperación mediante Local Self Help](#) en la página 26.
- Recuperación mediante desafío/respuesta, [consulte el apartado Recuperación mediante el procedimiento de desafío/respuesta](#) en la página 34.

El método de recuperación disponible depende de la directiva de seguridad aplicada.

Para iniciar el proceso de recuperación, haga clic en el botón **Recuperación** del cuadro de inicio de sesión.

3.5.6 Desbloquear el token

Si introduce el número PIN incorrectamente varias veces, el token se bloqueará. El responsable de seguridad puede configurar Sophos SafeGuard para que el usuario pueda desbloquear el token.

El responsable de seguridad le proporcionará el PIN del administrador para su token.

1. En el cuadro de diálogo **Desbloquear token**, introduzca el PIN del administrador.
2. Especifique un número PIN nuevo y confírmelo.

El número PIN estará sujeto a las reglas establecidas en su empresa (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 se iniciará la sesión.

Nota:

Si esta función no está disponible en el equipo, puede utilizar un procedimiento de desafío/respuesta. A través del procedimiento de desafío/respuesta, puede volver a obtener acceso a su equipo.

3.5.7 Conexión mediante Escritorio remoto

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

La captura remota no es posible en este caso.

3.6 Recuperación de inicio de sesión

Para la recuperación del inicio de sesión (por ejemplo, si ha olvidado la contraseña), Sophos SafeGuard ofrece varias opciones adaptadas a distintos escenarios: El método de recuperación disponible depende de la directiva de seguridad aplicada. Para más información, [consulte el apartado *Opciones de recuperación*](#) en la página 25.

3.7 Teclado virtual

En la POA, se puede utilizar un teclado virtual para poder introducir texto desde la pantalla.

Requisito previo: el responsable de seguridad debe habilitar esta opción.

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 ([consulte *Cambio de la distribución del teclado*](#) en la página 12).

3.8 Distribución del teclado

La práctica mayoría de los países cuenta con una distribución de teclado propio. La distribución del teclado de la POA es importante a la hora de introducir nombres de usuarios, contraseñas y códigos de respuesta.

Por defecto, Sophos SafeGuard utiliza el teclado predeterminado de Windows. 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, por ejemplo, "EN" representa el inglés. Además de la distribución predeterminada del teclado, también se puede utilizar la distribución US (inglés, Estados Unidos).

3.8.1 Cambiar la distribución del teclado

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

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 recuerda la distribución del teclado de la última sesión. Para esto es necesario reiniciar dos veces el equipo. Si se desactiva la anterior distribución del teclado desde la **Configuración regional y de idioma**, se sigue manteniendo a no ser que seleccione una diferente.

Nota:

También debe 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 mediante 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**.

3.9 Teclas de acceso rápido y de función compatibles en la POA (power-on authentication)

Ciertas funciones y configuración del hardware pueden causar problemas al arrancar el equipo, provocando a su vez que se bloquee el sistema. La POA permite disponer de una serie de teclas de acceso rápido para modificar la configuración del hardware y desactivar ciertas funciones. Además, el archivo de configuración .msi incluye una lista con configuraciones y funcionalidades de hardware que se sabe que pueden causar problemas.

Se recomienda obtener la última versión de configuración de la POA antes de una nueva distribución de Sophos SafeGuard en la red. El archivo de configuración se actualiza cada mes y está disponible en: <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

Puede modificar este archivo para ajustarse a sus necesidades.

Nota:

El archivo personalizado se utilizará en vez del archivo .msi predeterminado. La configuración predeterminada sólo se aplica si no existe ningún otro archivo de configuración de la POA.

Para aplicar un archivo de configuración de la POA, utilice el siguiente comando:

MSIEXEC /i <paquete MSI cliente> POACFG=<archivo de configuración POA>

Para más información, consulte <http://esp.sophos.com/support/knowledgebase/article/65700.html>.

POA también es compatible con ciertas teclas de función.

3.9.1 Teclas de acceso rápido

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 de acceso rápido

Mayús - F3	Mayús - F3	Mayús - F7	Heredado	USB 1.x	USB 2.0	Comentario
desactivado	desactivado	desactivado	activado	activado	activado	3.
activado	desactivado	desactivado	desactivado	activado	activado	Predefinido
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** deshabilita USB 1.x y USB 2.0.

Nota: si se pulsa **Mayús - F5** durante el arranque, se reduce considerablemente el tiempo de inicio de 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**.

La POA puede utilizar el teclado USB mediante el BIOS SMM. No es posible utilizar 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. 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. Dependiendo de la versión de BIOS utilizada, el sistema podría no responder.

Nota: los cambios que se pueden realizar con las teclas de acceso rápido es posible que ya se encuentren en el archivo de configuración **.mst** de Sophos SafeGuard.

Tras modificar la configuración de hardware con las teclas de acceso rápido en la POA, se muestra un cuadro de diálogo desde el que puede guardar los cambios. 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 seguirá utilizándose la configuración anterior una vez que se reinicie el equipo.

Si pulsa **F5** en cualquier cuadro de diálogo de la POA, se mostrará un cuadro con las teclas de acceso rápido a la POA. Si se han cambiado las teclas de acceso rápido durante el arranque, 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 valores sin modificar se mostrarán en negro. Para cerrar el cuadro de diálogo, pulse **F5** de nuevo o pulse **Intro**.

3.9.2 Teclas de función en el cuadro de inicio de sesión

Nota: las teclas de función no son teclas de acceso rápido.

F2 = cancela el inicio de sesión automático.

F5 = muestra un cuadro con las teclas de acceso rápido disponibles en la POA.

F8 = permite cambiar la contraseña de la POA. Se debe utilizar en lugar de la tecla **Intro** para activar el cambio de contraseña en la POA tras el inicio de sesión.

Alt + Mayús (las teclas **Alt** y **Mayús** situadas a la izquierda en el teclado) = cambiar 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 ordenador de forma segura. Esta combinación de teclas tiene la misma función que el botón **Apagar**.

Nota: si está activado el inicio de sesión mediante huella digital, puede utilizar la combinación **Ctrl + Alt + Supr** para cambiar a la POA de inicio de sesión con nombre de usuario y contraseña. Para más información sobre el inicio de sesión mediante huella digital, [consulte el apartado Inicio de sesión con el lector de huellas digitales de Lenovo](#) en la página 19.

3.10 Sincronización de la contraseña

Sophos SafeGuard 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 VPN, en otro equipo o en Active Directory.

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

La sincronización de la contraseña se producirá en dos situaciones:

- durante el inicio de sesión
- durante un procedimiento de bloqueo/desbloqueo de Windows

4 POA (power-on authentication) en Windows Vista y Windows 7

La POA en Windows Vista y Windows 7 tiene el mismo aspecto y funciona igual que en Windows XP. Solamente aparecen diferencias al iniciar la sesión en el sistema operativo.

Nota: en esta sección sólo se describen las diferencias relativas a Windows Vista y Windows 7. A menos que se indique lo contrario, se aplican los mismos procedimientos y procesos descritos en la sección sobre la POA ([consulte POA \(power-on authentication\)](#) en la página 5).

4.1 Primer inicio de sesión tras instalar Sophos SafeGuard en Windows Vista o Windows 7

Si Sophos SafeGuard se ha instalado con POA (power-on authentication), el procedimiento de inicio será diferente en el arranque del sistema. Aparecen una serie de nuevos mensajes de inicio (como por ejemplo, la pantalla de inicio de sesión automático), debido a que Sophos SafeGuard se ha incorporado al procedimiento de arranque del sistema. Después, se iniciará el sistema operativo Windows.

Nota: en Windows Vista y Windows 7, primero debe pulsar **Ctrl + Alt + Supr** para iniciar la sesión. 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** (para el inicio de sesión interactivo no es necesario **Ctrl+Alt+Supr**).

La primera vez que inicie la sesión tras la instalación, debe hacerlo en Windows con sus credenciales habituales. Posteriormente, se le registrará como usuario de Sophos SafeGuard. Este proceso de registro es necesario para asegurarse de que la POA reconozca sus credenciales la próxima vez que el sistema se inicie.

Tras iniciar la sesión, se le informa al usuario.

