SOPHOS
Security made simple.

SafeGuard Enterprise
Ayuda de usuario

Versión: 7
Edición: diciembre de 2014

Contenido

1 Acerca de SafeGuard Enterprise 7.0 5
2 SafeGuard Enterprise en equipos Windows 7
3 Prácticas recomendadas de seguridad 9
4 POA de SafeGuard 11
4.1 Primer inicio de sesión tras instalar SafeGuard Enterprise 11
4.2 Inicio de sesión en la POA de SafeGuard 13
4.3 Registro de usuarios de SafeGuard Enterprise adicionales 14
4.4 Contraseña temporal en la POA de SafeGuard 14
4.5 Inicio de sesión en la POA de SafeGuard mediante tarjetas inteligentes o tokens 15
4.6 Autoinicio de sesión en la POA de SafeGuard con token 18
4.7 Teclado virtual 19
4.8 Distribución del teclado 19
4.9 Teclas de acceso rápido y de función compatibles en la POA de SafeGuard 20
4.10 Sincronización de la contraseña 22
5 Inicio de sesión en Windows 23
5.1 Iniciar la sesión con SafeGuard Enterprise 23
5.2 Iniciar la sesión con la autenticación de Windows 23
6 Inicio de sesión con el lector de huellas digitales de Lenovo 24
6.1 Requisitos 24
6.2 Registrar huellas digitales 25
6.3 Iniciar sesión en la POA de SafeGuard mediante huella digital 26
6.4 Cambio de contraseña 29
6.5 Recuperación de inicio de sesión mediante huella digital 30
7 Cifrado de discos 31
7.1 Cifrado de discos SafeGuard 31
7.2 Cifrado de unidad BitLocker 34
8 SafeGuard Data Exchange 39
8.1 Configuración para tratar medios extraíbles 40
8.2 Una única frase de acceso para todos los dispositivos de medios extraíbles conectados al equipo 40
8.3 Cifrado de medios extraíbles 41
8.4 Intercambio de datos con SafeGuard Data Exchange 44
8.5 Grabación de archivos en un CD mediante el Asistente para grabación de CD de Windows 45

8.6 SafeGuard Portable....47
9 SafeGuard File Encryption....51
9.1 Cifrado según la directiva....51
9.2 Asistente de cifrado de archivos de SafeGuard....51
9.3 Cifrado permanente....52
10 SafeGuard Cloud Storage....53
10.1 Detección automática de Cloud Storage....53
10.2 Cifrado inicial de Cloud Storage....53
10.3 Establecer las claves predeterminadas....53
10.4 SafeGuard Portable para Cloud Storage....54
11 SafeGuard Enterprise y unidades autocifradas compatibles con Opal....55
11.1 Cifrado de unidades compatibles Opal....55
11.2 Icono de la bandeja del sistema y extensiones del Explorador de Windows con unidades compatibles Opal....55
12 Icono de la bandeja del sistema y la información mostrada....56
12.1 Crear claves locales....58
12.2 Iconos superpuestos....59
13 Acceder a funciones desde el Explorador de Windows....60
13.1 Extensiones del explorador para el cifrado de archivos....60
13.2 Extensiones del explorador para el cifrado de volúmenes....62
14 Opciones de recuperación....63
15 Recuperación mediante Local Self Help....64
15.1 Activar Local Self Help....64
15.2 Activar de Local Self Help - recordatorio....66
15.3 Editar preguntas....67
15.4 Cambios en los parámetros de preguntas....68
15.5 Cambio de condiciones o parámetros en Local Self Help durante la edición....69
15.6 Iniciar la sesión en la POA de SafeGuard mediante Local Self Help....70
15.7 Intentos fallidos de inicio de sesión....71
15.8 Reactivar las preguntas y respuestas tras el cambio de contraseña en diferentes equipos....72
16 Recuperación con desafío/respuesta o clave de recuperación....73
16.1 Desafío/respuesta para usuarios de POA de SafeGuard....73
16.2 Desafío/respuesta para usuarios de BitLocker....79
16.3 Clave de recuperación de BitLocker....80
17 SafeGuard Enterprise y Lenovo Rescue and Recovery....82
17.1 Introducción....82
17.2 Requisitos....82
17.3 Instalación....83

17.4 Actualización....84
17.5 Desinstalación....84
17.6 Opciones de recuperación y entorno de arranque....84
17.7 Crear una copia de seguridad....85
17.8 Restaurar copias de seguridad de archivos....85
17.9 Restaurar el sistema de SafeGuard Enterprise....85
17.10 Particiones de servicio y de recuperación de fábrica....86
17.11 POA de SafeGuard deshabilitada y Lenovo Rescue and Recovery....86
18 Soporte técnico....87
19 Aviso legal....88

1 Acerca de SafeGuard Enterprise 7.0

Esta versión de SafeGuard Enterprise es compatible con Windows 7 y Windows 8 en equipos con BIOS o UEFI.

- En el caso de plataformas con BIOS, los administradores puede escoger entre el cifrado de discos de SafeGuard Enterprise y el cifrado de BitLocker administrado con SafeGuard. La versión BIOS incluye el mecanismo de recuperación nativo de BitLocker.

  Nota: cuando en este manual se menciona la POA (power-on authentication) de SafeGuard o cifrado de discos de SafeGuard se refiere solo a equipos con Windows 7 BIOS.

- En el caso de plataformas UEFI, BitLocker administrado con SafeGuard Enterprise es el componente para el cifrado de discos. Para estos equipos, SafeGuard Enterprise ofrece una capacidades de desafío/respuesta ampliadas. Para más información sobre las versiones UEFI compatibles y las restricciones en la compatibilidad del mecanismo de desafío/respuesta para BitLocker de SafeGuard consulte las notas de la versión en http://downloads.sophos.com/readmes/readsgn_7_esp.html.

Nota: cuando una descripción de este manual se refiere solamente a UEFI se mencionará explícitamente.

La tabla muestra los componentes que están disponibles.

	Cifrado de discos SafeGuard con POA (power-on authentication) de SafeGuard	BitLocker con autenticación prearranque (PBA) administrado con SafeGuard	Recuperación de desafío/respuesta de SafeGuard para la autenticación prearranque (PBA) de BitLocker
Windows 7 BIOS	**SÍ**	**SÍ**	
Windows 7 UEFI		**SÍ**	**SÍ**
Windows 8 BIOS		**SÍ**	
Windows 8 UEFI		**SÍ**	**SÍ**
Windows 8.1 BIOS		**SÍ**	
Windows 8.1 UEFI		**SÍ**	**SÍ**

Nota: Recuperación de desafío/respuesta de SafeGuard para la autenticación prearranque (PBA) de BitLocker solo está disponible para sistemas de 64 bits.

Cifrado de discos de SafeGuard con POA de SafeGuard es el módulo de Sophos para cifrar volúmenes en equipos. Incluye un método de autenticación prearranque de Sophos denominado SafeGuard Power-on Authentication (POA) que es compatible con inicios de sesión con tarjetas inteligentes y huellas digitales entre otros, y un mecanismo de desafío/respuesta para la recuperación.

BitLocker con autenticación prearranque (PBA) administrado con SafeGuard es el componente que habilita y administra el motor de cifrado de BitLocker y la autenticación prearranque de BitLocker.

Está disponible para plataformas BIOS y UEFI:

- La versión UEFI ofrece adicionalmente un mecanismo de desafío/respuesta de SafeGuard para la recuperación de BitLocker en caso de que los usuarios olviden sus PIN. La versión UEFI se puede usar cuando se cumplen determinados requisitos de plataforma. Por ejemplo, la versión UEFI debe ser 2.3.1. Consulte las notas de la versión para más información.
- La versión BIOS no ofrece la opción de recuperación mediante el mecanismo de desafío/respuesta de SafeGuard y también sirve como opción alternativa cuando no se cumplen los requisitos para la versión UEFI. El instalador de Sophos comprueba si se cumplen los requisitos, y en caso contrario, automáticamente instala la versión de BitLocker sin desafío/respuesta.

Equipos Mac

Para equipos Mac están disponibles los siguientes productos. También son administrados por SafeGuard Enterprise o por lo menos proporcionan informes al centro de administración.

	Sophos SafeGuard File Encryption 7.0	Sophos SafeGuard Native Device Encryption (administración de FileVault 2) 7.0
OS X 10.8	**SÍ**	**SÍ**
OS X 10.9	**SÍ**	**SÍ**
OS X 10.10	**SÍ**	**SÍ**

La descripción en este manual se refiere solo a plataformas Windows. Para las versiones Mac, consulte los manuales de producto correspondientes.

Sophos Mobile Encryption

Con **Sophos Mobile Encryption** puede leer archivos cifrados por los módulos de SafeGuard Enterprise **SafeGuard Cloud Storage** o **SafeGuard Data Exchange** . Le permiten cifrar archivos mediante una clave local. Estas claves locales se derivan de una frase de acceso que introduce el usuario. Únicamente se puede descifrar un archivo cuando se conoce la frase de acceso que se utilizó para cifrar el archivo. Para más detalles sobre Encryption Sophos Mobile visite www.sophos.com/es-es/.

2 SafeGuard Enterprise en equipos Windows

SafeGuard Enterprise es una suite de productos de seguridad para equipos y dispositivos móviles con diferentes plataformas que se gestiona mediante directivas centralizadas. SafeGuard Enterprise es fácil de usar. La administración del sistema se realiza desde SafeGuard Management Center.

La protección de SafeGuard Enterprise se centra en el cifrado de datos y el control de acceso al sistema.

Módulos de SafeGuard Enterprise

- **Cifrado de discos SafeGuard**
  - **POA de SafeGuard**

    El inicio de sesión se realiza inmediatamente después de encender el ordenador. Tras identificarse correctamente en la POA de SafeGuard, se iniciará la sesión de forma automática en el sistema operativo. También puede desactivar la POA de SafeGuard. 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.

- **BitLocker con autenticación prearranque administrado con SafeGuard Enterprise**

  SafeGuard Enterprise administra el motor de cifrado de Microsoft BitLocker. En plataformas UEFI, la autenticación prearranque de BitLocker incluye el mecanismo de desafío/respuesta de SafeGuard mientras que la versión BIOS permite recuperar la clave de recuperación del centro de administración.

- **SafeGuard Data Exchange**
  - 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 USB, se cifran de forma transparente.

- **SafeGuard File Encryption**
  - SafeGuard File Encryption ofrece cifrado de archivos en unidades compartidas de red.
  - Los archivos en ubicaciones incluidas en las directivas de File Encryption se cifran automáticamente de forma transparente para el usuario.

- **SafeGuard Cloud Storage**

SafeGuard Cloud Storage ofrece cifrado de archivos en la nube. Los archivos se cifran de forma transparente en el equipo del usuario y permanecen cifrados al almacenarlos en la nube.

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.

3 Prácticas recomendadas de seguridad

A continuación se describen algunos sencillos pasos que le ayudarán a proteger los datos en sus equipos.

Cuando haya terminado de trabajar, apague el ordenador o póngalo en modo hibernación.

En equipos protegidos con SafeGuard Enterprise, las claves de cifrado pueden conseguirse en ciertos modo de suspensión cuando el sistema operativo no se apaga completamente y quedan ciertos procesos activos en segundo plano. El nivel de protección mejora si apaga el equipo o se pone en hibernación.

Cuando no esté utilizando el ordenador:

- Evite el modo de suspensión. Evite el modo híbrido de suspensión El modo híbrido combina hibernación y suspensión.
- No debe simplemente bloquear el escritorio y apagar el monitor (o cerrar la pantalla del portátil), si no se apaga o hiberna a continuación el equipo. Requerir una contraseña al reanudar la sesión no es protección suficiente.
- En su lugar, apague el ordenador o póngalo en modo de hibernación.

  Nota: es importante que el archivo de hibernación se encuentre en una unidad cifrada. Normalmente se utiliza la unidad C:\.

Siga estos pasos especialmente si utiliza el portátil en lugares públicos.

Cuando el equipo se apaga o se pone en hibernación, la POA de SafeGuard requiere autenticación al volver a utilizar el equipo, aumentando la seguridad.

Asegúrese de que todos los volúmenes tienen asignada una letra

Sólo se cifran los volúmenes con una letra asignada. De esta forma, volúmenes sin letra asignada pueden aprovecharse para obtener datos sin cifrar.

Para evitarlo:

- Si encuentra un volumen sin letra asignada, póngase en contacto con el responsable informático.
- No modifique la asignación de letra de unidades.

Utilice contraseñas seguras

Una contraseña segura es de vital importancia para proteger sus datos. Utilice contraseñas seguras, especialmente para iniciar la sesión en su equipo.

Siga estas reglas para crear una contraseña segura:

- Es lo suficientemente larga para ser segura: se recomienda un mínimo de 10 caracteres.
- Combine letras (en mayúsculas y minúsculas), número y caracteres especiales o símbolos.
- No utilice nombres o palabras comunes.

- Debe ser difícil de adivinar pero fácil de recordar.

Cambie sus contraseñas de forma regular. No las comparta con nadie y no las anote.

4 POA de SafeGuard

Con la POA (power-on authentication) de SafeGuard, 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 (suspender en disco).

Aspecto visual y operativo de POA de SafeGuard

El aspecto visual y operativo de la POA de SafeGuard se puede personalizar de acuerdo con las necesidades de la empresa en cuestión. El responsable de seguridad realiza esta configuración desde SafeGuard Management Center.

Se pueden realizar los siguientes ajustes:

- **Imagen de inicio de sesión**

  La imagen predeterminada que aparece en la POA de SafeGuard es un diseño de SafeGuard. Esta pantalla se puede personalizar mediante directivas, lo que le permite que aparezca el logotipo de su empresa, por ejemplo.