Cuando reinicie el equipo, se activará la POA. A partir de ese momento, debe especificar sus credenciales de Windows en la POA (power-on authentication), tras lo que se iniciará la sesión en Windows automáticamente sin tener que escribir ninguna contraseña (si está activado el inicio de sesión automático en Windows).

Puede iniciar la sesión en la POA mediante el nombre de usuario y la contraseña.

Nota: el responsable de seguridad define la configuración de forma centralizada y la aplica a las estaciones en modo de directivas.

4.1.1 Procedimiento del primer inicio de sesión

En esta sección se describe el primer inicio de sesión tras instalar Sophos SafeGuard. El procedimiento sólo corresponderá al descrito aquí si la POA ya se encuentra instalada y activada.

1. Se inicia el equipo y aparece el cuadro de autoinicio de sesión de Sophos SafeGuard.

Se realiza el autoinicio.

2. Aparece el cuadro de inicio de sesión de Windows Vista/Windows 7.

En Windows Vista/Windows 7, Sophos SafeGuard ofrece un método alternativo de autenticación.

3. Windows Vista y Windows 7 muestra un icono para cada método de autenticación:

- Haga clic en **Otro usuario** para introducir las credenciales.
- Haga clic en el segundo icono (con un nombre debajo) para ver la información del último usuario que inició la sesión. Sólo tiene que introducir la contraseña.

Si el nombre de usuario aparece debajo de un icono de SafeGuard Enterprise, seleccione dicho icono. De lo contrario, seleccione el icono **Otro usuario**.

4. Introduzca sus credenciales de usuario de Windows de la forma habitual.

La próxima vez que se inicie el sistema, sólo tendrá que introducir sus credenciales de Windows (nombre de usuario y contraseña) en la POA.

Para activar la POA, es necesario reiniciar el sistema. Tras el reinicio, el inicio de sesión se realiza a través de la POA.

4.2 Inicio de sesión en la POA (power-on authentication) en Windows Vista y Windows 7

Tras la correcta activación de la POA (sincronización inicial y reinicio), puede iniciar la sesión mediante las credenciales de Windows desde el cuadro de la POA. La sesión de Windows se inicia automáticamente.

Nota: para desactivar el inicio de sesión automático en Windows, haga clic en **Opciones >>** en el cuadro de la POA y desactive la opción **Inicio de sesión automático en Windows**. Puede que sea necesario desactivar el inicio de sesión automático, por ejemplo, para permitir que otros usuarios utilicen la POA en el mismo equipo ([consulte el apartado Importación de otros usuarios](#) en la página 7). El responsable de seguridad define en las directivas relevantes si se utiliza el inicio de sesión automático en Windows y si se permite que el usuario pueda modificar las opciones del cuadro de inicio de sesión.

Retraso en el inicio de sesión tras un intento fallido

Si se produce un fallo en el inicio de sesión 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 inicio de sesión. El período de retraso aumentará cada vez que tenga lugar un intento de inicio de sesión fallido. Los intentos fallidos quedan registrados.

Bloqueo del equipo

De acuerdo con la configuración de directivas, es posible que su equipo quede bloqueado tras un número determinado de intentos de inicio de sesión fallidos. Para desbloquearlo, inicie un procedimiento de desafío/respuesta, [consulte el apartado Recuperación mediante el procedimiento de desafío/respuesta](#) en la página 34.

5 Inicio de sesión en Windows Vista y Windows 7

En Windows Vista y Windows 7, Sophos SafeGuard ofrece un método de autenticación adicional.

Si desactiva la opción **Inicio de sesión automático en Windows** en la POA (power-on authentication), se mostrará el cuadro de inicio de sesión de Windows Vista o Windows 7. En este cuadro de diálogo también puede seleccionar un método de autenticación distinto.

Nota: el uso de otro método de autenticación no significa que Sophos SafeGuard se encuentra inactivo. En ese caso, el inicio de sesión de Sophos SafeGuard se realiza tras el inicio del sistema.

5.1 Iniciar la sesión con Sophos SafeGuard

Normalmente, la sesión de Windows se inicia de forma automática tras autenticarse en la POA (power-on authentication). Si desactiva la opción **Inicio de sesión automático en Windows** en el cuadro de inicio de sesión de la POA y utiliza el método alternativo de Sophos SafeGuard para iniciar la sesión en Windows, Sophos SafeGuard sólo estará disponible tras iniciar la sesión en Windows Vista o Windows 7.

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

5.2 Iniciar la sesión con la autenticación de Windows Vista/Windows 7

En el cuadro de inicio de sesión de Windows puede utilizar la autenticación de Windows, en lugar del método de autenticación de Sophos SafeGuard.

En este caso, la sesión de Sophos SafeGuard se activa tras iniciarse el sistema operativo.

Después de iniciar la sesión en Windows Vista/Windows 7, se ejecutará el programa de autenticación de Sophos SafeGuard si es necesario.

En función de la configuración aplicada, deberá introducir las credenciales de usuario o el número PIN.

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

Se activa Sophos SafeGuard para acceder a los datos cifrados (siempre que se tenga la clave necesaria).

5.3 Sincronización de contraseñas en Windows Vista y Windows 7

Sophos SafeGuard 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 VPN, en otro equipo o en Active Directory.

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

La sincronización de la contraseña se producirá en dos situaciones:

- durante el inicio de sesión
- durante un procedimiento de bloqueo/desbloqueo de Windows

6 Conexión con el Lector de huellas digitales de Lenovo

Nota:

Esta función no está disponible con ESDP (Endpoint Security and Data Protection).

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.

No podrá perder ni olvidar sus credenciales. También será imposible la suplantación de otro usuario. Así, el uso de lectores de huellas digitales simplifica el proceso de conexión y aumenta la seguridad.

Sophos SafeGuard permite la autenticación mediante huella digital en POA (power-on-authentication) 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.

Nota:

- Un ordenador sólo puede tener conectado un lector de huellas digitales a la vez.
- No se admite la conexión remota mediante huella digital.

6.1 Requisitos

Estos son los requisitos para disponer de inicio de sesión mediante huella digital:

Requisitos generales

- Hardware de Lenovo.
- Lector de huellas digitales de Lenovo en el portátil o en un teclado USB
- Se recomienda disponer de la BIOS más actualizada.
- Sophos SafeGuard
- El software del fabricante debe estar instalado antes de instalar Sophos SafeGuard:
 - ThinkVantage Fingerprint para AuthenTec
 - o
 - ThinkVantage Fingerprint para UPEK.
- El responsable de seguridad debe activar el uso de inicio de sesión mediante huella digital.

Requisitos del sistema

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

Hardware compatible

Para más información sobre el hardware compatible, consulte el artículo <http://esp.sophos.com/support/knowledgebase/article/108789.html>.

Software compatible

Para más información sobre el software compatible, consulte el artículo <http://esp.sophos.com/support/knowledgebase/article/111626.html>.

6.2 Registrar 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 asocia su huella digital 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 Sophos SafeGuard.

1. autentíquese en la POA (power-on authentication) 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 UPEK. Para AuthenTec este paso no es necesario.)
 - c) Para poder utilizar el inicio de sesión mediante huella digital en la POA, primero debe iniciar la sesión en 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 el primer inicio de sesión.
3. Reinicie el sistema.
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 iniciará la sesión en Windows de forma automática.

6.3 Iniciar la sesión en la POA (power-on authentication) mediante huella digital

Requisitos previos:

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

1. Reinicie el ordenador.

Se muestra la POA para iniciar la sesión con la huella digital.

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

Si el software reconoce la huella, la POA (power-on authentication) leerá las credenciales y las enviará a Windows.

Nota: el procedimiento de inicio de sesión utiliza iconos con mensajes cortos de texto, como solicitudes, notificaciones y advertencias ([consulte el apartado Iconos utilizados en el proceso de conexión](#) en la página 21).

Se iniciará la sesión en Windows sin que se le pidan más datos.

Nota:


- 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 reiniciado la sesión en Windows), la POA reconocerá la huella digital.







No obstante, no habrá ninguna credencial asociada. En este caso, se mostrará un mensaje de error, en el que se le solicitará que inicie la sesión con el nombre de usuario y contraseña, aunque sin inicio de sesión en Windows. Sus credenciales se transferirán al lector de huellas digitales.




- El responsable de seguridad especifica en las directivas que le afectan si se habilita el inicio de sesión en Windows y si se le permite cambiar esta opción en el cuadro de diálogo de la POA para iniciar la sesión con el nombre de usuario y contraseña ([consulte el apartado Inicio de sesión con nombre de usuario y contraseña](#) en la página 23).

6.3.1 Iconos utilizados en el proceso de inicio de sesión

Cuando se inicia sesión en la POA (power-on authentication) con huella digital, el sistema utiliza iconos como instrucciones, notificaciones y advertencias. Estos iconos se muestran durante el proceso de inicio de sesión junto a un mensaje corto de texto.

	<p>Le solicita que pase el dedo sobre el lector de huellas digitales.</p>
---	---

	Indica que el inicio de sesión mediante huella digital no está activada en esos momentos. Esto puede suceder, por ejemplo, si el módulo de inicio de sesión 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.

	
	<p>Indica que ha movido el dedo demasiado rápido. Vuelva a pasar el dedo por el lector de huellas digitales.</p>
	<p>Indica que no ha dejado el dedo en el lector tiempo suficiente. Vuelva a pasar el dedo por el lector de huellas digitales.</p>

6.3.2 Intentos fallidos de inicio de sesión

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

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

El período de retraso aumenta con cada intento fallido de inicio de sesión.

6.3.3 Iniciar la sesión con nombre de usuario y contraseña

Aunque el inicio de sesión mediante huella digital esté habilitada, también puede autenticarse con el nombre de usuario y contraseña, por ejemplo, en el caso de que no pueda conectarse con la huella digital porque el lector esté dañado.

1. Pulse la tecla **Esc** o bien **Ctrl+Alt+Supr** en la POA.

Aparecerá la POA para iniciar la sesión con el nombre de usuario y la contraseña.

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

El cuadro de la POA para el inicio de sesión 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: el inicio de sesión con nombre de usuario y contraseña también se habilita automáticamente si la caché local está dañada. Si esto ocurre, el equipo se bloqueará y deberá iniciar la sesión mediante un procedimiento de desafío/respuesta.

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

Si ha pulsado **Esc** para activar el cuadro de la POA para iniciar la sesión con el nombre de usuario y la contraseña, podrá iniciar la sesión 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.

6.4 Cambiar la contraseña

1. Si está habilitado el inicio de sesión en la POA (power-on authentication), 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.

6.4.1 Sincronizar 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 la POA. De esta forma se abre el cuadro de inicio de sesión mediante nombre de usuario y contraseña.
3. Haga clic en **Opciones** y desactive la **Inicio de sesión automático en Windows**.

Nota: el responsable de seguridad específica en las directivas si se habilita el inicio de sesión automático en Windows y si se le permite cambiar esta opción en la POA.

4. Inicie la sesión con su contraseña.

5. Aparecerá el cuadro de diálogo de inicio de sesión de Windows. Pase uno de los dedos registrados sobre el lector de huellas digitales.
6. El sistema reconocerá la huella digital, pero Windows rechazará la contraseña asociada a la huella. Esto no se considera como un intento fallido de inicio de sesión, por lo que se no se aplica un retraso.

Se mostrará un mensaje que indica que se ha cambiado la contraseña y el sistema le solicitará que introduzca la contraseña actual de Windows.

7. Introduzca la contraseña actual de Windows.

Nota:

Si introduce aquí una contraseña incorrecta de Windows, se registrará como intento fallido de conexión y se aplicará el retraso. Si cierra el cuadro sin introducir una contraseña, también se registra como intento fallido de inicio de sesión y se aplica el retraso.

Se completará el proceso de sincronización y podrá utilizar la contraseña para iniciar la sesión.

6.5 Recuperación de inicio de sesión mediante huella digital

Si el inicio de sesión mediante huella digital no funciona y se le ha olvidado la contraseña, Sophos SafeGuard dispone de los siguientes métodos de recuperación:

- Recuperación mediante Local Self Help, [consulte el apartado *Recuperación mediante Local Self Help*](#) en la página 26.
- Recuperación mediante desafío/respuesta, [consulte el apartado *Recuperación mediante el procedimiento de desafío/respuesta*](#) en la página 34.

El método de recuperación disponible depende de la directiva de seguridad aplicada.

Para iniciar el proceso de recuperación, haga clic en el botón **Recuperación** del cuadro de inicio de sesión de la POA.

Nota:

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.

7 Opciones de recuperación

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

- **Recuperación de inicio de sesión 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 iniciar la sesión, no tiene más que responder a una serie de preguntas en la POA (power-on authentication).

Para más información, [consulte el apartado Recuperación mediante Local Self Help](#) en la página 26.

■ **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.

Para más información, [consulte el apartado Recuperación mediante desafío/respuesta](#) en la página 34.

El responsable de seguridad define, mediante directivas, el tipo de recuperación disponible en los equipos.

8 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, Sophos SafeGuard pone Local Self Help a su disposición.

Al utilizar Local Self Help, puede volver a tener acceso a su equipo 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 responsable de seguridad puede definir las preguntas y distribuirlas a los equipos de los usuarios. También puede definir sus propias preguntas, siempre y cuando la directiva aplicable le permita hacerlo. El asistente de Local Self Help permite introducir las respuestas y editar las preguntas. Puede abrir el asistente de Local Self Help desde el icono de la bandeja del sistema de Sophos SafeGuard.

La recuperación mediante Local Self Help está disponible en los siguientes casos:

- Inicio de sesión con ID y contraseña
- Inicio de sesión con huella digital
- Inicio de sesión con token no criptográfico, si tiene disponible el inicio de sesión con ID y contraseña.

Nota:

Esta función no está disponible con ESDP (Endpoint Security and Data Protection).

Requisitos previos

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

- El responsable de seguridad ha habilitado Local Self Help en la directiva aplicable y ha definido la configuración de esta función (por ejemplo, los permisos necesarios para definir sus propias preguntas).

- Ha activado Local Self Help en su equipo (*consulte el apartado [Activar Local Self Help](#) en la página 27*).

8.1 Activar 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 el número mínimo de preguntas establecido. El número mínimo de preguntas lo define el responsable de seguridad. El asistente de Local Self Help le guiará en el proceso y le indicará el número de preguntas que necesita. 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 las preguntas necesarias. El asistente de Local Self Help le indicará el número de preguntas que necesita.

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

Responda y guarde las preguntas necesarias (predefinidas, sus propias preguntas 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 las preguntas necesarias.

Nota: para iniciar la sesión en la POA (power-on authentication) mediante Local Self Help, debe responder a preguntas seleccionadas aleatoriamente. El número mínimo de preguntas lo define el responsable de seguridad.

Requisitos previos: Tras recibir la directiva, se le informará de que existen preguntas de Local Self Help sin responder. Reinicie el equipo para que se añada el comando **Local Self Help** al menú contextual del icono de la bandeja del sistema.

Para activar Local Self Help:

1. Haga clic con el botón derecho en el icono de SafeGuard Enterprise en la bandeja del sistema.
2. Seleccione **Local Self Help**.

Se inicia el asistente de **Local Self Help**.

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

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

Se muestra el cuadro de diálogo **Descripción del estado**.

Este cuadro de diálogo indica cómo activar Local Self Help. Además, muestra información de estado (por ejemplo, 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, se mostrará el cuadro de diálogo **Preguntas predefinidas**.

- Si ha recibido diferentes temas de preguntas, seleccione el tema en la lista desplegable **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: al responder las preguntas durante el proceso de recuperación en la POA (power-on authentication), deberá escribir las respuestas de la misma manera. Por ejemplo, se distingue entre mayúsculas y minúsculas.

Nota:

Si va a escribir las respuestas en japonés, debe utilizar los caracteres Romaji (Roman). 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 **Siguiente**.

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 pregunta nueva, 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:

Al responder las preguntas durante el proceso de recuperación en la POA (power-on authentication), deberá escribir las respuestas de la misma manera. Por ejemplo, se distingue entre mayúsculas y minúsculas.

Nota:

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

En la última página del asistente de Local Self Help se muestra la información de estado. Se indicará si se cumplen los requisitos para activar Local Self Help.