- **Texto de los cuadros de diálogo**

  Todo el texto que se muestra en la POA de SafeGuard aparece en el idioma predeterminado que esté configurado por defecto en la Configuración regional y de idioma de Windows del equipo del usuario. El idioma usado en la POA se puede cambiar cambiando el idioma por defecto. El responsable de seguridad también puede especificar el idioma del texto de los cuadros de diálogo.

4.1 Primer inicio de sesión tras instalar SafeGuard Enterprise

Si SafeGuard Enterprise se ha instalado con la POA de SafeGuard, el procedimiento de inicio la primera vez que se arranque el sistema tras la instalación de SafeGuard Enterprise presenta diferencias. Cuando SafeGuard Enterprise se incorpora al procedimiento de inicio, aparecerán varios mensajes de inicio nuevos (por ejemplo, la pantalla de inicio de sesión automático). Después, se iniciará el sistema operativo Windows.

Nota:

SafeGuard Enterprise emplea certificados para el inicio de sesión. Sin embargo, las claves y los certificados específicos del usuario sólo se crean después de iniciar la sesión en 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 SafeGuard Enterprise. Este proceso de registro es necesario para asegurarse de que la POA de SafeGuard reconozca sus credenciales la próxima vez que el sistema se inicie.

El sistema la informará de que el registro se ha realizado correctamente y que se han recibido todo los datos necesarios.

Cuando reinicie el equipo, se activará la POA de SafeGuard. A partir de ese momento, debe especificar sus credenciales de Windows en la POA de SafeGuard, 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 de SafeGuard 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.

Procedimiento del primer inicio de sesión

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

4.1.1 Autoinicio de sesión de SafeGuard

1. Se arranca el ordenador y aparece el cuadro Autoinicio de sesión de SafeGuard.
   - Se realiza el autoinicio.
   - Si dispone de conexión al servidor de SafeGuard Enterprise, el equipo se registrará de forma automática.
   - La clave del equipo se envía al servidor de SafeGuard Enterprise y se almacena en la base de datos de SafeGuard Enterprise.
   - El equipo recibirá las directivas correspondientes.

4.1.2 Inicio de sesión en Windows

1. Aparecerá el cuadro de diálogo de inicio de sesión de Windows.
2. SafeGuard Enterprise ofrece el método de autenticación de SafeGuard Enterprise y de Windows. Windows 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, haga clic en dicho icono. Si éste no es el caso, seleccione el icono de SafeGuard Enterprise **Otro usuario**.
3. Introduzca sus credenciales de usuario de Windows de la forma habitual.
   - Se enviarán al servidor el identificador de usuario y las credenciales cifradas.
   - Las directivas, los certificados y las claves del usuario se crearán y se enviarán al equipo de dicho usuario.

   Los datos de usuario solo estarán disponibles en la POA de SafeGuard después de que todos los datos se hayan sincronizado entre el servidor de SafeGuard Enterprise y el equipo.

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

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

4.1.3 Inicio de sesión en la POA de SafeGuard tras reiniciar

1. Tras reiniciar el ordenador, aparece el cuadro de inicio de sesión de la POA de SafeGuard.

   Los certificados y las claves están disponibles y puede iniciar la sesión en la POA de SafeGuard con sus credenciales de Windows.

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

   Se comprobarán las credenciales. Cuando el sistema haya comprobado sus credenciales de usuario, iniciará automáticamente sesión en Windows.

   Nota: el inicio de sesión automático en Windows se puede desactivar desde la directiva. En tal caso, se mostrará el cuadro de inicio de sesión de Windows y tendrá que introducir sus credenciales.

4.2 Inicio de sesión en la POA de SafeGuard

Tras la correcta activación de la POA de SafeGuard (sincronización inicial y reinicio), puede iniciar la sesión mediante las credenciales de Windows desde el cuadro de la POA de SafeGuard. 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 diálogo 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 de SafeGuard en el mismo equipo, consulte el Registro de usuarios de SafeGuard Enterprise adicionales en la página 14. 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 de SafeGuard, 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

El equipo se bloqueará tras el número establecido de intentos fallidos de inicio de sesión. Para desbloquearlo, inicie un procedimiento de desafío/respuesta, consulte Recuperación con desafío/respuesta o clave de recuperación en la página 73.

4.2.1 Recuperación de inicio de sesión

Para la recuperación del inicio de sesión (por ejemplo, si ha olvidado la contraseña), SafeGuard Enterprise ofrece varias opciones adaptadas a distintos escenarios: El método de recuperación disponible depende de la directiva de seguridad aplicada. Para más información, consulte Opciones de recuperación en la página 63.

4.3 Registro de usuarios de SafeGuard Enterprise adicionales

Para permitir que otros usuarios de Windows puedan iniciar sesión en su equipo:

1. Encienda el equipo.

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

2. Para que el segundo usuario pueda iniciar la sesión en la POA de SafeGuard el propietario del equipo debe autorizarlo.

   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 de SafeGuard, haga clic en **Opciones** y desactive la opción **Inicio de sesión automático en Windows**. Inicie sesión con sus credenciales como el propietario del equipo.

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

4. El segundo usuario introduce sus credenciales de Windows.
5. Si el certificado y la clave del segundo usuario están disponibles (como resulta evidente del globo de información de herramientas), SafeGuard Enterprise incorporará dicho usuario.

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

Nota: los responsables de seguridad pueden asignar usuarios a la POA de SafeGuard en un equipo nuevo en SafeGuard Management Center. Los usuarios asignados de esta forma también pueden iniciar sesión en la POA de SafeGuard en el equipo correspondiente.

4.4 Contraseña temporal en la POA de SafeGuard

SafeGuard Enterprise le permite cambiar temporalmente la contraseña en la POA de SafeGuard. 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 de SafeGuard. Como no está conectado a Active Directory (AD), no puede cambiar su contraseña de Windows.

Solución: Puede cambiar temporalmente la contraseña de la POA de SafeGuard 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 de SafeGuard, 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 de SafeGuard.

5. Haga clic en **Aceptar**.

Se inicia la sesión en Windows.

Para iniciar la sesión en la POA de SafeGuard, 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 de SafeGuard hasta que no realice este paso.

Cambio de la contraseña temporal

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

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

Puede cerrar este cuadro de diálogo 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 de SafeGuard 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 de SafeGuard. Puede cerrar este cuadro de diálogo sin realizar ningún cambio y usar la "contraseña antigua" para iniciar sesión. Después, podrá cambiar la contraseña.

4.5 Inicio de sesión en la POA de SafeGuard mediante tarjetas inteligentes o tokens

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

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

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

El responsable de seguridad le proporcionará la tarjeta inteligente o token necesario. También se pueden incorporar las credenciales de Windows en la tarjeta inteligente o token.

Nota: SafeGuard Enterprise trata las tarjetas inteligentes y los tokens 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".

4.5.1 Primer inicio de sesión con token tras la instalación

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

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

Nota: se recomienda que configure su token con las credenciales de Windows antes de reiniciar el equipo, consulte Almacenamiento de credenciales de Windows en el token en la página 16. Las directivas de seguridad que se le aplican pueden exigir que utilice un token en la POA de SafeGuard. Si el token no contiene las credenciales, no podrá iniciar la sesión en la POA de SafeGuard.

4.5.2 Inicio de sesión en la POA de SafeGuard 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 un token en la POA de SafeGuard.

3. Introduzca el número PIN del token.

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

4.5.3 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 de SafeGuard, 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 de SafeGuard.

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.

4.5.4 Almacenar las credenciales de Windows en el token

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

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 de SafeGuard. Si el token no contiene las credenciales, no podrá iniciar la sesión en la POA de SafeGuard.

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 en 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 (es decir que ya ha iniciado la sesión en la POA de SafeGuard 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 de SafeGuard, 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.

4.5.5 Recuperación de inicio de sesión mediante token

Si utiliza un token no criptográfico y ha olvidado el PIN, puede volver a tener acceso a su equipo de dos formas:

- Recuperación mediante Local Self Help en la página 64.
- Recuperación con desafío/respuesta o clave de recuperación en la página 73.

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.

Nota: estos método de recuperación no están disponibles para tokens criptográficos. Si tiene problemas con el inicio de sesión, póngase en contacto con el responsable de seguridad.

4.5.6 Desbloquear el token

Si introduce el número PIN incorrectamente varias veces, el token se bloqueará. El responsable de seguridad puede configurar SafeGuard Enterprise 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).

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. Sin embargo, no puede cambiar el PIN o sus credenciales de usuario mediante dicho procedimiento.

4.5.7 Tokens criptográficos - Kerberos

Si utiliza un token criptográfico, la autenticación en la POA de SafeGuard se realizará mediante el certificado almacenado en el token.

Para este tipo de inicio de sesión, necesita un token aprobado. El responsable de seguridad o una persona autorizada le proporcionará este token. Para iniciar la sesión, sólo tiene que especificar el PIN del token. Si este tipo de inicio de sesión es el único válido para su equipo, no podrá iniciar la sesión sin el token.

Nota: si utiliza un token de esta forma, no podrá utilizar el procedimiento de desafío/respuesta ni Local Self Help para iniciar la sesión. Si tiene problemas con el inicio de sesión, póngase en contacto con el responsable de seguridad.

4.5.8 Cambiar el certificado del token

El responsable de seguridad debe asignar un certificado nuevo al equipo para cambiar o renovar el certificado para el inicio de sesión con token. Tras la sincronización con el servidor de SafeGuard Enterprise, se indicará al usuario que el sistema está **Preparado para cambiar certificado**.

El responsable de seguridad le proporcionará el token nuevo.

Para cambiar el certificado:

1. Inicie la sesión en la POA de SafeGuard con el método antiguo (token, o nombre de usuario y contraseña) sin inicio de sesión automático en Windows.

   Haga clic en **Opciones** y desactive **Inicio de sesión automático en Windows**, o cierre la sesión de Windows.

2. Inicie la sesión en Windows con el token nuevo.

Ya puede utilizar el token para iniciar sesión en la POA de SafeGuard. El token antiguo ya no es válido.

4.6 Autoinicio de sesión en la POA de SafeGuard con token

Requisitos previos:

- En la BIOS debe estar activada la compatibilidad con USB.
- La compatibilidad con token debe estar inicializada, y debe haber un token generado.
- El responsable de seguridad ha aplicado las directivas correspondientes.

Si se aplica una directiva con el PIN predeterminado, podrá iniciar la sesión directamente en la POA de SafeGuard con un token. No tiene que introducir credenciales ni el número PIN, sino que se transfieren de manera automática en la POA de SafeGuard. Según la directiva, también se podría iniciar la sesión en Windows.

Para iniciar la sesión en la POA de SafeGuard automáticamente con un token:

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

Se inicia la sesión automáticamente en la POA de SafeGuard. Según la directiva, también se podría iniciar la sesión en Windows.

- En este caso, se inicia Windows.
- De lo contrario, se le pedirá que introduzca el número PIN del token. Entonces inicia la sesión en la POA de SafeGuard.

4.7 Teclado virtual

En la POA de SafeGuard, 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 de SafeGuard, haga clic en **Opciones** en el cuadro de diálogo de la POA y marque la casilla **Teclado virtual**.

El teclado virtual es compatible con varias distribuciones de teclado. También es posible cambiar esta distribución utilizando las mismas opciones que las utilizadas para cambiar la distribución del teclado de la POA de SafeGuard, consulte Cambiar la distribución del teclado en la página 19.

4.8 Distribución del teclado

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

Por defecto, SafeGuard Enterprise utiliza el teclado predeterminado de Windows.

El idioma de la distribución del teclado utilizada se muestra en la POA de SafeGuard, por ejemplo, "EN" representa el inglés. Además de la distribución predeterminada del teclado, también se puede utilizar la distribución US (inglés, Estados Unidos).

4.8.1 Cambiar la distribución del teclado

Tanto la distribución del teclado de la POA de SafeGuard (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 de SafeGuard recuerda la distribución del teclado de la última sesión. Es necesario reiniciar el equipo dos veces. 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 de SafeGuard pueda configurar la nueva distribución.

Puede cambiar la distribución del teclado necesaria para la POA de SafeGuard 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`**.

4.9 Teclas de acceso rápido y de función compatibles en la POA de SafeGuard

Ciertas funciones y configuración del hardware pueden causar problemas al arrancar el equipo, provocando a su vez que se bloquee el sistema. La POA de SafeGuard 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 de SafeGuard antes de una nueva distribución de SafeGuard Enterprise en la red. El archivo de configuración se actualiza cada mes y está disponible en: http://www.sophos.com/es-es/support/knowledgebase/65700.aspx.

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 de SafeGuard.

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

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

La POA de SafeGuard también es compatible con ciertas teclas de función.

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

1. **Mayús - F5** 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 de SafeGuard. 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 de SafeGuard 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 de SafeGuard intenta realizar una copia de seguridad del controlador USB y restaurarlo. Dependiendo de la versión de BIOS utilizada, el sistema podría no responder.

Nota: los cambios que se pueden realizar mediante una combinación de teclas se pueden especificar durante la instalación de SafeGuard Enterprise mediante un archivo `.mst`.

Tras modificar la configuración de hardware con las teclas de acceso rápido en la POA de SafeGuard, 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 de SafeGuard, 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 de SafeGuard, 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**.

Para más información, consulte http://www.sophos.com/es-es/support/knowledgebase/107785.aspx.

4.9.2 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 de SafeGuard.

F8 = permite cambiar la contraseña de la POA de SafeGuard. Se debe utilizar en lugar de la tecla **Intro** para activar el cambio de contraseña en la POA de SafeGuard 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 de SafeGuard 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 SafeGuard de inicio de sesión con nombre de usuario y contraseña. Para más información, consulte Inicio de sesión con el lector de huellas digitales de Lenovo en la página 24.