8. Haga clic en **Finalizar**.

Se guardarán tanto las preguntas como las respuestas. Se indicará si 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 (power-on authentication).

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 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.

8.2 Editar 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 establecidas. Sin embargo, las preguntas predefinidas no pueden eliminarse.
- Con respecto a las preguntas definidas por el usuario, puede modificar las respuestas, eliminar preguntas o agregar otras nuevas.

1. Haga clic con el botón derecho en el icono de Sophos SafeGuard en la bandeja del sistema.
2. Seleccione **Local Self Help**.

Se inicia el asistente de **Local Self Help**.

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

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

Se muestra el cuadro de diálogo **Descripción del estado**.

Este cuadro de diálogo indica cómo activar Local Self Help. Además, muestra información de estado (por ejemplo, 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 diferentes temas de preguntas, seleccione el tema en la lista desplegable **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, active la opción **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, active la opción **Mostrar respuestas**.

a) Para cambiar las respuestas existentes, haga clic en cada pregunta y escriba la nueva respuesta en la columna **Respuestas**.

b) Para agregar una pregunta nueva, 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, selecciónela y haga clic en **Eliminar pregunta**.

Se pedirá confirmación. Haga clic en **Sí**.

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

En la última página del asistente de Local Self Help se muestra la información de estado. Se indicará si se cumplen los requisitos para que Local Self Help permanezca activo.

8. Haga clic en **Finalizar**.

Se guardarán tanto las preguntas como las respuestas. Se indicará si Local Self Help permanece activo tras los cambios.

9. Haga clic en **Aceptar**.

Las modificaciones entran en vigor.

La próxima vez que inicie Local Self Help en la POA (power-on authentication), se utilizarán las preguntas nuevas o modificadas. Se aplicarán las preguntas nuevas o modificadas.

Nota:

Si el número de preguntas contestadas es inferior al número mínimo necesario, Local Self Help se desactivará.

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 es inferior al necesario, Local Self Help se desactivará. Para volver a activar Local Self Help, [consulte el apartado Activar Local Self Help](#) en la página 27.

8.3 Cambios en los parámetros de preguntas

El responsable de seguridad puede definir los siguientes parámetros de Local Self Help:

- El número de preguntas que debe responder para activar Local Self Help. El número de respuestas para que Local Self Help siga activo.
- El número de preguntas que debe responder en la POA para iniciar la sesión con Local Self Help. Las preguntas que aparecen en la POA se seleccionan de forma aleatoria.

Si estos parámetros cambian, se pueden dar los siguientes escenarios:

Condición	Acción de LSH	Acción del usuario
Se reduce el número de preguntas con respuesta necesario para utilizar Local Self Help.	Local Self Help seguirá activo en el equipo.	Ninguna
Se incrementa el número de preguntas con respuesta necesario para utilizar Local Self Help.	Se indicará al usuario que ha cambiado la configuración de Local Self Help. Las preguntas disponibles no son válidas. Local Self Help ya no estará activo en su equipo.	Utilice el asistente de Local Self Help para volver a activarlo.
Cambia el número de preguntas que debe responder en la POA para iniciar la sesión con Local Self Help.	Se indicará al usuario que ha cambiado la configuración de Local Self Help. Las preguntas disponibles siguen siendo válidas. Cambia el índice de	Siga las instrucciones del asistente de Local Self Help.

Condición	Acción de LSH	Acción del usuario
	preguntas disponibles y respuestas.	

8.4 Cambio de condiciones o parámetros en Local Self Help durante la edición

Los parámetros de Local Self Help podrían cambiar mientras se están definiendo las preguntas en el asistente de Local Self Help. Por ejemplo, se podría aplicar una nueva política de Local Self Help y/o nuevas preguntas.

Si esto ocurre, puede que se pierdan las preguntas y respuestas definidas y que Local Self Help no se pueda activar con los datos existentes.

El asistente de Local Self Help comprueba las siguientes condiciones e inicia la acción necesaria:

Condición	Acción	Result
Una nueva directiva global ha desactivado Local Self Help.	El asistente de Local Self Help informa al usuario y se cierra.	Ya no se puede utilizar Local Self Help.
Una nueva directiva ha cambiado los parámetros de Local Self Help (por ejemplo, la longitud de las preguntas, el permiso para definir las mismas). Local Self Help sigue activo. Las preguntas y respuestas definidas son válidas y Local Self Help sigue activo.	El asistente de Local Self Help informa al usuario y se cierra.	Local Self Help estará activo en su equipo. Sin embargo, puede haber cambiado el índice de preguntas disponibles y respuestas. Para equilibrar esta situación, puede que tenga que añadir o borrar preguntas y/o respuestas.
Una nueva directiva ha cambiado los parámetros de Local Self Help (por ejemplo, la longitud de las preguntas, el permiso para definir las mismas). Local Self Help sigue activo. Sin embargo, las preguntas y respuestas definidas no son válidas y no existen suficientes preguntas para mantener Local Self Help activo.	El asistente de Local Self Help informa al usuario y se cierra. Local Self Help ya no estará activo en su equipo. Tendrá que volver a iniciar el asistente. El asistente se cierra.	Para activar Local Self Help, vuelva a iniciar el asistente y defina las preguntas y respuestas necesarias. Local Self Help estará disponible cuando complete el asistente.

8.5 Iniciar la sesión en la POA mediante Local Self Help

1. En la POA, 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**.

Nota:

Si normalmente inicia la sesión en la POA con PIN o smartcard, primero deberá retirar el PIN/smartcard. Aparecerá la POA para iniciar la sesión con el nombre de usuario y la contraseña. Introduzca la identificación de usuario y haga clic en **Recuperación**.

Nota:

Esta función no está disponible con ESDP (Endpoint Security and Data Protection).

Aparecerá el cuadro de bienvenida de **Local Self Help**.

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

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

Se muestra la primera pregunta.
3. 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**.
4. 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.
5. Responda a todas las preguntas. Cuando responda a la última, haga clic en **Aceptar**.

El siguiente cuadro de diálogo mostrará su contraseña actual.
6. Para visualizar la contraseña, pulse Intro o la barra espaciadora, o bien haga clic en el cuadro azul.

Nota:

NO haga clic en **Aceptar**. Si hace 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 de que nadie pueda ver el contenido de la pantalla. Puede ocultar inmediatamente la contraseña pulsando la **barra espaciadora**, **Intro** o haciendo clic en el cuadro azul.

7. Puede utilizar esta contraseña para iniciar la sesión en la POA (power-on authentication) y en Windows.
8. 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.

Se inicia la sesión en la POA y en Windows

8.6 Intentos fallidos de inicio de sesión

Si alguna de las respuestas es incorrecta, no podrá iniciar la sesión. En este caso, aparece un mensaje en el que se indica que se ha producido un fallo en el inicio de sesión. 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 el intento de inicio de sesión. El período de retraso aumenta con cada intento fallido de inicio de sesión.

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

9 Recuperación mediante el procedimiento de desafío/respuesta

Para la recuperación, Sophos SafeGuard ofrece un **procedimiento de desafío/respuesta** para intercambiar información de forma confidencial.

Nota:

Se recomienda utilizar Local Self Help si ha olvidado la contraseña. Si utiliza Local Self Help podrá seguir utilizando la contraseña existente. De esta forma se ahorra tener que cambiar la contraseña y evita tener que ponerse en contacto con el 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.

La recuperación mediante Local Self Help está disponible en los siguientes casos:

- Inicio de sesión con ID y contraseña
- Inicio de sesión con huella digital

Nota:

Esta función no está disponible con ESDP (Endpoint Security and Data Protection).

9.1 Requisitos previos

Un requisito previo para la recuperación del inicio de sesión mediante el procedimiento de desafío/respuesta es que el centro de ayuda pueda acceder al archivo de recuperación de la clave. Estos archivos deben proporcionarse al servicio de asistencia a través de rutas compartidas, correo electrónico u otros medios.

Si ha olvidado la contraseña, debe existir otra cuenta de usuario disponible en el equipo para poderla restaurar. También puede utilizar un disco de recuperación de contraseñas.

El procedimiento de desafío/respuesta le permitirá iniciar la sesión en la POA (power-on authentication). También puede iniciar la sesión en Windows, incluso si es necesario restablecer la contraseña de Windows.

9.2 Ha escrito una contraseña incorrecta demasiadas veces

Si ha introducido demasiadas veces una contraseña incorrecta, el procedimiento desafío/respuesta le permitirá iniciar la sesión en la POA (power-on authentication). A continuación, aparece el cuadro de diálogo de inicio de sesión de Windows. Puede introducir sus credenciales de Windows en este cuadro de diálogo.

El contador del número máximo de intentos de introducción de contraseña permitidos se pone a cero.

9.3 Ha olvidado la contraseña

Tras recuperar una contraseña mediante el procedimiento de desafío/respuesta, deberá cambiar la contraseña.

Nota:

Si utiliza Local Self Help podrá seguir utilizando la contraseña existente. De esta forma se ahorra tener que cambiar la contraseña y evita tener que ponerse en contacto con el centro de ayuda. Para más información, [consulte el apartado *Recuperación mediante Local Self Help*](#) en la página 26.

1. Inicie el procedimiento de desafío/respuesta y siga las instrucciones en pantalla. Podrá iniciar la sesión a través de la POA (power-on authentication).
2. No conoce la contraseña de Windows. Deberá recuperar la contraseña de Windows. Este procedimiento no se engloba en el uso de Sophos SafeGuard.

Existen dos métodos para restablecer la contraseña en Windows.

- A través de una cuenta de servicio o de administrador disponible en su equipo con los permisos de Windows necesarios.
- A través de un disco de recuperación de contraseñas de Windows.

El responsable del centro de ayuda le indicará el procedimiento que se debe utilizar y le proporcionará credenciales de Windows adicionales o el disco correspondiente.

3. Utilice las credenciales proporcionadas para iniciar la sesión en Windows y cambie su contraseña inmediatamente.

Sophos SafeGuard detectará el cambio de contraseña. Se le pedirá que introduzca la contraseña anterior.

4. Si ha modificado usted mismo la contraseña de Windows y aún conoce la contraseña anterior, podrá modificar la contraseña de Sophos SafeGuard. Si éste no es el caso, haga clic en **Cancelar**.

Si no conoce la contraseña anterior, necesita un nuevo certificado para poder cambiar la contraseña de Sophos SafeGuard. Debe confirmar este procedimiento. Se creará un nuevo certificado basado en la nueva contraseña de Windows. Esto le permitirá iniciar la sesión en el equipo con la nueva contraseña.

5. Inicie la sesión en la POA con la nueva contraseña.

Nota:

Claves de SafeGuard Data Exchange: Si ha olvidado la contraseña de Windows y debe restablecerla, no podrá utilizar las claves de SafeGuard Data Exchange creadas previamente sin las frases de acceso correspondientes. Para seguir utilizando las claves de usuario de SafeGuard Data Exchange generadas previamente, debe recordar las frases de acceso de SafeGuard Data Exchange para volver a activar dichas claves.

SafeGuard Data Exchange no está disponible con ESDP (Endpoint Security and Data Protection).

9.4 Ya no puede acceder a su equipo

Si ya no le es posible acceder al equipo, tal vez se deba a que la POA (power-on authentication) esté dañada. Incluso en esta situación tan preocupante, Sophos SafeGuard 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 del entorno WinPE. Si se encuentra en este tipo de situación, póngase en contacto con el centro de ayuda de Sophos SafeGuard. 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.

9.5 Procedimiento de desafío/respuesta

Se debe iniciar el procedimiento de desafío/respuesta:

- si ha introducido demasiadas veces una contraseña incorrecta.
- si ha olvidado su contraseña.
- para reparar una caché dañada.

Nota:

La recuperación del inicio de sesión se desactiva, de forma predeterminada, cuando la memoria caché local presenta daños. Se restaurará de forma automática a partir de la copia de seguridad. En este caso, no es necesario iniciar un procedimiento de desafío/respuesta para reparar la

memoria caché local. Sin embargo, la recuperación del inicio de sesión se puede activar a través de una directiva, si es que la memoria caché local debe repararse explícitamente mediante un procedimiento de desafío/respuesta. En tal caso, se le solicitará que inicie un procedimiento de desafío/respuesta.

Nota:

Tras iniciar el desafío, dispone de 30 minutos para introducir la respuesta generada desde el centro de ayuda. A los 30 minutos, el código de respuesta dejará de ser válido y no se podrá utilizar.

1. En la POA, haga clic en **Recuperación**.

- Si sólo está activado el procedimiento de desafío/respuesta para la recuperación del inicio de sesión, se iniciará este procedimiento.
- Si tanto el procedimiento de desafío/respuesta como Local Self Help están activados para la recuperación de la conexión, aparecerá un cuadro de diálogo con ambos métodos de recuperación. Haga clic en el botón **Desafío/Respuesta** para iniciar el procedimiento de desafío/respuesta.

Se abre un cuadro de diálogo que indica el nombre del archivo requerido para el procedimiento de desafío/respuesta.

2. Póngase en contacto con el centro de ayuda. Indique el nombre del archivo.

3. Haga clic en **Siguiente**.

Aparecerán sus datos de usuario y un código de desafío generado aleatoriamente. Para facilitar la lectura, el código aparece dividido en grupos de cinco caracteres. Indique el código de desafío. Si necesita ayuda para ver cuál es el código de desafío, puede hacer clic en el botón **Ayuda a la ortografía**.

4. Haga clic en **Siguiente**.

Se abrirá el cuadro de diálogo **Desafío/Respuesta - Paso 3 de 3**.

El responsable del centro de ayuda le proporcionará el código de respuesta por teléfono o con un mensaje al móvil.

5. Introduzca el código de respuesta en los campos habilitados al efecto del cuadro de diálogo **Desafío/Respuesta - Paso 3 de 3**.

Si introduce incorrectamente el código de respuesta, el grupo de caracteres que contenga el error aparecerá resaltado en rojo.

6. Haga clic en **Aceptar**.

Se inicia la sesión en la POA.

10 Icono de la bandeja del sistema e información de ayuda

La funcionalidad que se describe a continuación está disponible a través del icono de la bandeja del sistema:

- **Mostrar**

- **Juego de claves**

Muestra todas las claves que tiene a su disposición.

Nota:

El cliente de Sophos SafeGuard utiliza una clave definida para el cifrado de volúmenes y el cifrado de archivos de las unidades. Esta clave *no* es visible en el cuadro de diálogo. Sólo se muestran aquellas claves que se hayan creado localmente en el ordenador. Si no ha creado ninguna clave, en el cuadro de diálogo no aparecerá ninguna. Fíjese en que en SafeGuard Portable con ESDP (Endpoint Security and Data Protection) no está disponible el cifrado basado en archivos.

■ **Certificado**

Muestra la información relativa a su certificado.

■ **Crear nueva clave**

Abre un cuadro de diálogo para crear una clave nueva que se usa para intercambiar datos mediante medios extraíbles.

Nota:

Esta función no está disponible con ESDP.

■ **Copia de seguridad de la clave**

Con esta función puede crear una copia de seguridad del archivo de clave. Este archivo de clave es necesario para la recuperación del inicio de sesión mediante el procedimiento de desafío/respuesta.

■ **Local Self Help**

Si se ha activado Local Self Help para su equipo mediante la directiva correspondiente, el comando Local Self Help aparecerá en el menú del icono. Utilice este comando para iniciar el asistente de Local Self Help. Local Self Help es un método de recuperación del inicio de sesión que no requiere de la ayuda del centro de ayuda. Para más información, [consulte el apartado Recuperación mediante Local Self Help](#) en la página 26.

■ **Estado:** Muestra información sobre el estado actual del equipo protegido con Sophos SafeGuard:

Campo	Información
Última directiva recibida	Muestra la fecha y la hora en que el equipo ha recibido una directiva nueva por última vez.
Última clave recibida	Muestra la fecha y la hora en que el equipo ha recibido una clave nueva por última vez.
Último certificado recibido	Muestra la fecha y la hora en que el equipo ha recibido un certificado nuevo por última vez.