4.10 Sincronización de la contraseña

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

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

La sincronización de la contraseña se producirá en dos situaciones:

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

5 Inicio de sesión en Windows

SafeGuard Enterprise ofrece un método de autenticación adicional.

Si desactiva la opción **Inicio de sesión automático en Windows** en la POA de SafeGuard, se mostrará el cuadro de inicio de sesión de Windows. En este cuadro de diálogo también puede seleccionar un método de autenticación distinto.

Nota: el uso de otro método de autenticación no significa que SafeGuard Enterprise no esté activo en el equipo. En ese caso, el inicio de sesión de SafeGuard Enterprise se realiza una vez iniciada la sesión en Windows.

5.1 Iniciar la sesión con SafeGuard Enterprise

Normalmente, la sesión de Windows se inicia de forma automática tras autenticarse en la POA de SafeGuard. Si desactiva la opción **Inicio de sesión automático en Windows** en el cuadro de inicio de sesión de la POA de SafeGuard y utiliza el método de SafeGuard Enterprise para iniciar la sesión en Windows, SafeGuard Enterprise sólo estará disponible tras iniciar la sesión en Windows.

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

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

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

Después de iniciar la sesión en Windows, se ejecutará el programa de autenticación de SafeGuard Enterprise 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**.

   A partir de ese momento, la funcionalidad de SafeGuard Enterprise está disponible y se puede, por ejemplo, tener acceso a los datos cifrados, siempre que se tenga la clave necesaria.

6 Inicio de sesión con el lector de huellas digitales de Lenovo

Nota: el inicio de sesión con el lector de huellas digitales de Lenovo solo es compatible en sistemas con Windows 7 (BIOS).

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

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 inicio de sesión y aumenta la seguridad.

SafeGuard Enterprise 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. 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.
- No es posible combinar en un mismo equipo procedimientos de conexión mediante token y huella digital.
- No se admite el inicio de sesión remoto 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 con un lector de huellas digitales
- Se recomienda disponer de la BIOS más actualizada
- SafeGuard Enterprise
- La versión del software recomendada por el fabricante debe estar instalada antes que SafeGuard Enterprise:
  - 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 7, 32 bits, 64 bits
- Windows 8, 32 bits, 64 bits

Hardware compatible

Para más información sobre software de inicio de sesión mediante huella dactilar compatible, consulte el artículo http://www.sophos.com/es-es/support/knowledgebase/108789.aspx.

Software compatible

Para más información sobre software de inicio de sesión mediante huella dactilar compatible, consulte el artículo http://www.sophos.com/es-es/support/knowledgebase/111626.aspx.

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 SafeGuard Enterprise.

1. autentíquese en la POA de SafeGuard (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 de SafeGuard, 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 ordenador.
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 sesión en la POA de SafeGuard 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 de SafeGuard 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 de SafeGuard 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 Iconos utilizados en el proceso de conexión en la página 26.

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 de SafeGuard 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 de SafeGuard para iniciar la sesión con el nombre de usuario y contraseña, consulte Inicio de sesión con nombre de usuario y contraseña en la página 28.

6.3.1 Iconos utilizados en el proceso de inicio de sesión

Cuando se inicia sesión en la POA (power-on authentication) de SafeGuard 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.

	Le solicita que pase el dedo sobre el lector de huellas digitales.
	Indica que el inicio de sesión mediante huella digital no está activado 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.

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

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 con huella digital esté habilitado, puede seguir iniciando sesión en la POA de SafeGuard con su nombre de usuario y contraseña, por ejemplo, si el lector de huellas digitales no funciona.

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

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

   Nota: si pulsa **Ctrl+Alt+Supr** en la POA de SafeGuard 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 de SafeGuard 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 de SafeGuard e iniciar la sesión mediante la huella digital.

   Si pulsó **Esc** para ir al cuadro de diálogo de la POA de SafeGuard e iniciar sesión con un nombre de usuario y una contraseña, puede seguir iniciando sesión mediante el lector de huellas digitales sin tener que volver primero al cuadro de diálogo de inicio de sesión con huella digital de la POA de SafeGuard.

6.4 Cambio de contraseña

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

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

3. Haga clic en **Opciones** y desactive la opción **Inicio de sesión automático en Windows**.

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

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, SafeGuard Enterprise dispone de los siguientes métodos de recuperación:

- Recuperación mediante Local Self Help en la página 64.
- Recuperación con desafío/respuesta o clave de recuperación en la página 73.

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 mediante huella digital.

Nota: debido al procedimiento de recuperación es posible que tenga que cambiar su contraseña al arrancar el equipo, por ejemplo, si ha olvidado su contraseña. En este caso, el sistema también le ofrecerá la posibilidad de actualizar las credenciales de la huella digital.

7 Cifrado de discos

SafeGuard Enterprise ofrece lo siguiente para cifrado de discos dependiendo del sistema operativo usado:

- **Windows 7:**
  - Cifrado completo de discos SafeGuard con SafeGuard Power-on Authentication, consulte Cifrado de discos SafeGuard en la página 31
  - BitLocker Drive Encryption con inicio de sesión de Windows, consulte Cifrado de unidad BitLocker en la página 34
- **Estaciones de trabajo con Windows 8:** BitLocker Drive Encryption con inicio de sesión de Windows, consulte Cifrado de unidad BitLocker en la página 34

7.1 Cifrado de discos SafeGuard

SafeGuard Enterprise proporciona cifrado transparente de discos por volúmenes. En las directivas de seguridad, el responsable de seguridad define los volúmenes que deben cifrarse.

7.1.1 Cifrado transparente

Los archivos de los volúmenes cifrados 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 un volumen cifrado a otra ubicación del equipo sin cifrado, se descifrarán. Los archivos se almacenarán en la nueva ubicación en estado original.

7.1.2 Cifrado inicial

Durante la configuración inicial de los equipos protegidos por SafeGuard Enterprise, se pueden crear y distribuir políticas de cifrado en un paquete de configuración a los ordenadores.

El cifrado inicial del sistema se realiza según la directiva que haya recibido el equipo.

7.1.2.1 Cifrado inicial para el cifrado de volúmenes

El cifrado inicial del sistema se inicia tan pronto como el equipo reciba una directiva de cifrado.

El cifrado inicial de volúmenes se realiza en segundo plano.

Nota: no debe poner el equipo en hibernación durante el cifrado inicial de la partición del sistema (es decir, la partición con el archivo hiberfil.sys). Tras el cifrado inicial de dicha partición, reinicie el equipo para asegurarse de que la hibernación funciona correctamente.

7.1.2.2 Restricciones para el cifrado inicial de equipos protegidos con SafeGuard Enterprise

Durante la configuración inicial de los equipos protegidos por SafeGuard Enterprise, se pueden crear y distribuir políticas de cifrado en un paquete de configuración a los ordenadores. Si el cliente de SafeGuard Enterprise no se conecta a un servidor de SafeGuard Enterprise inmediatamente después de instalar el paquete de configuración, sino que temporalmente está sin conexión, solamente las directivas de cifrado con esta configuración en concreto se activarán inmediatamente en el equipo protegido con SafeGuard Enterprise:

- Protección de dispositivos por volúmenes, utilizando la **clave del equipo** como clave de cifrado

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

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

7.1.3 Cifrado de discos por volúmenes

El cifrado de volúmenes en equipos de un volumen con SafeGuard Enterprise se inicia automáticamente si el responsable de seguridad ha definido la directiva correspondiente.

1. Se le pedirá que seleccione una clave de acceso.

   Nota: todos los usuarios que dispongan de esta clave podrán acceder a este volumen. El responsable de seguridad define el ámbito de las claves disponibles. Si el responsable de seguridad ha definido una clave, no podrá seleccionar ninguna otra.

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

   Se mostrará un visor de cifrado que indica el progreso 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 mostrarlo. 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:

   - El cifrado/descifrado de volúmenes no es posible en volúmenes que tienen una letra de unidad asignada.
   - En Windows 7 Professional, Enterprise y Ultimate se crea una partición de sistema en las estaciones que no tengan una letra de unidad asignada. Esta partición no se puede cifrar con SafeGuard Enterprise.
   - Si existe una directiva de cifrado para un volumen o un tipo de volumen y el cifrado falla, se impedirá el acceso a dicho volumen.
   - El equipo se puede apagar y reiniciar durante el proceso de cifrado o descifrado.
   - Si se va a realizar la desinstalación tras el descifrado, se recomienda no suspender ni hibernar el sistema.
   - Si tras el cifrado del volumen se aplica a una estación de trabajo una nueva política que permita el descifrado, tras completar el cifrado del disco, debe reiniciar la estación de trabajo al menos una vez antes de poder iniciar el descifrado.

   Nota:

   Al contrario que con el Cifrado de unidad Bitlocker de SafeGuard, el cifrado de volúmenes de SafeGuard no admite discos GPT. La instalación se interrumpirá si se encuentra este tipo de disco. Si se añade un disco GPT al sistema en un momento posterior, los volúmenes del disco se cifrarán. Por favor, tenga en cuenta que las herramientas de recuperación de SafeGuard, como por ejemplo BE_Restore.exe y recoverkeys.exe, no pueden manejar dichos volúmenes y Sophos recomienda evitar el cifrado de discos GPT. Para descifrar volúmenes cifrados accidentalmente, cambie sus políticas de SGN en consecuencia y haga que el usuario los descifre.

7.1.3.1 Restricciones de acceso a volúmenes

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

Volúmenes con un cifrado fallido

Si alguna directiva especifica 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 SafeGuard Enterprise no puede identificar con claridad si están cifrados o no.

Si alguna directiva especifica que se debe cifrar un 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.

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

7.2 Cifrado de unidad BitLocker

Cifrado de unidad BitLocker es una completa función de cifrado de discos con autenticación en la fase previa al arranque del equipo, incluida en los sistemas operativos de Windows. Permite proteger los volúmenes de datos el cifrado de la unidad de arranque. SafeGuard Enterprise administra Cifrado de unidad BitLocker y proporciona funciones adicionales.

7.2.1 Directivas de cifrado para BitLocker

El responsable de seguridad puede crear una directiva para el cifrado en SafeGuard Management Center y distribuirla a los equipos en los que se ejecute BitLocker.

Los clientes de BitLocker se gestionan de forma transparente en el SafeGuard Management Center. La misma política de cifrado se puede utilizar para clientes de Mac, el cifrado completo de discos de SafeGuard y de BitLocker. SafeGuard Enterprise conoce el estado de los clientes y selecciona el cifrado de BitLocker en consecuencia.

7.2.2 Autenticación con BitLocker

BitLocker ofrece toda una gama de opciones de autenticación. El responsable de seguridad establece el tipo de inicio de sesión desde SafeGuard Management Center y distribuye las directivas apropiadas a las estaciones.

Estos son los tipos de inicio de sesión disponibles para los usuarios de BitLocker de SafeGuard Enterprise:

- TPM
- TPM + PIN
- TPM + clave de inicio
- Clave de inicio únicamente (sin TPM)
- Contraseña (sin TPM)

Debe proporcionar estas credenciales cuando inicie su estación de trabajo de BitLocker.

Módulo de plataforma segura (TPM)

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

Clave de inicio en lápiz de memoria USB

Las claves externas se pueden almacenar en un lápiz de memoria USB no protegido. Debe insertar la memoria USB para la autenticación durante el arranque.

7.2.3 Cifrado en equipos protegidos con BitLocker

Cuando se envía la directiva de cifrado a un equipo protegido con BitLocker y antes de que el equipo vuelva a comenzar el cifrado inicial, BitLocker genera las claves de cifrado. Dependiendo del sistema utilizado, el comportamiento difiere ligeramente.

Estaciones con TPM

El responsable de seguridad puede definir TPM, TPM + PIN,TPM + Clave de inicio, Clave de inicio o contraseña como modo de inicio de sesión para BitLocker. Si se establece un modo de inicio de sesión con TPM, BitLocker almacena sus propias claves de cifrado en un dispositivo de hardware llamado el Módulo de plataforma segura (TPM). Las claves no se almacenan en el disco duro del equipo. El sistema básico de entrada/salida (BIOS) debe poder acceder al TPM durante el inicio. Al iniciar el equipo, BitLocker obtendrá dichas claves del TPM de forma automática.

Estaciones sin TPM

Si el equipo no cuenta con un TPM, bien se le pedirá que introduzca una contraseña o se le pedirá que cree una clave de inicio de BitLocker utilizando un lápiz de memoria USB para almacenar las claves de cifrado. A continuación, aparece un cuadro de diálogo con las unidades de destino válidas para almacenar la clave de inicio. Deberá insertar el lápiz de memoria cada vez que inicie el equipo.

Nota: en el caso de los **volúmenes de arranque**, es esencial que la clave de inicio esté disponible al iniciar la estación. Por lo tanto, la clave de inicio sólo puede almacenarse en medios extraíbles.

Para volúmenes de datos, la clave de inicio de BitLocker se puede almacenar en un volumen de arranque que ya esté cifrado. Esto se hará automáticamente, si el responsable de seguridad especificó **Desbloqueo automático** como el modo de inicio de sesión para los volúmenes que no son de arranque. De lo contrario, seleccione un dispositivo extraíble que se muestra en **Unidades de destino válidas** como lugar de almacenamiento.

Claves de recuperación de BitLocker

Para la recuperación de BitLocker, SafeGuard Enterprise ofrece un procedimiento de desafío/respuesta que permite el intercambio de información de forma confidencial y la obtención de la clave de recuperación de BitLocker del centro de ayuda, consulte Desafío/respuesta para usuarios de BitLocker en la página 79 y Clave de recuperación de BitLocker en la página 80.