Campo	Información
Estado de usuario de SGN	<p>Muestra el estado del usuario que está conectado al equipo (conexión con Windows):</p> <ul style="list-style-type: none"> <p>■ Pendiente</p> <p>Se asigna al usuario a la instalación de Sophos SafeGuard como un usuario de Sophos SafeGuard. Espere hasta que se hayan procesado los datos de usuario. Posteriormente, el estado de usuario se establecerá automáticamente como usuario SGN, es decir, usuario de Sophos SafeGuard.</p> <p>■ Usuario SGN</p> <p>Se ha asignado al usuario a la instalación de Sophos SafeGuard como un usuario de Sophos SafeGuard.</p> <p>■ Invitado de SGN</p> <p>El usuario que está conectado a Windows es un usuario invitado de Sophos SafeGuard. Al usuario se le permite que se conecte a Windows sin asignarlo a este equipo protegido con Sophos SafeGuard en calidad de usuario de Sophos SafeGuard.</p> <p>■ Invitado de SGN (cuenta de servicio)</p> <p>El usuario conectado a Windows es un usuario invitado de Sophos SafeGuard que se ha conectado mediante una cuenta de servicio para tareas de administración.</p> <p>■ Desconocido</p> <p>Indica que no se ha podido determinar el estado del usuario.</p>
Estado de Local Self Help (LSH) Activado Activo	<p>Indica si Local Self Help se ha habilitado mediante una directiva y si el usuario lo ha activado en el equipo.</p>

■ **Ayuda**

Abre la ayuda de Sophos SafeGuard.

■ **Acerca de Sophos SafeGuard**

Muestra información acerca de la versión de Sophos SafeGuard.

La información sobre herramientas del icono de la bandeja del sistema indica que el equipo es un cliente (independiente) de Sophos SafeGuard.

Nota:

Una información sobre herramientas en forma de globo indica la correcta finalización del proceso de sincronización inicial.

Reinicie el equipo una vez finalizada correctamente la sincronización inicial. Las funciones de Sophos SafeGuard solamente estarán completamente disponibles tras reiniciar el equipo.

11 Acceder a funciones desde el Explorador de Windows

Puede acceder a las funciones de cifrado desde el menú contextual del Explorador de Windows.

11.1 Extensiones del explorador para el cifrado de archivos

Nota:

Con ESDP (Endpoint Security and Data Protection) no está disponible el cifrado de archivos.

Puede acceder a las funciones de cifrado de archivos ([consulte el apartado Cifrado de archivos](#) en la página 42) desde el menú contextual 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 entradas de cifrado 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:** abre un cuadro de diálogo para crear claves locales definidas por el usuario.

11.2 Extensiones del explorador para el cifrado de 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.

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

Para más información, [consulte el apartado Cifrado de volúmenes](#) en la página 42.

12 Cifrado de datos

Sophos SafeGuard cifra los datos en un equipo ya sea basándose en volúmenes o en archivos.

Nota:

Nota: con ESDP (Endpoint Security and Data Protection) no está disponible el cifrado de archivos.

En las directivas de seguridad, el responsable de seguridad define los volúmenes (unidades) que deben cifrarse.

12.1 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 mediante **Guardar como**) de una unidad cifrada a otra ubicación del equipo sin cifrado, se descifrarán. Los archivos se almacenarán en la nueva ubicación en estado original.

12.2 Cifrado inicial

El cifrado inicial del sistema se realiza según la directiva que haya recibido el equipo. Si el cifrado inicial no comienza de forma automática, tendrá que iniciarlo de forma manual.

12.3 Cifrado de volúmenes

En un equipo protegido por Sophos SafeGuard, se utiliza una clave informática generada automáticamente para el cifrado de volúmenes.

Si una directiva establece el cifrado de este tipo, los datos se cifrarán automáticamente. No se pueden añadir más claves al volumen.

Se mostrará una barra de evolución del cifrado. También se muestran los volúmenes ya cifrados. Puede aparecer minimizado en la barra de tareas de Windows. Haga clic en el icono para mostrar la barra de evolución. Si desea minimizar el visor de cifrado, puede activar 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:

En Windows 7 Professional, Enterprise y Ultimate se crea una partición del sistema que no tiene ninguna letra asignada. Esta partición no se puede cifrar con Sophos SafeGuard.

Nota:

Si se aplica una nueva política que permita el descifrado: Tras completar el cifrado del disco, debe reiniciar el sistema antes de poder realizar el descifrado.

12.4 Cifrado de archivos

Nota:

Con ESDP (Endpoint Security and Data Protection) no está disponible el cifrado de 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.

Para el cifrado de archivos, se utilizarán las claves que usted crea localmente. El cifrado de un volumen puede comenzar de modo automático o bien tendrá que iniciar manualmente el proceso.

1. Si el cifrado no comienza de forma automática, seleccione **Cifrado de archivos > Iniciar cifrado** mediante las extensiones del explorador de Sophos SafeGuard.
2. Cuando dé comienzo el cifrado, se le pedirá que seleccione una clave local.
3. Si no se muestra ninguna clave, debe primero crear alguna (**Icono de la bandeja del sistema > Crear nueva clave**).
4. Reinicie la sesión.

El cifrado comenzará de nuevo y ahora las claves aparecerán en el cuadro de diálogo del cifrado inicial.

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

Se cifrarán todos los archivos del volumen correspondiente.

12.4.1 Definir la clave predeterminada

La clave predeterminada es la 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 o del medio extraíble.
2. Para poder definir la clave, 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.

12.4.2 Estado del cifrado

En los volúmenes cifrados por archivo, cada archivo se marca con el símbolo de una llave. El color de la llave indica el estado del cifrado.

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

El estado de cifrado de un archivo también se puede ver a través de su menú contextual. Seleccione **Cifrado de archivos > Mostrar estado de cifrado** para ver el estado de cifrado.

Seleccione **Cifrado de archivos > Estado de cifrado** en el menú contextual del propio volumen, para ver estado de cifrado de todos los archivos.

12.5 Restricciones de acceso a volúmenes

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

Volúmenes con un cifrado fallido

Si alguna directiva específica que se debe cifrar un volumen o un tipo de volumen y se producen errores en el proceso de cifrado, se impedirá el acceso al volumen.

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

Objetos del sistema de archivos no identificados

Los objetos del sistema de archivos no identificados son volúmenes que Sophos SafeGuard no puede identificar con claridad si están cifrados o no.

Si alguna directiva específica que se debe cifrar un volumen de este tipo, se impedirá el acceso al 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.

13 SafeGuard Data Exchange

Nota:

SafeGuard Data Exchange y SafeGuard Portable no son compatibles con ESDP (Endpoint Security and Data Protection).

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 acceder al 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 cada equipo se define mediante una directiva creada por el departamento informático.

La directiva define cómo se tratan los datos de los medios extraíbles. Por ejemplo, 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 cifrarán en principio. Además, se cifrarán todos los archivos nuevos guardados en medios extraíbles. Si los archivos existentes no se van a cifrar, se 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 cifrarán los archivos nuevos. Por tanto, puede leer y editar los archivos no cifrados existentes, pero se cifrarán en cuanto les cambie el nombre. La directiva también puede impedir el acceso a archivos no cifrados, que permanecerán sin cifrar.

Los archivos cifrados en unidades extraíbles se pueden compartir de dos formas:

- Si **Sophos SafeGuard está instalado 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, tendrá que proporcionar el destinatario de los datos la frase de contraseña para la clave.
- Si **Sophos SafeGuard no está instalado en el equipo del destinatario**: Sophos SafeGuard 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 acceso pertinente, el destinatario puede descifrar los archivos cifrados y volver a cifrarlos sin necesidad de instalar SafeGuard Data Exchange en su equipo.

13.1 Configuración para tratar medios extraíbles

Si SafeGuard Data Exchange está instalado en su equipo, el responsable de seguridad define cómo se tratan los medios extraíbles. Se pueden definir los siguientes aspectos de SafeGuard Data Exchange:

- **Cifrado inicial de todos los archivos:** el cifrado de todos los datos 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 permite cancelar el cifrado inicial:** cuando comience el cifrado inicial, se muestra un cuadro de diálogo que le permite cancelarlo.
- **Acceso denegado a datos sin cifrar:** 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 permite descifrar archivos:** 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 permite definir una contraseña de acceso al medio:** se le pedirá que introduzca una contraseña de acceso al medio la primera vez que conecte un medio extraíble.
- **Carpeta sin cifrar en medios extraíbles:** el responsable de seguridad puede definir una carpeta sin cifrar que se creará en todos los medios extraíbles. SafeGuard Data Exchange no cifrará los archivos incluidos en esta carpeta.
- **Se permite decidir sobre el cifrado:** al conectar un medio extraíble, se le preguntará si desea cifrar los archivos en dicho medio.

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

En SafeGuard Data Exchange es posible definir una única frase 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 frase de acceso. La frase de acceso a medios está vinculada a los equipos.

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

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

También puede restringir el acceso a todos los archivos, proporcionándole al usuario externo la contraseña de acceso para una clave en concreto. En este caso, el usuario externo sólo tendrá acceso a los archivos cifrados con esta clave y no podrá visualizar los demás archivos.

Medios compatibles

SafeGuard Data Exchange admite los siguientes medios extraíbles:

- Memoria USB
- Discos duros externos con conexión USB o FireWire
- Unidades CD RW (UDF)
- Unidades DVD RW (UDF)
- FireWire
- Tarjetas de memoria en lectores USB (incl. ZIP, JAZ)

13.3 Cifrado de medios extraíbles

13.3.1 Cifrado inicial

El cifrado de datos en los medios extraíbles o bien comienza automáticamente tan pronto como conecte los medios al sistema, o deberá iniciar el proceso manualmente. Si se permite al usuario decidir sobre el cifrado, se le preguntará si desea cifrar los medios extraíbles que se conecten.

Par iniciar el cifrado de forma manual:

1. Seleccione **Cifrado de archivos > Iniciar cifrado** en el menú contextual del medio en el 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.

Si el cuadro de diálogo de selección de claves no contiene ninguna, ciérrelo y cree primero una o varias claves (**Icono de la bandeja del sistema > Crear nueva clave**).

3. Haga clic en **Aceptar**.

Se cifrarán todos los datos que contengan los medios extraíbles.

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.

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.

Cifrado inicial en caso de utilizar una frase de acceso al medio

Si se ha especificado el uso de una frase de acceso al medio en la administración central, se le pedirá que introduzca la frase de contraseña de medios antes del proceso de 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.

13.3.2 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 sin cifrar. Si en la nueva ubicación de los archivos está vigente una directiva de cifrado distinta, los datos se cifrarán en consecuencia.

Frase de acceso a unidades

Si la directiva hace uso de una frase de acceso, tendrá que introducirla cuando conecte por primera vez un dispositivo extraíble tras haber instalado SafeGuard Data Exchange.

Indique la frase de acceso si se pide. Puede utilizar esta misma frase de acceso para acceder a todos los archivos cifrados de sus medios extraíbles, independientemente de la clave utilizada para cifrarlos.

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

Cambiar/restablecer la frase de acceso

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

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

Reinicie la sesión inmediatamente. A continuación, seleccione **Cambiar la frase de acceso al soporte** en el menú del icono de la bandeja del sistema. Se le informará de que no hay ninguna frase de acceso en su equipo y se le pedirá que introduzca una nueva.

Sincronización de la frase de acceso

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

Nota: una vez que haya cambiado la frase de acceso, conecte las unidades externas. De esta manera, se garantiza que la nueva frase de acceso se utilizará inmediatamente en todos los dispositivos (sincronización).

Definir la 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 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.

13.4 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 Sophos SafeGuard 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 Sophos SafeGuard 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 sin Sophos SafeGuard

Los usuarios que no tengan Sophos SafeGuard instalado en sus máquinas 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 de almacenamiento 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 de almacenamiento extraíble. Dado que SafeGuard Portable es una aplicación autosuficiente, no hay que instalar ningún software adicional para acceder a los datos cifrados.

Nota: el responsable de seguridad determinará mediante una directiva si SafeGuard Portable se copia al medio extraíble.

13.4.1 Importar claves desde un archivo

Si recibe alguna unidad extraíble con datos cifrados con una clave local definida por el usuario, puede importar la clave requerida para el descifrado a su juego de claves privado.

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

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

Introduzca la frase de acceso. La clave se importará y tendrá acceso al archivo.

13.4.2 Crear claves locales

Para crear una clave local definida por el usuario:

1. Haga clic con el botón derecho en el icono de Sophos SafeGuard en la bandeja del sistema.
2. Seleccione **Crear nueva clave**.
3. En el cuadro de diálogo **Crear clave**, introduzca el **Nombre** y la **Frase de acceso** para la clave.

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

4. Confirme la frase de acceso.

Si especifica una frase de acceso que no sea segura, aparecerá un mensaje de advertencia. Para aumentar el nivel de seguridad, se aconseja el uso de frases complejas. A pesar del mensaje de advertencia, puede utilizar la frase que desee. La frase de acceso tiene que corresponderse con las directivas de la empresa. De lo contrario, se mostrará un mensaje de advertencia.

5. La opción **Utilizar como nueva clave predeterminada para la unidad** le permite establecer de manera inmediata la nueva clave como la predeterminada.

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**.

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.

Las claves locales no se guardan en la copia de seguridad y no se pueden utilizar para la recuperación.

Para que el destinatario pueda descifrar todos los datos en 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 dispositivo en el Explorador de Windows. Seleccione la clave local necesaria y cifre los datos. Esto no será necesario si utiliza una frase de acceso al medio.

13.5 Grabación de archivos en un CD mediante el Asistente para grabación de CD de Windows

Nota:

En Windows XP, sólo se pueden copiar archivos a un CD con el asistente de grabación de Windows. Windows XP no permite copiar archivos a un DVD mediante dicho asistente.

SafeGuard Data Exchange permite grabar archivos cifrados en un CD a través del asistente de grabación de Windows.

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 de grabación. 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 **Estadísticas** se muestra la siguiente información:

- cuántos archivos se han seleccionado para la grabación en CD
- cuántos están cifrados
- cuántos están sin cifrar

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.

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 el resto 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.

Grabación de archivos en CD sin cifrar

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

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.

13.5.1 Grabación en CD/DVD con Windows Vista y Windows 7

Windows Vista y Windows 7 disponen de un asistente para grabar CD/DVD.

La extensión de grabación de SafeGuard para el asistente de grabación de Windows sólo permite para la grabación de CD/DVD en formato **Mastered**. 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.

13.6 SafeGuard Portable

Nota:

SafeGuard Portable no está disponible con ESDP (Endpoint Security and Data Protection).

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 con 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 local que se haya utilizado para cifrarlos. Con la contraseña de una clave local, que le proporcionará acceso a los archivos que se hayan cifrado con esta clave determinada. El destinatario podrá 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 persona. Permanece en el medio extraíble.

Nota: como usuario de Sophos SafeGuard, no necesitará SafeGuard Portable. La descripción que se facilita a continuación asume que los usuarios no tienen instalado Sophos SafeGuard en sus equipos y que, por lo tanto, deben utilizar SafeGuard Portable para editar los datos cifrados.

13.6.1 Editar 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 en 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.

- 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:

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

13.6.1.1 Establecer la clave de cifrado

Para cifrar archivos en medios extraíbles y crear una clave de cifrado:

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

La frase de acceso tiene que corresponderse con las directivas de 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.

13.6.1.2 Cifrar archivos 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 le pedirá la clave a utilizar. Introduzca el nombre de la clave y la frase 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 o desde el menú **Archivo**.

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

Nota: la última clave que SafeGuard Portable haya utilizado se usará para todos los procesos de cifrado posteriores, hasta que seleccione otra diferente.

13.6.1.3 Descifrar un archivo en un medio extraíble

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

Deberá introducir la frase de acceso al medio o la frase de acceso de una clave local.

2. Introduzca la frase de acceso (proporcionada por el remitente) y haga clic en **Aceptar**.

El archivo se descifrará.

La frase de acceso al medio le da acceso a todos los archivos cifrados en dicha unidad, sin que importe la clave local de cifrado. Si sólo dispone de la frase de acceso de una clave local, sólo tendrá acceso a los archivos cifrados con dicha clave.

El descifrado de archivos cifrados con claves generadas en SafeGuard Portable se realiza de forma automática.