Para habilitar la recuperación mediante el procedimiento de desafío/respuesta, el centro de ayuda tendrá que disponer de los datos necesarios. Los datos necesarios para la recuperación se cargan y se guardan en la base de datos de SafeGuard Enterprise.

Nota: si un volumen cifrado por BitLocker en un equipo se sustituye por un nuevo volumen cifrado por BitLocker y a éste se le asigna la misma letra de unidad que el anterior, SafeGuard Enterprise sólo guarda la clave de recuperación del nuevo volumen. Debe hacer una copia de seguridad de la clave del volumen anterior usando los mecanismos de seguridad que ofrece Microsoft.

Administrar volúmenes ya cifrados con BitLocker

Si ya existen volúmenes cifrados con BitLocker en su equipo, SafeGuard Enterprise se hace cargo de su gestión al instalarlo.

Cifrar volúmenes de arranque

- Según la compatibilidad con BitLocker de la versión de SafeGuard Enterprise utilizada, puede que necesite reiniciar el equipo. Es importante reiniciar el equipo lo antes posible.
- Si se aplica una política de cifrado de SafeGuard Enterprise para el volumen cifrado:
  - **Desafío/respuesta de BitLocker** está instalado: Se traspasa la administración y es posible el desafío/respuesta de SafeGuard.
  - **SafeGuard BitLocker** está instalado: Se traspasa la administración y es posible la recuperación con SafeGuard.
- Si no se aplica ninguna política de cifrado de SafeGuard Enterprise para el volumen cifrado:
  - **Desafío/respuesta de BitLocker** está instalado: No se traspasa la administración y no es posible el desafío/respuesta de SafeGuard.
  - **SafeGuard BitLocker** está instalado: No es posible la recuperación con SafeGuard.

Volumen de datos cifrados

- Si se aplica una política de cifrado de SafeGuard Enterprise para el volumen cifrado:

  Se traspasa la administración y es posible la recuperación de SafeGuard.
- Si no se aplica ninguna política de cifrado de SafeGuard Enterprise para el volumen cifrado:

  Es posible la recuperación de SafeGuard.

Importante: si un volumen cifrado por BitLocker en un equipo se sustituye por un nuevo volumen cifrado por BitLocker y a éste se le asigna la misma letra de unidad que el anterior, SafeGuard Enterprise sólo guarda la clave de recuperación del nuevo volumen. Debe hacer una copia de seguridad de la clave del volumen anterior usando los mecanismos de seguridad que ofrece Microsoft.

Nota: en ciertos casos, SafeGuard Enterprise no puede hacerse cargo de la administración de un volumen ya cifrado. En este caso, no puede usar SafeGuard Enterprise para el proceso de recuperación. Póngase en contacto con el responsable de seguridad.

7.2.4 Cifrado inicial en un equipo protegido con BitLocker

Dependiendo del modo de inicio de sesión que haya especificado el responsable de seguridad para su estación de trabajo, el comportamiento del uso de SafeGuard Enterprise BitLocker difiere ligeramente.

En cualquier caso se le presentará un cuadro de diálogo en el que se le ofrece la posibilidad de proceder con el cifrado o posponerlo.

Si confirma que desea guardar, reiniciar y/o cifrar, el cifrado todavía no se iniciará inmediatamente. Se realizará una prueba de hardware para asegurarse de que la estación de trabajo cumple los requisitos para el cifrado de SafeGuard Enterprise BitLocker. El sistema realiza un reinicio y comprueba si se cumplen todos los requisitos de hardware. Si por ejemplo el lápiz de memoria USB o el TPM no está disponible o no es accesible, se le pedirá que almacene la clave externa en otro dispositivo. El sistema también verifica si es capaz de proporcionar las credenciales correctamente. Si no puede proporcionar las credenciales, el

ordenador arrancará de todos modos, pero no se iniciará el cifrado. Deberá introducir su contraseña o PIN otra vez. Después de una prueba exitosa de hardware, comenzará el cifrado de BitLocker.

Si selecciona **Posponer**, el cifrado no se iniciará y no se le pedirá otra vez que cifre este volumen hasta que:

- llegue una nueva política,
- el estado de cifrado de BitLocker de cualquier volumen cambie, o
- inicie sesión en el sistema otra vez.

Nota: si SafeGuard Enterprise gestiona el cifrado de la unidad de BitLocker para su unidad de sistema operativo o volúmenes de datos fijos, no active BitLocker de forma manual para estos volúmenes.

7.2.4.1 Guardar clave de inicio

Si su oficial de seguridad especificó que debía usar **TPM + clave de inicio** o **Clave de inicio** como la forma en la que debe iniciar sesión, deberá especificar la ubicación en la que se guarda la llave de arranque. Inserte un lápiz de memoria USB para almacenar la clave. No utilice un dispositivo de memoria USB cifrado. Las unidades de destino válidas para la clave de inicio se muestran en el cuadro de diálogo. Más adelante, deberá insertar la clave cada vez que inicie el equipo.

Seleccione la unidad de destino y haga clic en **Guardar y reiniciar**.

7.2.4.2 Establecer contraseña

Si su responsable de seguridad especificó **Contraseña** como el modo de inicio de sesión, se le pedirá que escriba su nueva contraseña y que la confirme. Más adelante necesitará esta contraseña cada vez que inicie su equipo. La longitud y la complejidad que se requieren para la contraseña depende de los objetos de la política de grupos que haya especificado su responsable de seguridad. En el cuadro de diálogo se le informa sobre los requisitos de la contraseña.

Nota: si utiliza caracteres especiales en su contraseña, tenga en cuenta que la distribución del teclado que utilice puede ser diferente de la distribución del teclado EN-US que utiliza BitLocker. Considere establecer la distribución de su teclado temporalmente a EN-US con el propósito de establecer la contraseña.

7.2.4.3 Establecer PIN

Si su responsable de seguridad especificó **TPM + PIN** como el modo de inicio de sesión, se le pedirá que escriba su nuevo PIN y que lo confirme. Más adelante necesitará este PIN cada vez que inicie su equipo. La longitud y la complejidad que se requieren depende de los objetos de la política de grupos que haya especificado su responsable de seguridad. En el cuadro de diálogo se le informa sobre los requisitos de lo PIN.

Nota: si su responsable de seguridad ha activado los llamados PIN mejorados, puede usar caracteres especiales en su PIN. Tenga en cuenta que la distribución del teclado que utilice puede ser diferente de la distribución del teclado EN-US que utiliza BitLocker. Considere establecer la distribución de su teclado temporalmente a EN-US con el propósito de establecer el PIN.

7.2.4.4 Diálogo para TPM sólo

Si su responsable de seguridad especificó **TPM** como el modo de inicio de sesión, sólo tiene que confirmar el reinicio y el cifrado de su estación de trabajo.

7.2.5 Descifrado con BitLocker

Los equipos cifrados con BitLocker no se pueden descifrar automáticamente. El descifrado debe llevarse a cabo utilizando ya sea el elemento **Cifrado de unidad BitLocker** del **Panel de control** o la herramienta de línea de comandos de Microsoft "Manage-bde".

8 SafeGuard Data Exchange

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

Sólo los usuarios que dispongan de las claves apropiadas podrán 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 accesos no autorizados. Los usuarios no autorizados pueden acceder a los archivos físicamente, pero no pueden leerlos sin SafeGuard Data Exchange y la clave pertinente.

Nota: el comportamiento de SafeGuard Data Exchange en su equipo lo define centralmente el responsable de seguridad.

En la administración central, el responsable de seguridad 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:

- **El equipo destinatario dispone de SafeGuard Enterprise**: puede usar las claves disponibles para ambos (usted y el destinatario) o puede crear una nueva. Si genera una clave nueva, tendrá que proporcionar al destinatario de los datos la frase de acceso para la clave.
- **El equipo destinatario *no* dispone de SafeGuard Enterprise:** SafeGuard Enterprise 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.

Importante: cuando se extrae un archivo ZIP usando el archivador integrado de Microsoft Windows, el proceso se detiene tan pronto como se encuentra un archivo cifrado para el cual no está disponible la clave. El usuario recibe un mensaje de que se ha denegado el acceso, pero no se le informa de que hay archivos que no han sido procesados y, por tanto, están desaparecidos. Otros archivadores, por ejemplo, 7-Zip, trabajan muy bien con archivos ZIP que contienen archivos cifrados.

8.1 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.
- **El usuario puede cancelar el cifrado inicial**: cuando comience el cifrado inicial, se muestra un cuadro de diálogo que le permite cancelarlo.
- **El usuario puede acceder a archivos sin cifrar**: **No**: en este caso, SafeGuard Data Exchange sólo aceptará datos cifrados en los medios extraíbles. Si hay datos sin cifrar en los medios extraíbles, el sistema no le permitirá tener acceso a ellos. Sólo después de cifrar los archivos, obtendrá acceso a los datos.
- **El usuario puede 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.
- **El usuario puede definir una contraseña de acceso al medio para dispositivos**: se le pedirá que introduzca una contraseña de acceso al medio la primera vez que conecte un medio extraíble.
- **Carpeta sin cifrar**: el responsable de seguridad puede definir una carpeta sin cifrar que se creará en todos los medios extraíbles. Los archivos en esta carpeta no se cifran.
- **El usuario puede decidir sobre el cifrado**: al conectar un medio extraíble, se le preguntará si desea cifrar los archivos en dicho medio. Además, si la directiva lo permite, se le ofrecerá la posibilidad de recordar la respuesta y aplicarla cada vez que se conecte el medio. En ese caso, podrá seleccionar la opción **Recordar y no mostrar de nuevo**; el cuadro de diálogo no se volverá a mostrar para el medio en cuestión. En este caso, en el Explorador de Windows dispondrá de la opción **Reactivar cifrado** en el menú contextual de dicho medio. Utilice este comando si desea cambiar su decisión respecto al cifrado del medio en cuestión. Si no es posible, por ejemplo si no dispone de los derechos necesarios, se mostrará un mensaje de error. Una vez cambiada su decisión, deberá decidir en otro cuadro de diálogo el cifrado del dispositivo en cuestión.

8.2 Una única frase de acceso para todos los dispositivos de medios 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 al medio está vinculada a los equipos para los que tenga permiso de acceso. Esto significa que puede utilizar la misma frase de acceso en todos ellos.

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

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

- Desea utilizar los datos cifrados de medios extraíbles en equipos en los que SafeGuard Enterprise 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 proporcionando al usuario externo sólo la frase de acceso al medio de una clave determinada (denominada clave local, que puede crear un usuario de SafeGuard Data Exchange). En este caso, el usuario externo sólo tendrá acceso a los archivos cifrados con esta clave y no podrá visualizar los demás archivos.

Nota: no es necesario especificar una frase de acceso al medio si utiliza claves de grupo de SafeGuard Enterprise para intercambiar datos de medios extraíbles en un grupo de trabajo cuyos miembros comparten dicha clave. En ese caso, si así lo establece el responsable de seguridad, el acceso a los archivos cifrados en medios extraíbles es totalmente transparente. No es necesario que introduzca la clave ni frase de acceso. Esto se debe a que las claves de grupo y las frase de acceso para medios extraíbles se pueden utilizar simultáneamente. Ya que el sistema detecta de manera automática si hay una clave de grupo disponible, los usuarios que compartan dicha clave tendrán total acceso. Si no se detecta ninguna clave de grupo, SafeGuard Data Exchange solicitará la frase de acceso al medio o la frase de acceso de una clave local.

Medios compatibles

SafeGuard Data Exchange admite los siguientes medios extraíbles:

- Claves de inicio
- Discos duros externos con conexión USB o FireWire
- Unidades CD RW (UDF)
- Unidades DVD RW (UDF)
- Tarjetas de memoria en lectores de tarjetas USB

8.3 Cifrado de medios extraíbles

El cifrado de datos no cifrados en los medios extraíbles o bien comienza automáticamente tan pronto como conecte los medios al sistema, o deberá iniciar el proceso manualmente. Todos los procesos de cifrado y descifrado posteriores se ejecutan de forma transparente e implican una interacción mínima del usuario.

8.3.1 Cifrado inicial

El cifrado de datos no cifrados 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.

Para iniciar el cifrado de forma manual:

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

Nota: para intercambiar datos con los usuarios que tengan SafeGuard Enterprise instalado en sus equipos, pero que no utilicen la misma clave que usted, se requieren claves locales generadas por el usuario o se debe utilizar una frase de acceso al medio. Estas claves también se requieren para proteger el intercambio de datos con usuarios que no utilizan SafeGuard Enterprise. Puede identificar las claves locales por su prefijo (Local_).

Si está activada la opción **Cifrar archivos sin cifrar y actualizar archivos cifrados**, los archivos cifrados para los que existe una clave se descifrarán y se volverán a cifrar con la clave nueva.

Cancelar 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 una directiva, se le pedirá que introduzca la frase de acceso al medio antes del proceso de cifrado inicial. La frase 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 comenzará al introducir la frase de acceso al medio.

Tras introducir una vez la frase de acceso al medio, el cifrado inicial comenzará automáticamente cuando conecte otro dispositivo al equipo.

Nota: el cifrado inicial no se inicia en equipos que no cuentan con una frase de acceso al medio.

8.3.2 Cifrado manual

Si se le permite decidir sobre el cifrado de unidades externas, podrá iniciar el proceso de cifrado de forma manual. De esta forma podrá cifrar archivos ya cifrados mediante otra clave.

Para 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 y 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.

Nota: para intercambiar datos con los usuarios que tengan SafeGuard Enterprise instalado en sus equipos, pero que no utilicen la misma clave que usted, se requieren claves locales generadas por el usuario o se debe utilizar una frase de acceso al medio. Estas claves también se requieren para proteger el intercambio de datos con usuarios que no utilizan SafeGuard Enterprise. Puede identificar las claves locales por su prefijo (Local_).