Sólo es necesario introducir la frase de acceso la primera vez.

SafeGuard Portable guarda la frase de acceso mientras la aplicación se esté ejecutando. La última clave utilizada por SafeGuard Portable se utiliza para el cifrado.

Tras descifrar los archivos, podrá utilizarlos como cualquier otro. Los archivos que se hayan descifrado se cifrarán de nuevo al cerrar SafeGuard Portable.

13.6.1.4 Cifrar archivos nuevos con SafeGuard Portable

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

1. Arrastre los archivos que desee copiar al explorador de SafeGuard Portable.

Se le preguntará si desea cifrar el archivo pertinente.

2. Confirme que desea cifrar el archivo. El archivo se cifrará con la última clave utilizada y se copiará al medio extraíble.

13.6.1.5 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 o desde el menú **Archivo**.

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

13.6.2 Otras operaciones con SafeGuard Portable

Están disponibles las siguientes funciones:

- ❖ **Abrir:** este comando sólo está disponible en el menú **Archivo** de SafeGuard Portable.
Al abrir un archivo cifrado mediante este comando, se le pedirá que introduzca su frase de acceso. Escríbala y haga clic en **Aceptar**. El archivo se descifrá y se abrirá.
- ❖ **Suprimir:** elimina el archivo seleccionado.
- ❖ **Copiar a:** este comando sólo está disponible en el menú contextual desde el explorador de SafeGuard Portable.
Con este comando, puede copiar los archivos de los medios extraíbles a otra unidad del equipo.
- ❖ **Salir:** este comando sólo está disponible en el menú **Archivo** de SafeGuard Portable.
Salir cierra SafeGuard Portable.

14 Sophos SafeGuard y unidades autocifradas compatibles con Opal

Las unidades con autocifrado realizan el cifrado automático de los datos que se copian a las mismas. La organización Trusted Computing Group (TCG) ha hecho público es estándar Opal que se utiliza en este tipo de unidades. Diferentes fabricantes utilizan Opal. Sophos SafeGuard es compatible con Opal.

14.1 Cifrado de unidades compatibles Opal

Las unidades compatibles Opal disponen de cifrado automático. Los datos que se copian a estas unidades se cifran de forma automática.

Estas unidades utilizan una clave AES 256. Esta contraseña se puede administrar en Sophos SafeGuard mediante una directiva de cifrado. El responsable de seguridad especifica la directiva de cifrado en SafeGuard Policy Editor y la distribuye a los equipos.

14.2 Icono de la bandeja del sistema y extensiones del Explorador de Windows con unidades compatibles Opal

Cuando Sophos SafeGuard se instala en un equipo, el icono del producto se muestra en la bandeja del sistema. Podrá definir de forma centralizada todas las funciones ofrecidas por Sophos SafeGuard para las estaciones. Tenga en cuenta que las funciones disponibles dependen de la configuración definida por el responsable de seguridad.

Si se permite descifrar unidades compatibles Opal, el menú contextual del Explorador de Windows incluirá el comando **Descifrar** de Sophos SafeGuard.

15 Sophos SafeGuard y Lenovo Rescue and Recovery

Para obtener información sobre las versiones de Lenovo Rescue and Recovery (RnR) compatibles con Sophos SafeGuard, consulte el artículo de la base de conocimiento <http://esp.sophos.com/support/knowledgebase/article/108383.html>

Puede restaurar copias de seguridad completas del sistema operativo en una partición cifrada sin tener que descifrar primero el disco duro. Esto supone un ahorro de tiempo en las recuperaciones ante desastres. Sophos SafeGuard ha recibido la certificación oficial de Lenovo.

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 Introducción

Sophos SafeGuard 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 Sophos SafeGuard. Las copias de seguridad de los sistemas cifrados de Sophos SafeGuard 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.

Sophos SafeGuard 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 Sophos SafeGuard, Rescue and Recovery se basa en la recuperación de WinPE. WinPE se puede iniciar desde:

- una partición virtual o de servicio.

- un dispositivo extraíble como puede ser un CD/DVD o un disco duro USB.

15.2 Requisitos

- La BIOS más reciente para el ordenador
- Para más información sobre la compatibilidad de Rescue and Recovery con Sophos SafeGuard, consulte: <http://esp.sophos.com/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery se puede utilizar para recuperar volúmenes cifrados con Sophos SafeGuard. Debe estar instalado el paquete de instalación **SGNClient.msi**.
- Para Rescue and Recovery, los volúmenes deben estar cifrados con la clave del equipo. Rescue and Recovery no es compatible con volúmenes cifrados con cualquier otra clave.

15.3 Instalación

Cuando se instala Rescue and Recovery en un disco duro que no tiene una partición de servicio:

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

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

15.3.1 Instalar Rescue and Recovery y Sophos SafeGuard

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 Sophos SafeGuard Device Encryption (**SGNClient.msi**).

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

3. Compruebe que está activada la POA (power-on authentication), de forma que no sea posible restaurar copias de seguridad no autorizadas.

La POA se activa durante la instalación de Sophos SafeGuard.

15.3.2 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 Sophos SafeGuard Device Encryption (**SGNClient.msi**).

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

15.4 Actualización

La actualización implica que Sophos SafeGuard y Rescue and Recovery ya están instalados y desea actualizar uno de ellos o ambos a una versión más reciente.

Actualización de Sophos SafeGuard

Si actualiza Sophos SafeGuard, se actualiza todo el sistema, por lo que no tendrá realizar ninguna configuración adicional.

15.5 Desinstalación

Al desinstalar los productos:

- Se recomienda desinstalar primero Sophos SafeGuard y, a continuación, Rescue and Recovery. Si se desinstala Sophos SafeGuard mientras Rescue and Recovery sigue instalado, se eliminan del entorno WinPE de RnR todas las modificaciones específicas de Sophos SafeGuard, como las entradas de registro, los archivos y las unidades agregadas.
- No desinstale Sophos SafeGuard inmediatamente después de haber restaurado el sistema. Tras una restauración del sistema, reinicie el equipo una vez y, a continuación, desinstale Sophos SafeGuard.
- Si se elimina Rescue and Recovery mientras Sophos SafeGuard 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

Sophos SafeGuard 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 Sophos SafeGuard con la clave del equipo. 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: Sophos SafeGuard no le permite arrancar en el entorno de Rescue and Recovery cuando arranca directamente desde la BIOS.

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

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

15.7 Crear una copia de seguridad

Las copias de seguridad se crean mediante Rescue and Recovery en Windows. En los equipos en los que Rescue and Recovery ya esté instalado, en los que instalará Sophos SafeGuard 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.

Sophos SafeGuard sólo admite guardar copias de seguridad en:

- el disco duro local
- un segundo disco duro
- un disco duro USB
- la 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 Sophos SafeGuard. Sólo tiene que iniciar Windows, a continuación, Rescue and Recovery y restaurar los archivos que desee. No es necesario reiniciar el equipo cuando haya finalizado la restauración.

15.9 Restaurar el sistema de Sophos SafeGuard

Para restaurar una copia de seguridad del sistema que incluya Sophos SafeGuard, 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 POA (power-on authentication).
 - b) Introduzca las credenciales de Sophos SafeGuard.
2. Si no utiliza un equipo Lenovo:
 - a) Inicie la sesión en la POA con sus credenciales de Sophos SafeGuard.
 - b) Mientras el equipo se inicia, 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 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 de fábrica del 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 Sophos SafeGuard. Si desea obtener más información, consulte la documentación de Lenovo.

15.11 POA deshabilitada y Lenovo Rescue and Recovery

Si la POA (power-on authentication) 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://esp.sophos.com/support/>
- Descargar la documentación correspondiente desde <http://esp.sophos.com/support/docs/>
- Enviar un email a 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 Aviso legal

Copyright © 1996 - 2011 Sophos Group. Todos los derechos reservados. SafeGuard es una marca registrada de Sophos Group.

Sophos es una marca registrada de Sophos Limited, Sophos Group y Utimaco Safeware AG, según corresponda. Otros productos y empresas mencionados son marcas registradas de sus propietarios.

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.

El documento Disclaimer and Copyright for 3rd Party Software.rtf, en la carpeta de instalación del producto, incluye información sobre copyright de terceros.