Si está activada la opción **Cifrar archivos sin cifrar y actualizar archivos cifrados**, los archivos cifrados para los que existe una clave se descifrarán y se volverán a cifrar con la clave nueva.

8.3.3 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 un directiva de cifrado distinta, los datos se cifrarán en consecuencia.

8.3.3.1 Frase de acceso a medios

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.

8.3.3.2 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 inicie la sesión.

Reinicie la sesión inmediatamente. Se le informará de que no hay ninguna frase de acceso en su equipo y se le pedirá que introduzca una nueva.

8.3.3.3 Sincronización de la frase de acceso

La frase de acceso a medios en sus dispositivos y 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).

8.4 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 SafeGuard Enterprise que tienen al menos una clave que está incluida en su juego de claves.

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

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

  En este caso, cree una clave local y cifre los datos con ella. Las claves que se crean localmente se protegen mediante una frase de acceso y SafeGuard Enterprise puede importarlas. El destinatario de los datos se proporciona con la frase de acceso. Con la frase de acceso, el destinatario podrá importar la clave y acceder a los datos.

- Intercambio de datos con usuarios sin SafeGuard Enterprise

  Los usuarios que no dispongan de SafeGuard Enterprise pueden utilizar SafeGuard Portable. Para intercambiar datos con SafeGuard Portable también hay que utilizar claves locales, combinadas con una frase de acceso.

  Además, SafeGuard Portable se tiene que copiar al medio de almacenamiento extraíble. También debe proporcionar la frase de acceso pertinente al destinatario de los datos cifrados. Con la frase de acceso 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.

8.4.1 Importar claves desde un archivo

Si recibe alguna unidad extraíble o desea acceder a una unidad compartida 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.

1. Seleccione el archivo pertinente en el dispositivo extraíble y haga clic en **Cifrado de archivos > Importar clave desde archivo**.
2. Introduzca la frase de acceso.

La clave se importará y tendrá acceso al archivo.

8.4.2 Crear claves locales

1. Haga clic con el botón derecho en el icono de SafeGuard Enterprise en la bandeja del sistema de Windows o en un volumen/carpeta/archivo.
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. Si accedió a este cuadro haciendo clic con el botón derecho, se incluirá la opción **Utilizar como nueva clave predeterminada para la ruta**. La opción Utilizar como nueva clave predeterminada para la ruta le permite establecer de manera inmediata la nueva clave como la predeterminada para el volumen seleccionado o la carpeta de sincronización de Cloud Storage.

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

6. Haga clic en **Aceptar**.

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

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

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.

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

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 no cifrados).

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 no cifrado. 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 sin cifrar 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 cifrar los archivos al grabarlos en el 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.

8.5.1 Grabación de CD/DVD

Windows tiene un Asistente para grabación de CD para 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.

8.6 SafeGuard Portable

Con SafeGuard Portable puede intercambiar datos cifrados a través de medios extraíbles con destinatarios que no tengan SafeGuard Data Exchange instalado en sus equipos. Los datos cifrados 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 frase de acceso al medio relevante se obtendrá acceso a todos los archivos cifrados, independientemente de la clave local que se haya utilizado para cifrarlos. La frase de acceso de una clave local solo le proporciona 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 frase de acceso al medio o la frase de acceso 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: los usuarios de SafeGuard Enterprise no suelen necesitar SafeGuard Portable. La descripción que se facilita a continuación asume que los usuarios no tienen instalado SafeGuard Enterprise en sus equipos y que, por lo tanto, deben utilizar SafeGuard Portable para editar los datos cifrados.

8.6.1 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.

2. Para editar archivos en el medio extraíble, seleccione el archivo 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.
Borrar	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.

8.6.1.1 Establecer la clave de cifrado

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

1. En el menú contextual, o bien desde el menú **Archivo**, seleccione **Establecer clave de cifrado**.

   Aparecerá el cuadro de diálogo **Clave**.

2. Especifique un **Nombre** y una **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.

8.6.1.2 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.

8.6.1.3 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.

8.6.1.4 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.

8.6.1.5 Cómo 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.

8.6.2 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 descifrará y se abrirá.

- **Borrar**: 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 otro volumen del equipo.

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

  Salir cierra SafeGuard Portable.

9 SafeGuard File Encryption

El módulo File Encryption de SafeGuard Enterprise ofrece el cifrado de archivos en unidades locales y de red. Está especialmente diseñado para el trabajo en grupo y permite almacenar de forma segura los datos en unidades compartidas de red.

Tras aplicarse una directiva de **File Encryption** en su equipo, los archivos en los lugares especificados por dicha directiva se cifrarán de forma transparente sin interacción del usuario:

- Los archivos nuevos se cifran de forma automática.
- Si dispone de la clave para los archivos cifrados, podrá ver y modificar el contenido.
- Si no dispone de la clave para los archivos cifrados, no podrá abrirlos.
- Si accede a un archivo cifrado en un equipo que no dispone de File Encryption, se mostrará el contenido cifrado.
- Puede comprobar el estado de cifrado de los archivos mediante la extensión SafeGuard Enterprise Explorer para el cifrado basado en archivos, consulte Extensiones del explorador para el cifrado basado en archvivos en la página 60.

9.1 Cifrado según la directiva

Tras aplicarse una directiva de **File Encryption** a su equipo, los archivos existentes en las ubicaciones especificadas por dicha directiva no se cifrarán de forma automática. Se tiene que realizar un cifrado inicial.

Se recomienda realizar este cifrado inicial tan pronto como el equipo disponga de la directiva File Encryption, aunque es posible que el responsable de seguridad inicie el cifrado de forma automática. Esto es para asegurar que los datos se cifren lo antes posible según la directiva una vez haya recibido la directiva File Encryption.

Algunas aplicaciones crean un nuevo archivo después de modificar el contenido de un archivo y eliminar el antiguo. Únicamente para estas aplicaciones es cierto que el archivo se cifra después de ser modificado. El resto de aplicaciones dejan el archivo sin cifrar si no estaba cifrado antes de modificarse.

Para iniciar el cifrado de forma manual:

1. Seleccione **Cifrado de archivos > Cifrar según directiva** en el menú contextual de *Mi PC* en el Explorador de Windows.
2. Se mostrará el asistente de cifrado de archivos de SafeGuard.

   Se cifrarán todos los archivos en las carpetas y subcarpetas incluidas en las reglas de cifrado con la clave correspondiente.

9.2 Asistente de cifrado de archivos de SafeGuard

El asistente de cifrado de archivos de SafeGuard aparece cuando selecciona **Cifrar según directiva** en el menú contextual de Mi PC o **Iniciar cifrado** en el menú contextual de carpetas y archivos en el Explorador de Windows.

Esta aplicación se encarga de comprobar las carpetas definidas en las directivas aplicadas:

- Los archivos sin cifrar se cifrarán con la clave correspondiente.
- Los archivos cifrados con otra clave se volverán a cifrar con la clave correspondiente.
- Se mostrará un error si el usuario no dispone de la clave actual.
- Los archivos cifrados que deberían ser de texto según la política de cifrado aplicable siguen cifrados.

Un icono indica el estado de la operación:

- **Verde:** la operación se completó con éxito.
- **Rojo:** la operación se completó con errores.
- **Amarillo:** la operación se encuentra en progreso.

Diferentes fichas incluyen información detallada sobre los archivos procesados:

- La ficha **Resumen** muestra el número de archivos encontrados, cifrados, vueltos a cifrar, etc. El botón **Exportar** permite guardar el resultado del proceso en un archivo XML.
- La ficha **Errores** muestra los archivos que no se pudieron procesar correctamente.
- La ficha **Modificado** muestra los archivos que se han modificado correctamente.
- La ficha Todo muestra todos los archivos procesados y sus resultados.

Haga clic en el botón **Detener** si desea cancelar la operación. A continuación, el botón **Detener** cambia a **Reiniciar**.

Si el proceso se completa con errores, el botón **Detener** cambia a **Reintentar**. Haga clic en el botón **Reintentar** si desea volver repetir la operación en los archivos que no se pudieron procesar.

9.3 Cifrado permanente

El contenido de los archivos cifrados con File Encryption se descifran automáticamente si dispone de la clave correspondiente. Cuando el contenido se guarda en un nuevo archivo en una ubicación fuera de las especificadas en la regla de cifrado, el archivo resultante no cifrará.

Con el cifrado persistente, se cifrarán copias de archivos cifrados, incluso cuando estén guardadas en una ubicación fuera de las especificadas en una regla de cifrado.

Nota: los responsables de seguridad pueden desactivar este comportamiento. Si se desactiva, no se cifrarán los archivos que copie o mueva a otra ubicación.

10 SafeGuard Cloud Storage

El módulo Cloud Storage de SafeGuard Enterprise ofrece cifrado de archivos para datos almacenados en la nube.

No afecta al modo en que trabaja con archivos almacenados de este modo. Pero Cloud Storage asegura que las copias locales de sus datos en la nube se cifren de forma transparente y que permanecen cifrados al almacenarlos en la nube.

Nota: no arrastre y suelte archivos en el icono de Dropbox del escritorio de Windows para añadirlos a la carpeta de Dropbox. Los archivos se copiarán en la carpeta de Dropbox sin cifrar. Para cifrar archivos de forma transparente, cópielos directamente en la carpeta de Dropbox.

Importante: cuando se extrae un archivo ZIP usando el archivador integrado de Microsoft Windows, el proceso se detiene tan pronto como se encuentra un archivo cifrado para el cual no está disponible la clave. El usuario recibe un mensaje de que se ha denegado el acceso, pero no se le informa de que hay archivos que no han sido procesados y, por tanto, están desaparecidos. Otros archivadores, por ejemplo, 7-Zip, trabajan muy bien con archivos ZIP que contienen archivos cifrados.

10.1 Detección automática de Cloud Storage

SafeGuard Cloud Storage detecta de forma automática el proveedor de almacenamiento en la nube. La política de cifrado se aplicará de forma automática a la carpeta de sincronización.

10.2 Cifrado inicial de Cloud Storage

SafeGuard Cloud Storage no realiza un cifrado inicial de los archivos en la nube. Los archivos existentes antes de instalar SafeGuard Cloud Storage permanecerán sin cifrar.

Si desea cifrar estos archivos, debe eliminarlos de la nube primero y luego añadirlos de nuevo.

10.3 Establecer las claves predeterminadas

SafeGuard Cloud Storage permite establecer las claves predeterminadas para el cifrado de datos almacenados en la nube. Mediante las claves predeterminadas puede aplicar una clave diferente a cada subcarpeta en la nube. Establezca las claves predeterminadas seleccionando **Cifrado de archivos > Establecer clave predeterminada...** en SafeGuard Explorer Extensions como se describe en la sección Definir la clave predeterminada en la página 61.

Nota: el responsable de seguridad debe autorizar explícitamente el uso de claves predeterminadas para Cloud Storage. De esta forma el usuario podrá seleccionar la clave predeterminada de entre las que se incluyan en el juego de llaves predefinido.

Nota: para leer archivos cifrados en dispositivos Android e iOS con Sophos Mobile Encryption es necesario usar claves locales para el cifrado. Para más información sobre Sophos Mobile Encryption, consulte la *Ayuda de Sophos Mobile Encryption*.

Por ejemplo, puede que desee ofrecer datos seguros a diferentes socios a través de Dropbox. Cada socio sólo debe disponer de acceso a una subcarpeta. Para conseguirlo, basta con asignar una clave diferente a cada subcarpeta. SafeGuard Enterprise añadirá SafeGuard

Portable a cada subcarpeta para que los socios que no dispongan de SafeGuard Cloud Storage puedan acceder a los datos cifrados. Debe proporcionar la frase de acceso correspondiente a cada clave. Con SafeGuard Portable y la frase de acceso correspondiente, sus socios podrá descifrar los datos en la carpeta que ha creado para ellos, pero no podrán acceder a los datos almacenados en las demás carpetas ya que están cifradas con una clave distinta.

10.4 SafeGuard Portable para Cloud Storage

Posiblemente quiera acceder a su almacenamiento en la nube desde su casa o compartir datos cifrados en la nube mediante una carpeta compartida en la nube. SafeGuard Portable permite el acceso a archivos cifrados almacenados en la nube sin tener instalado SafeGuard Cloud Storage.

Los datos cifrados con SafeGuard Cloud Storage se pueden cifrar y descifrar con SafeGuard Portable. Esto se logra mediante un programa (SGPortable.exe) que se copia automáticamente a la carpeta de sincronización.

La frase de acceso de una clave local solo brinda acceso a los archivos que se hayan cifrado con esta clave determinada. Usted o cualquier destinatario podrá descifrar los datos cifrados y volverlos a cifrar de nuevo.

Nota: la frase de acceso de una clave local debe comunicarse por adelantado al destinatario.

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

No es necesario que SafeGuard Portable se instale o se copie en el equipo de la otra persona. Permanece en la nube.

Para más información sobre cómo utilizar SafeGuard Portable, consulte Editar archivos con SafeGuard Portable en la página 47.

Nota: al hacer doble clic en un archivo o al seleccionar el comando abrir, el archivo en cuestión no se descifra de forma automática, ya que cualquier archivo descifrado en las carpeta de sincronización del almacenamiento en la nube se sincroniza automáticamente en la nube. En su lugar, se mostrará un cuadro de diálogo donde podrá seleccionar una ubicación segura para copiar el archivo descifrado. Los archivos descifrados no se borran de forma automática al cerrar SafeGuard Portable. Los cambios realizados en archivos descifrados usando SafeGuard Portable para Cloud Storage no se realizan en los originales cifrados.

Nota: no debe crear carpetas de sincronización con la nube en unidades extraíbles ni en la red. De lo contrario, SafeGuard Portable creará archivos sin cifrar en estas carpetas No debe utilizar SafeGuard Portable de esta forma. Cree las carpetas de sincronización con la nube en discos duro.

11 SafeGuard Enterprise 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 el estándar Opal que se utiliza en este tipo de unidades. Diferentes fabricantes utilizan Opal. SafeGuard Enterprise es compatible con Opal y permite el uso de estas unidades. Para más información, consulte http://www.sophos.com/es-es/support/knowledgebase/113366.aspx.

11.1 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 128/256. Esta contraseña se puede administrar en SafeGuard Enterprise mediante una directiva de cifrado. El responsable de seguridad especifica la directiva de cifrado en SafeGuard Management Center y la distribuye a los equipos.

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

Cuando SafeGuard Enterprise se instala en un equipo, el icono de SafeGuard Enterprise se muestra en la bandeja del sistema. Podrá definir de forma centralizada todas las funciones ofrecidas por SafeGuard Enterprise en su equipo. Tenga en cuenta que las funciones disponibles dependen de la configuración definida en SafeGuard Management Center. El responsable de seguridad especifica centralmente esta configuración en SafeGuard Management Center y la distribuye a las estaciones.

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

12 Icono de la bandeja del sistema y la información mostrada

El icono de SafeGuard Enterprise permite acceder a las funciones necesarias. El icono de SafeGuard Enterprise se encuentra en la bandeja del sistema.

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

A través del icono de la bandeja del sistema puede visualizar información y realizar acciones concretas. Haga clic en el icono con el botón derecho del ratón para mostrar un menú con las siguientes entradas:

- **Mostrar**:
  - **Juego de claves**: Muestra todas las claves que tiene a su disposición.

    Nota: si su estación de trabajo ha sido migrada desde un entorno no gestionado a uno gestionado, puede que sea necesario un segundo inicio de sesión en SafeGuard Enterprise para que se puedan mostrar las claves locales definidas por el usuario en su archivo de claves.

  - **Certificado de usuario**: Muestra la información relativa al certificado.
  - **Certificado de empresa**: Muestra la información relativa al certificado de empresa utilizado.
- **Crear nueva clave**: Permite crear una clave nueva para el intercambio de datos con medios extraíbles o SafeGuard Cloud, consulte SafeGuard Data Exchange en la página 39 y SafeGuard Cloud Storage en la página 53.
- **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 contextual del icono de la bandeja del sistema. 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 64.
- **Cambiar frase de acceso del medio**: Permite cambiar la frase de acceso del medio, consulte SafeGuard Data Exchange en la página 39.
- **Sincronizar**: Inicia la sincronización de datos con el servidor de SafeGuard Enterprise. La información sobre herramientas muestra el progreso y el resultado de la sincronización de datos.

  Nota: la sincronización también se puede iniciar haciendo doble clic en el icono de la bandeja del sistema.
- **Estado**: Muestra información sobre el estado actual del equipo protegido con **SafeGuard Enterprise**:

Campo	Información
Última directiva recibida	Muestra la fecha y la hora en que el equipo recibió una directiva nueva por última vez.
Última clave recibida	Muestra la fecha y la hora en que el equipo recibió una clave nueva por última vez.
Último certificado recibido	Muestra la fecha y la hora en que el equipo recibió un certificado nuevo por última vez.
Último contacto con el servidor	Muestra la fecha y la hora del último contacto con el servidor.
Estado de usuario de SGN	Muestra el estado del usuario que tiene la sesión iniciada en el equipo (sesión de Windows): ▪ **Pendiente**: La replicación del usuario en la POA de SafeGuard está pendiente, es decir, aún no ha finalizado la sincronización inicial del usuario. Esto es especialmente importante al iniciar la sesión por primera vez tras instalar SafeGuard Enterprise, ya que sólo se puede iniciar la sesión en la POA de SafeGuard cuando se haya completado la sincronización inicial de usuario. ▪ **Usuario SGN**: El usuario que está conectado a Windows es un usuario de SafeGuard Enterprise. Un usuario de SGN tiene permiso para iniciar la sesión en la SafeGuard POA (power-on authentication), se añade a la UMA (Asignación de usuarios de equipos) y se le facilita un certificado de usuario y un juego de claves para que pueda acceder a datos cifrados. ▪ **Usuario de SGN (propietario)**: Siempre que no se hayacambiado la configuración predeterminada, un propietario tiene derecho a permitir que otros usuarios puedan iniciar sesión en la estación de trabajo y convertirse en usuarios de SGN. ▪ **Invitado de SGN**: Los usuarios de SGN invitados no se añaden a la UMA, no se les facilitan derechos para iniciar sesión en la SafeGuard POA, no se les asigna un certificado o un juego de claves y no se guardan en la base de datos. ▪ **Invitado de SGN (cuenta de servicio)**. El usuario que tiene iniciada la sesión en Windows es un usuario invitado de SafeGuard Enterprise mediante una cuenta de servicio para tareas de administración.

Campo	Información
	▪ **Usuario de Windows de SGN** Un usuario de Windows de SafeGuard Enterprise no es añadido a la POA de SafeGuard, pero tiene un juego de claves para acceder a los archivos cifrados, igual que un usuario de SafeGuard Enterprise. Los usuarios se añaden a la UMA. Esto significa que pueden iniciar sesión en Windows en esa estación de trabajo. ▪ **Desconocido**: Indica que no se ha podido determinar el estado del usuario.
Estado de la memoria caché de la directiva **Paquetes de datos preparados para la transmisión**	Indica si hay algún paquete que enviar al servidor de SafeGuard Enterprise.
Estado de Local Self Help (LSH) **Activado** **Activo**	Indica si Local Self Help se ha habilitado mediante una directiva y si el usuario lo ha activado en el equipo.
Listo para el cambio de certificado	Se muestra si el responsable de seguridad ha asignado un certificado nuevo al equipo para iniciar sesión con token. Ahora puede cambiar el certificado para el inicio de sesión con token, consulte Cambiar el certificado para el inicio de sesión con token en la página 18.

- **Ayuda**: Abre la ayuda de SafeGuard Enterprise.
- **Acerca de SafeGuard Enterprise**: Muestra información sobre la versión de SafeGuard Enterprise.

12.1 Crear claves locales

1. Haga clic con el botón derecho en el icono de SafeGuard Enterprise en la bandeja del sistema de Windows o en un volumen/carpeta/archivo.
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. Si accedió a este cuadro haciendo clic con el botón derecho, se incluirá la opción **Utilizar como nueva clave predeterminada para la ruta**. La opción Utilizar como nueva clave predeterminada para la ruta le permite establecer de manera inmediata la nueva clave como la predeterminada para el volumen seleccionado o la carpeta de sincronización de Cloud Storage.

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

6. Haga clic en **Aceptar**.

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

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

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.

12.2 Iconos superpuestos

Los iconos superpuestos son pequeños iconos que aparecen en elementos del explorador de Windows. Los iconos superpuestos de Data Exchange sólo se muestran en archivos y volúmenes. Su función es proporcionar información rápida sobre el estado del cifrado de un archivo o si se aplica una regla de cifrado a un volumen.

- La llave roja indica que no tiene una clave para descifrar un archivo. Este icono sólo aparece en archivos.
- La llave verde se muestra si un archivo está cifrado y su clave está en su juego de claves. Este icono sólo aparece en archivos.
- La llave gris se muestra si un archivo no está cifrado, pero hay disponible una regla de cifrado para ese archivo. Este icono sólo aparece en archivos.
- La llave amarilla se muestra si una unidad tiene una política de cifrado definida. Este icono sólo aparece en unidades.

Los iconos superpuestos sólo se mostrarán en volúmenes, medios extraíbles y CD/DVD que no sean de arranque. En las unidades de arranque, los iconos superpuestos se mostrarán en la carpeta provisional de grabación (la carpeta donde Windows almacena los archivos antes de grabarlos en un CD o DVD). Si se especifica una carpeta cifrada, entonces no se mostrará ninguna llave gris en los archivos sin cifrar de esa carpeta y sus subcarpetas. En términos generales, si un archivo no tiene ninguna norma de cifrado aplicada, no se muestra ninguna llave gris.

13 Acceder a funciones desde el Explorador de Windows

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

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/carpeta/archivo.

13.1 Extensiones del explorador para el cifrado de archivos

Puede acceder a las funciones de cifrado de archivos (Data Exchange, File Encryption, Cloud Storage) desde el menú contextual del Explorador de Windows. Las funciones están disponibles en los menús contextuales de

- 'Mi PC'
- medios extraíbles
- carpetas
- archivos

Las funciones que se muestran en los menús dependen de los componentes instalados.

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

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

Están disponibles las siguientes funciones:

- **Cifrar según directiva**: sólo está disponible si dispone de File Encryption y sólo en el menú contextual de 'Mi PC'. Si selecciona esta opción, se cifrarán todos los archivos en las carpetas especificadas con la clave correspondiente.
- **Iniciar cifrado**: si selecciona esta opción, todos los archivos se podrán cifrar o volver a cifrar. Se iniciará un asistente de cifrado si dispone de una directiva File Encryption.
- **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 los archivos seleccionados.

  Nota: no es posible descifrar archivos que corresponden a la directiva File Encryption.

- **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.

- **Crear nueva clave**: abre un cuadro de diálogo para crear claves locales definidas por el usuario.
- **Reactivar cifrado**: el responsable de seguridad puede permitir al usuario decidir si se deben cifrar archivos en medios extraíbles. Al conectar un medio extraíble, se le preguntará si desea cifrar los archivos en dicho medio. Además, el responsable de seguridad puede permitir que la decisión se recuerde para dicho medio. En ese caso, podrá seleccionar la opción **Recordar y no mostrar de nuevo**; el cuadro de diálogo no se volverá a mostrar para el medio en cuestión. Si lo hace, en el Explorador de Windows dispondrá de la opción **Reactivar cifrado** en el menú contextual de dicho medio. Utilice este comando si cambia de opinión. Si no es posible, por ejemplo si no dispone de los derechos necesarios, se mostrará un mensaje de error. A continuación, tendrá que tomar la decisión de nuevo.

13.1.1 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 de SafeGuard Data Exchange o SafeGuard Cloud Storage.

Puede definir la clave predeterminada de cifrado desde el menú contextual

- de un archivo en una unidad extraíble
- de una unidad extraíble
- de una carpeta o subcarpeta de sincronización de Cloud Storage
- de un archivo en una carpeta o subcarpeta de sincronización de Cloud Storage
- Además, puede definir una clave como la predeterminada inmediatamente después de crear una nueva clave local en el cuadro de diálogo **Crear clave**.

Para definir la clave predeterminada:

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

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

Nota: si utiliza una clave local para el cifrado de Cloud Storage, SafeGuard Portable se copiará en la carpeta de sincronización de Cloud Storage.

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

13.1.2 Importar claves desde un archivo

Si recibe alguna unidad extraíble o desea acceder a una unidad compartida 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.

1. Seleccione el archivo pertinente en el dispositivo extraíble y haga clic en **Cifrado de archivos > Importar clave desde archivo**.
2. Introduzca la frase de acceso.

La clave se importará y tendrá acceso al archivo.

13.2 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. Si se muestra el símbolo de una llave verde, significa que tiene las claves necesarias y puede acceder al volumen.

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.

Agregar o quitar claves

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

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

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

Con la opción **Quitar clave** puede eliminar claves que se utilizan para acceder al medio.

14 Opciones de recuperación

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

- **Recuperación de inicio de sesión con Local Self Help** (disponible para POA de SafeGuard solamente)

  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 de SafeGuard.

  Para más información, consulte el apartado Recuperación mediante Local Self Help en la página 64.

- **Recuperación con desafío/respuesta o clave de recuperación de BitLocker**

  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 equipo.

  En las estaciones de trabajo que no son compatibles con desafío/respuesta se proporcionan claves de recuperación. Este es el procedimiento estándar de Microsoft. Durante la recuperación, usted proporciona el nombre del equipo al responsable del centro de ayuda, quien a su vez le proporciona la clave de recuperación que necesita para iniciar el equipo.

  Para más información, consulte Recuperación con desafío/respuesta o clave de recuperación en la página 73.

El responsable de seguridad define, mediante directivas, todas las opciones de recuperación disponibles en los equipos.

15 Recuperación mediante Local Self Help

Nota: local Self Help únicamente está disponible para estaciones de trabajo con Windows 7 con SafeGuard Power-on Authentication (POA).

Si ha olvidado la contraseña, Local Self Help le permite acceder al equipo sin la asistencia del centro de ayuda.

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 de SafeGuard (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 SafeGuard Enterprise.

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 de usuario.

15.1 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 de SafeGuard (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 o el número de preguntas predefinidas respondidas).

4. Haga clic en **Next**.

   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 de SafeGuard (power-on authentication), deberá escribir las respuestas de la misma manera. Por ejemplo, se distingue entre mayúsculas y minúsculas.

   Nota: la POA de SafeGuard no puede manejar todos los caracteres que pueden introducirse en Windows, por ejemplo, no se pueden utilizar caracteres hebreos o árabes. 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 de SafeGuard.

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 de SafeGuard (power-on authentication), deberá escribir las respuestas de la misma manera. Por ejemplo, se distingue entre mayúsculas y minúsculas.

Nota:

La POA de SafeGuard no puede manejar todos los caracteres que pueden introducirse en Windows, por ejemplo, no se pueden utilizar caracteres hebreos o árabes. 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 de SafeGuard.

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 **Finish**.

   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 de SafeGuard (power-on authentication).

15.2 Activar de Local Self Help - recordatorio

Es esencial que active Local Self Help. Por este motivo, SafeGuard Enterprise le recordará que se inscriba en Local Self Help.

SafeGuard Enterprise le recordará que configure sus preguntas de Local Self Help en tres fases:

- **Fase 1**

  Aparecerá un mensaje emergente cada hora durante un día indicando que es necesario configurar Local Self Help. Al siguiente día, se inicia la fase 2.

- **Fase 2**

  Además del comportamiento de la fase 1, se iniciará el Asistente de Local Self Help cada vez que inicie sesión o desbloquee el equipo. Puede posponer ejecutar el asistente. Después de 3 días, se inicia la fase 3.

- **Fase 3**

  Además del comportamiento de la fase 2, pero sin el mensaje emergente, el Asistente de Local Self Help se iniciará cada 60 minutos.

Se notifica inmediatamente al usuario mediante un globo con sugerencias y se introduce la fase 1 cuando Local Self Help tiene que ser reactivado debido a cambios en uno de los siguientes:

- parámetros de Local Self Help
- la contraseña de Windows
- certificado

15.3 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 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 **Next**. Si ha recibido y respondido varias preguntas predefinidas, aparecerá el cuadro de diálogo de preguntas predefinidas, en el que se muestran las preguntas contestadas.

   a) Si ha recibido diferentes temas de preguntas, seleccione el tema en la lista desplegable **Tema**.

   b) 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.

   c) Para que se muestre el texto introducido, active la opción **Mostrar respuestas**.

   d) Para cambiar las respuestas, haga clic en las preguntas pertinentes y escriba la nueva respuesta en la columna **Respuestas**.

5. Haga clic en **Next**. 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.

   a) Para que se muestre el texto introducido, active la opción **Mostrar respuestas**.

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

   c) 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**.

d) Para eliminar una pregunta, selecciónela y haga clic en **Eliminar pregunta**.

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

6. Haga clic en **Next**.

   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.

7. Haga clic en **Finish**.

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

8. Haga clic en **Aceptar**.

   Las modificaciones entran en vigor.

La próxima vez que inicie Local Self Help en la POA de SafeGuard (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. Sin embargo, en este caso puede volver a activar Local Self Help.

15.4 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 de SafeGuard para iniciar la sesión con Local Self Help. Las preguntas que aparecen en la POA de SafeGuard se seleccionan de forma aleatoria de entre las preguntas que ha respondido en el asistente de Local Self Help.

Si estos parámetros cambian, debido a la imposición de una directiva nueva, 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	Se indicará al usuario que ha cambiado la configuración de Local Self Help. Las preguntas	Utilice el asistente de Local Self Help para volver a activarlo.

Condición	Acción de LSH	Acción del usuario
necesario para utilizar Local Self Help.	disponibles no son válidas. Local Self Help ya no estará activo en su equipo.	
El número de preguntas que debe responder en la POA de SafeGuard para iniciar la sesión con Local Self Help ha cambiado.	Se indicará al usuario que ha cambiado la configuración de Local Self Help. Las preguntas disponibles siguen siendo válidas. Cambia el índice de preguntas disponibles y respuestas.	Siga las instrucciones del asistente de Local Self Help.

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

Los parámetros de Local Self Help, y otras condiciones necesarias para su uso, podrían cambiar mientras se están definiendo las preguntas en el asistente de Local Self Help.

Por ejemplo:

- Si se establece una contraseña nueva o se cambia el certificado.
- Si se aplica una nueva política de Local Self Help y/o nuevas preguntas de forma centralizada.

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	Resultado
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 definirlas o el número de 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.
▪ Se ha cambiado la contraseña	El asistente de Local Self Help informa al usuario. 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

Condición	Acción	Resultado
y/o ▪ Una nueva directiva ha cambiado los parámetros de Local Self Help (por ejemplo, la longitud de las preguntas, el permiso para definirlas o el número de las mismas). Local Self Help sigue activo. Las preguntas y respuestas definidas no son válidas y no existen suficientes preguntas para mantener Local Self Help activo.		preguntas y respuestas necesarias. Local Self Help estará disponible cuando complete el asistente.
El certificado del usuario ha cambiado.	El asistente de Local Self Help informa al usuario. 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.

15.6 Iniciar la sesión en la POA de SafeGuard mediante Local Self Help

1. En la POA de SafeGuard, 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 de SafeGuard con token o smartcard, primero deberá retirar el token/smartcard. Aparecerá la POA de SafeGuard para iniciar la sesión con el nombre de usuario y la contraseña. Introduzca la identificación de usuario y haga clic en **Recuperación**.

   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 de SafeGuard (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 de SafeGuard y en Windows

15.7 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.

15.8 Reactivar las preguntas y respuestas tras el cambio de contraseña en diferentes equipos

Si utiliza distintos equipos con Local Self Help y cambia la contraseña de Windows en uno de ellos, ya no podrá utilizar las preguntas y respuestas de Local Self Help en los otros equipos. Sin embargo, las preguntas y respuestas seguirán disponibles en el asistente de Local Self Help. Para poder utilizar las preguntas de nuevo en otros equipos, debe confirmarlo en el asistente de Local Self Help.

1. Tras cambiar la contraseña en un equipo, inicie la sesión en otro equipo.

   Se le indicará que hay preguntas de Local Self Help sin responder.

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

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

3. Introduzca la contraseña y haga clic en **Siguiente**.
4. Haga clic en **Siguiente** en cada página del asistente y haga clic en **Finalizar** al concluir.

Las preguntas y respuestas almacenadas anteriormente en el equipo estarán activas de nuevo y se pueden utilizan para iniciar la sesión en la POA de SafeGuard a través de Local Self Help.

16 Recuperación con desafío/respuesta o clave de recuperación

Si utiliza SafeGuard Enterprise y, por ejemplo, ha olvidado la contraseña, puede volver a tener acceso rápidamente a su equipo con la asistencia del centro de ayuda central.

Nota: si utiliza Windows 7 y la POA de SafeGuard, le recomendamos que utilice Local Self Help para recuperar una contraseña olvidada. Puede visualizar la contraseña actual en Local Self Help y continuar usándola, así no hay necesidad de restablecer la contraseña o involucrar al centro de ayuda.

16.1 Desafío/respuesta para usuarios de POA de SafeGuard

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

Durante el procedimiento de desafío/respuesta, se genera un código de desafío (una cadena de caracteres ASCII) que debe proporcionar al oficial 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 el procedimiento de desafío/respuesta 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

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

- Ha olvidado la contraseña.
- Ha escrito una contraseña incorrecta demasiadas veces en la POA de SafeGuard. El ordenador se ha bloqueado.
- Ha olvidado o perdido el token/la tarjeta inteligente.
- La caché local de la POA de SafeGuard está parcialmente dañada.
- Otro usuario tiene que iniciar el equipo protegido con SafeGuard Enterprise.

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

- **Arrancar el cliente de SafeGuard Enterprise sin sesión de usuario:**

  Arrancar el equipo sin sesión de usuario puede ayudar si ha introducido incorrectamente la contraseña (por ejemplo, debido a errores de escritura, a que la tecla Bloq Mayús estaba

activada, etc.) y, sin embargo, conoce la contraseña correcta. El procedimiento de desafío/respuesta le permitirá iniciar la sesión sin restablecer la contraseña.

Si ha escrito varias veces la contraseña incorrecta, el centro de ayuda generará automáticamente un código de respuesta para arrancar el cliente sin sesión de usuario. El requisito en este caso se incluye en el desafío. Después, podrá volver a iniciar la sesión con su nombre de usuario y contraseña.

- **Arrancar el cliente de SafeGuard Enterprise con sesión de usuario:**

  Si ha olvidado la contraseña, no intente hacer pruebas, solicite un desafío directamente. El centro de ayuda generará una respuesta para iniciar la sesión con o sin nombre de usuario. Si inicia la sesión con el nombre de usuario, pida al centro de ayuda que se muestre la contraseña antigua durante el procedimiento de desafío/respuesta. De esta forma se ahorra tener que cambiar la contraseña. De lo contrario, al iniciar la sesión con el nombre de usuario, tendrá que cambiar la contraseña en Windows durante el procedimiento de desafío/respuesta.

  Nota: para los usuarios que trabajan sin conexión, es decir, sin estar conectados al controlador de dominio, hay que tener en cuenta algunas consideraciones especiales, consulte Desafío/respuesta para los usuarios sin conexión en la página 77.

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

  Este procedimiento es necesario si la caché de directivas de SafeGuard sufre daños. La caché local se utiliza para almacenar todas las claves, directivas, certificados y otros archivos de control. La recuperación del inicio de sesión se desactiva, de forma predeterminada, cuando la memoria caché local presenta daños, es decir 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.

16.1.3 Procedimiento de desafío/respuesta

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

   Nota: cuando se genera el desafío, hay disponible un período de tiempo de 30 minutos para introducir la respuesta que ha generado el centro de ayuda en un procedimiento de desafío/respuesta. A los 30 minutos, el código de respuesta deja de ser válido y no se puede utilizar.

2. Solicitud de un desafío:

   Abra el cuadro **Desafío** en la POA de SafeGuard. Se generará un código de desafío en forma de cadena de caracteres ASCII.

3. Póngase en contacto con el centro de ayuda.

   Indique los datos (identificación de usuario, identificación del equipo, etc.) que aparecen en el cuadro de **Desafío** y el código de desafío.

4. El centro de ayuda generará un código de respuesta a través de SafeGuard Management Center.
5. El responsable del centro de ayuda le proporcionará la respuesta por teléfono o con un mensaje al móvil.

6. Escriba el código de respuesta en la POA de SafeGuard.

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

Ya puede retomar el trabajo.

16.1.4 Solicitar desafío

1. En el cuadro de inicio de sesión de la POA (power-on authentication) de SafeGuard, haga clic en **Recuperación**.

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

   Nota: si ha introducido una contraseña o número PIN incorrectos demasiadas veces, o bien si la caché de directivas tiene daños, SafeGuard Enterprise le informará y se ofrecerá un procedimiento de desafío/respuesta.

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

2. Llame al centro de ayuda de SafeGuard Enterprise y proporcione los datos de usuario y el código de desafío.

   Si necesita ayuda para ver cuál es el código de desafío, puede hacer clic en el botón **Ayuda de deletreo**.

   El responsable en el centro de ayuda podrá identificar el escenario mediante el código de desafío.

3. Haga clic en **Siguiente**.

16.1.5 Introducir la respuesta

1. Introduzca el código de respuesta que le ha proporcionado el responsable del centro de ayuda en el cuadro de diálogo de **Respuesta** y haga clic en **Aceptar**.

   Si introduce incorrectamente el código de respuesta, se indicará en color rojo el grupo de caracteres que contenga el error.

2. Inicia la sesión en la POA de SafeGuard.

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

16.1.6 Recomendación

16.1.6.1 Ha escrito una contraseña incorrecta demasiadas veces

Ha introducido incorrectamente la contraseña en la POA de SafeGuard (por ejemplo, debido a errores de escritura, a que la tecla Bloq mayús estaba activada, etc.) y, sin embargo, conoce la contraseña correcta. Está conectado al dominio.

1. El ordenador está bloqueado. Se solicita que inicie un procedimiento de desafío/respuesta para desbloquearlo.

2. El responsable del centro de ayuda genera una respuesta para arrancar sin credenciales.

   De esta forma no tendrá que cambiar la contraseña para iniciar la sesión en Windows.

3. Aparecerá el cuadro de diálogo de inicio de sesión de Windows. Introduzca la contraseña de Windows.

   Se inicia la sesión.

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

   Nota: también puede solicitar una respuesta con credenciales. En este caso, tendrá que cambiar las credenciales de Windows al iniciar la sesión.

16.1.6.2 Ha olvidado la contraseña

Si ha olvidado la contraseña, puede seguir los siguientes métodos de recuperación, que evitan que la contraseña se restablezca de forma centralizada:

- Mediante Local Self Help. Local Self Help permite mostrar la contraseña actual sin tener que contactar con centro de asistentcia.

- Mediante el procedimiento de desafío/respuesta: Pida al centro de ayuda que se genere una respuesta al iniciar la sesión y que se muestre la contraseña. De esta forma se ahorra tener que cambiarla. Si lo desea, una vez iniciada la sesión puede cambiar la contraseña.

Como método alternativo:

1. Si ha olvidado la contraseña, recibirá una respuesta para iniciar la sesión. En ese caso, tendrá que cambiar la contraseña al iniciar la sesión en Windows (si está conectado al dominio).
2. Después de cambiar la contraseña, utilícela para iniciar la sesión en la POA.

16.1.6.3 Ha olvidado o perdido el token

En este caso, se tiene que llevar a cabo el procedimiento de desafío/respuesta durante el inicio de sesión del usuario.

1. Durante el procedimiento de desafío/respuesta, se le solicitará que cambie la contraseña.

   Nota: el cuadro de diálogo para cambiar la contraseña sólo aparece si está conectado al controlador del dominio.

2. Si es obligatorio el inicio de sesión con un token y el PIN, puede omitir el cambio de contraseña haciendo clic en **Cancelar**.

   - **Ha olvidado el token**

     Omitir el cambio de contraseña haciendo clic en **Cancelar** sólo tiene sentido si ha olvidado su token pero lo seguirá utilizando en el futuro. Tras hacer clic en **Cancelar**, se iniciará la sesión y podrá seguir usando el equipo.

     Sin token, sólo puede iniciar la sesión mediante el procedimiento de desafío/respuesta en la POA de SafeGuard (power-on authentication). Una vez que vuelva a tener su token, podrá conectarse con él a la POA de SafeGuard.

- **Ha perdido el token**

  Si ha perdido el token, especifique una contraseña nueva. Se iniciará la sesión de Windows con esta contraseña. Si las directivas de seguridad se lo permiten (es decir, no es obligatorio el uso del token), también puede iniciar la sesión en la POA de SafeGuard con esta contraseña.

  El uso no autorizado del token por parte de cualquiera que lo encuentre se puede descartar. Los usuarios no autorizados no pueden utilizar el token para iniciar la sesión, aunque conozcan el número PIN, ya que la contraseña ha cambiado.

16.1.6.4 Ha olvidado el número PIN

1. Si ha olvidado el número PIN del token, solicite una respuesta e introduzca la contraseña nueva. Se iniciará la sesión de Windows con esta contraseña. También puede utilizar esta contraseña en la POA de SafeGuard (power-on authentication) si se permite el uso de credenciales.
2. El responsable de seguridad debe asignar un número PIN nuevo al token y almacenar las credenciales. A continuación, podrá utilizarlo de nuevo para iniciar la sesión.

16.1.6.5 Ya no puede acceder a su equipo

Si ya no le es posible acceder al equipo, tal vez se deba a que la POA de SafeGuard (power-on authentication) esté dañada. Incluso en esta situación tan preocupante, SafeGuard Enterprise 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 SafeGuard Enterprise. La persona responsable del centro de ayuda le proporcionará los archivos necesarios y le guiará por los pasos necesarios para conseguir acceder de nuevo a su equipo.

16.1.7 Desafío/respuesta para usuarios sin conexión

Deben tenerse en cuenta algunas consideraciones especiales al utilizar el procedimiento de desafío/respuesta para usuarios sin conexión. Los usuarios sin conexión (es decir, los que no están conectados al controlador del dominio, por ejemplo usuarios de portátiles fuera de la oficina) no pueden iniciar un cambio de contraseña automático durante el procedimiento de desafío/respuesta.

16.1.7.1 Desafío/respuesta para usuarios sin conexión con inicio de sesión mediante nombre de usuario/contraseña

Ejemplo:

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

SafeGuard Enterprise también puede iniciar la sesión en Windows durante el procedimiento de desafío/respuesta. Sin embargo, como después de este procedimiento no conocería la contraseña, tendría que repetirlo cada vez que iniciase el equipo. Además, no podrá desbloquear el equipo (por ejemplo, si se bloquea al activarse el protector de pantalla). En ese caso, tendría que reiniciar el equipo, lo que supondría el peligro de pérdida de datos, y volver a iniciar un procedimiento de desafío/respuesta.

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

Proceda de la siguiente forma:

1. Para iniciar el procedimiento de desafío/respuesta, haga clic en **Recuperación** en la POA de SafeGuard.
2. Llame al centro de ayuda e indique el código de desafío.
3. Pida que se pueda iniciar la sesión mediante credenciales y que desea ver su contraseña.
4. Haga clic en **Siguiente** en el cuadro de desafío/respuesta e introduzca la respuesta.
5. Haga clic en **Aceptar**.

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

6. Responda **Sí** y haga clic en **Aceptar**.
7. A continuación se informa de que la contraseña se mostrará cuando pulse **Intro** o la **barra espaciadora**, o bien cuando haga clic en el texto.

   Nota: No haga clic en **Aceptar**. Si hace clic en **Aceptar**, el proceso de arranque continuará SIN mostrar la contraseña.

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

8. Pulse **Intro** o la **barra espaciadora**, o bien haga clic en el texto.

   Se mostrará la contraseña.

   Nota: asegúrese de que nadie pueda ver el contenido de la pantalla. Puede ocultar la contraseña pulsando la **barra espaciadora**, **Intro** o haciendo clic en el cuadro azul. La contraseña sólo se mostrará durante un máximo de cinco segundos.

9. Puede utilizar esta contraseña para iniciar la sesión en la POA de SafeGuard (power-on authentication) y en Windows.

   Ya puede volver a trabajar con el equipo.

16.1.7.2 Desafío/respuesta para usuarios sin conexión con inicio de sesión "Sólo token"

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

- Conoce las credenciales de Windows

  a) Si conoce las credenciales de Windows, inicie el procedimiento de desafío/respuesta tal como se ha descrito. Se inicia la sesión en Windows.

  El modo de inicio de sesión **Sólo token** se desactiva durante el tiempo que dure la sesión de trabajo después del procedimiento de desafío/respuesta. Por consiguiente, también podrá iniciar la sesión en Windows con el nombre de usuario y la contraseña.

  En el caso de que deba bloquearse el equipo, podrá desbloquearlo especificando la contraseña de Windows. El inicio de sesión en la POA de SafeGuard (power-on authentication) sólo será posible a través del procedimiento de desafío/respuesta.

- No conoce las credenciales de Windows

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

  b) Indique al responsable del centro de ayuda que se debe mostrar la contraseña.

  Como el modo de inicio de sesión **Sólo token** se desactiva, también puede utilizar esta contraseña para desbloquear el equipo. Sin embargo, el inicio de sesión en la POA de SafeGuard (power-on authentication) sólo será posible a través del procedimiento de desafío/respuesta.

16.2 Desafío/respuesta para usuarios de BitLocker

Consejos generales para usar el ratón y/o el teclado

- Los controles también se puede seleccionar con el ratón y/o el teclado Para cambiar de un control a otro con el teclado se debe pulsar la tecla **Tab**. Para volver al control anterior se debe pulsar la combinación de teclas **Shift+Tab**.
- Para confirmar la selección realizada pulse la tecla **Intro**.

Procedimiento Desafío/Respuesta

Siga estos pasos si necesita una clave de recuperación de BitLocker:

1. Reinicie el equipo. Tras reiniciar el equipo aparecerá un mensaje amarillo. Pulse una tecla cualquiera antes de tres segundos.
2. Aparece la pantalla de desafío/respuesta de Sophos.
3. En el paso 2 se proporciona información para llamar al centro de ayuda.
4. Proporcione la información siguiente al centro de ayuda:

   Equipo, por ejemplo, Sophos\<nombre del equipo>

   Código de **desafío**, por ejemplo, ABC12-3DEF4-56GHO-892UT-Z654K-LM321. Pase el ratón por los caracteres para mostrar la ayuda de deletreo. O pulse **F1** varias veces para abrir el cuadro de ayuda. El código caduca en 30 minutos, provocando el apagado automático del ordenador.

5. A continuación, introduzca el **código de respuesta** proporcionado por el centro de ayuda (seis bloques con dos campos de texto cada uno y cinco caracteres necesarios por campo).
   - Al rellenar un campo de texto con todos los caracteres, el sistema pasa automáticamente al siguiente.
   - Si introduce un carácter erróneo por equivocación, el bloque se marcará en rojo. Utilice las teclas **Suprimir** o **Retroceso** para corregir los datos introducidos.
6. Una vez haya introducido correctamente el código de respuesta, haga clic en **Continuar** o pulsar **Intro** para completar la desafío/respuesta.

Restablecer credenciales de BitLocker

Tan pronto como haya iniciado sesión en el sistema de nuevo, especifique las nuevas credenciales de BitLocker de manera que no sea necesario ningún otro procedimiento de desafío/respuesta para su próximo inicio de sesión. Dependiendo de su sistema operativo y

la versión del BIOS/UEFI, el sistema mostrará un cuadro de diálogo para restablecer las credenciales.

Si este cuadro de diálogo no aparece automáticamente, haga clic en el icono de SafeGuard Enterprise situado en la barra de tareas. Se abrirá un menú contextual. Seleccione **Restablecer credenciales de BitLocker** y siga las instrucciones en pantalla.

Nota:

Si desea apagar o reiniciar el equipo, haga clic con el ratón en el botón de apagado o pulse la tecla **Tab** hasta que aparezca resaltado el botón de apagado:

16.3 Clave de recuperación de BitLocker

Como usuario BitLocker en un sistema no compatible con el procedimiento de desafío/respuesta de SafeGuard, puede solicitar una clave de recuperación a su centro de ayuda.

Consejos generales para usar el ratón y/o el teclado

- Los controles también se puede seleccionar con el ratón y/o el teclado Para cambiar de un control a otro con el teclado se debe pulsar la tecla **Tab**. Para volver al control anterior se debe pulsar la combinación de teclas **Shift+Tab**.
- Para confirmar la selección realizada pulse la tecla **Intro**.

Solicite la clave de recuperación

Siga los pasos siguientes si necesita que su centro de ayuda le proporcione una clave de recuperación para BitLocker:

1. Reiniciar la estación de trabajo. Después de reiniciar, presione la tecla **Esc** en la pantalla de inicio de sesión de BitLocker.
2. Aparecerá la pantalla para introducir la clave de recuperación de BitLocker.
3. En el paso 2 se proporciona información para llamar al centro de ayuda.

   Por ejemplo: <Nombre del ordenador> C: 9/25/2014

4. Proporcione el **Nombre de equipo** al centro de ayuda.
5. A continuación introduzca la **clave de recuperación de BitLocker** proporcionada por el centro de ayuda (ocho bloques de seis caracteres por cada campo).
6. Una vez haya introducido correctamente el código de respuesta, haga clic en **Continuar** o pulsar **Intro** para completar la recuperación.

Restablecer credenciales de BitLocker

Tan pronto como haya iniciado sesión en el sistema de nuevo, especifique las nuevas credenciales de BitLocker de manera que no sea necesario ningún otro procedimiento de desafío/respuesta para su próximo inicio de sesión. Dependiendo de su sistema operativo y la versión del BIOS/UEFI, el sistema mostrará un cuadro de diálogo para restablecer las credenciales.

Si este cuadro de diálogo no aparece automáticamente, haga clic en el icono de SafeGuard Enterprise situado en la barra de tareas. Se abrirá un menú contextual. Seleccione **Restablecer credenciales de BitLocker** y siga las instrucciones en pantalla.

Nota:

Si desea apagar o reiniciar el equipo, haga clic con el ratón en el botón de apagado o pulse la tecla **Tab** hasta que aparezca resaltado el botón de apagado:

17 SafeGuard Enterprise y Lenovo Rescue and Recovery

Nota: Lenovo Rescue and Recovery solo está disponible en equipos con Windows 7.

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

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

Lenovo Rescue and Recovery resulta especialmente útil para los usuarios que no dispongan de la ayuda de un administrador. Por ejemplo, en un viaje de negocios, los usuarios pueden restaurar sus equipos con Lenovo Rescue and Recovery.

Para más información sobre las versiones de Lenovo Rescue and Recovery (RnR) compatibles con SafeGuard Enterprise, consulte http://www.sophos.com/es-es/support/knowledgebase/108383.aspx

17.1 Introducción

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

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

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

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

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

17.2 Requisitos

- La BIOS más reciente para el ordenador

- Para obtener información sobre las versiones de Lenovo Rescue and Recovery compatibles con SafeGuard Enterprise, consulte el artículo de la base de conocimiento http://www.sophos.com/es-es/support/knowledgebase/108383.aspx
- Lenovo Rescue and Recovery se puede utilizar para recuperar volúmenes cifrados con SafeGuard Enterprise. 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.

17.3 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 SafeGuard Enterprise. Se recomienda instalar la función Rescue and Recovery de Lenovo en primer lugar y después SafeGuard Enterprise.

17.3.1 Instalar Rescue and Recovery y SafeGuard Enterprise

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

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

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

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

   La POA de SafeGuard se activa durante la instalación de SafeGuard Enterprise.

17.3.2 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 Device Encryption de SafeGuard Enterprise (SGNClient.msi).

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

17.4 Actualización

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

Actualizar SafeGuard Enterprise

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

17.5 Desinstalación

Al desinstalar los productos:

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

17.6 Opciones de recuperación y entorno de arranque

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

Desde el disco duro local

- La partición virtual en el disco duro local o la partición de servicio local.
- Los volúmenes deben estar cifrados en SafeGuard Enterprise con la clave definida para el 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: SafeGuard Enterprise 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 de SafeGuard, 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. SafeGuard Enterprise se eliminará durante el proceso de restauración. Para volver a proteger el sistema, se debe volver a instalar SafeGuard Enterprise.

17.7 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, y en los que instalará SafeGuard Enterprise más adelante, se muestra un mensaje que pide al usuario que cree una copia de seguridad nueva del sistema.

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

SafeGuard Enterprise sólo admite guardar copias de seguridad en:

- el disco duro local
- un segundo disco duro
- un disco duro USB
- la red
- clave de inicio
- 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.

17.8 Restaurar copias de seguridad de archivos

Rescue and Recovery puede restaurar archivos o carpetas de copias de seguridad en las que está instalado SafeGuard Enterprise. 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.

17.9 Restaurar el sistema de SafeGuard Enterprise

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

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

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

      Se muestra la POA de SafeGuard.

   b) Introduzca las credenciales de SafeGuard Enterprise.

2. Si no utiliza un equipo Lenovo:
   a) Inicie la sesión en la POA de SafeGuard con sus credenciales de SafeGuard Enterprise.
   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 en el que podrá seleccionar la copia de seguridad.
5. Selecciónela y restáurela.

17.10 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 SafeGuard Enterprise. Si desea obtener más información, consulte la documentación de Lenovo.

17.11 POA de SafeGuard deshabilitada y Lenovo Rescue and Recovery

Si la POA de SafeGuard 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.

18 Soporte técnico

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

- Visitar el foro SophosTalk en community.sophos.com/ para consultar casos similares.
- Visitar la base de conocimiento de Sophos en www.sophos.com/es-es/support.aspx/.
- Descargar la documentación correspondiente desde www.sophos.com/es-es/support/documentation/.
- Abrir un ticket de incidencia con nuestro equipo de soporte en https://secure2.sophos.com/support/contact-support/support-query.aspx.

19 Aviso legal