SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise

Ayuda de usuario

Versión del producto: 8.3

Contenido

Acerca de SafeGuard Enterprise 1
Módulos 2
- Cifrado completo de discos con BitLocker 2
- SafeGuard File Encryption (basado en aplicación) 2
- SafeGuard File Encryption (basado en ubicación) 3
- SafeGuard Cloud Storage 3
- SafeGuard Data Exchange 4

Bandeja del sistema de Sophos SafeGuard 7
Cómo 10
- Cifrar un ordenador con BitLocker 10
- Restablecer una contraseña o un PIN de BitLocker olvidado 11
- Restablecer una contraseña o un PIN de BitLocker olvidado con Desafío/Respuesta 12
- Cifrar todos los archivos según la política 12
- Cifrar/Descifrar archivos de forma manual 13
- Ver dónde se cifran los archivos 14
- Usar una contraseña para proteger un archivo 14
- Enviar archivos cifrados por correo electrónico 15
- Crear una clave local 17
- Intercambiar datos con SafeGuard Data Exchange 18
- Intercambiar datos en la nube sin SafeGuard Enterprise 21
- Usar claves predeterminadas 22
- Recuperar archivos cifrados 23
- Comprobar la conexión con el servidor de SafeGuard Enterprise 23
- Editar archivos con SafeGuard Portable 24

Soporte 26
Aviso legal 27

1 Acerca de SafeGuard Enterprise

Sophos SafeGuard se ejecuta en estaciones de trabajo Windows para protegerlas. Consta de varios módulos.

Es posible que no disponga de todas las funciones descritas en esta ayuda. Esto depende de la licencia que tenga y de las políticas que haya recibido de su responsable de seguridad.

Sophos SafeGuard se configura y administra de forma centralizada desde Sophos SafeGuard Management Center.

Para acceder a información general sobre su instalación de Sophos SafeGuard, haga clic en el icono de Sophos SafeGuard de la Bandeja del sistema de Sophos SafeGuard (página 7).

Las opciones más importantes para cifrar y descifrar archivos están disponibles en un menú contextual en el Explorador de Windows.

Este documento se refiere únicamente a las estaciones Windows. Para estaciones de trabajo Mac, consulte la Ayuda de usuario de Mac de SafeGuard Enterprise.

Módulos:

Cifrado de discos

- **Cifrado completo de discos con BitLocker (página 2)**

Synchronized Encryption

- **SafeGuard File Encryption (basado en aplicación) (página 2)**

Cifrado de archivos

- **SafeGuard File Encryption (basado en ubicación) (página 3)**
- **SafeGuard Cloud Storage (página 3)**
- **SafeGuard Data Exchange (página 4)**

2 Módulos

2.1 Cifrado completo de discos con BitLocker

El cifrado completo de discos con BitLocker parte de la tecnología de Cifrado de unidad BitLocker incluida en su sistema operativo. Cifra todo el disco duro para que los datos estén protegidos incluso en caso de pérdida o robo del ordenador.

Cuando inicie sesión en su estación de trabajo, deberá introducir las credenciales de usuario para desbloquear BitLocker. Para obtener más información, consulte Cifrar un ordenador con BitLocker (página 10).

Sophos SafeGuard le permite gestionar BitLocker en estaciones de trabajo con uno de los siguientes sistemas operativos:

- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise

2.2 SafeGuard File Encryption (basado en aplicación)

El cifrado de archivos basado en la aplicación cifra los archivos creados o modificados con aplicaciones específicas (por ejemplo, Microsoft Word). Una política define una lista de aplicaciones para las que el cifrado de archivos se ejecuta automáticamente. Este cifrado es persistente, por lo que su archivo está seguro aunque lo mueva a otra ubicación, lo cargue a un proveedor de almacenamiento en la nube o lo envíe por correo electrónico.

Si su responsable de seguridad ha especificado Microsoft Word como una aplicación para la que el cifrado de archivos está activo, cada archivo que cree o guarde con Microsoft Word se cifrará con una clave definida. Cualquier usuario que tenga esta clave en su conjunto de claves podrá acceder a su archivo.

- Los archivos nuevos creados con apps definidas o extensiones de archivos se cifran automáticamente.
- 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 leer su contenido.
- Si accede a un archivo cifrado desde un ordenador en que File Encryption no está instalado, no podrá leer su contenido.
- Los archivos que se copian o mueven desde una carpeta sin cifrar a una carpeta en la que se aplican reglas de cifrado se cifrarán.
- Los archivos que se copian o mueven desde una carpeta cifrada a una carpeta sin cifrar se descifrarán.
- Los archivos que se copian o mueven desde una carpeta cifrada a una carpeta con una regla de cifrado distinta se cifrarán de acuerdo con la regla de la carpeta de destino.
- Los archivos creados por aplicaciones para las que File Encryption no está activo pero para las que existe una regla de cifrado para la extensión de archivo, se cifrarán pero no se podrán abrir

con la aplicación que ha creado el archivo. Por ejemplo, si crea un archivo .doc con OpenOffice y OpenOffice no está especificado en **Listas de aplicaciones**.

Importante
Si se interrumpe el proceso de copia o mover archivos, por ejemplo, debido a un reinicio, la operación no se reanudará automáticamente. Esto puede tener como resultado que queden archivos sin cifrar de forma no intencionada. Para asegurarse de que los archivos se cifran siempre correctamente, consulte Cifrar todos los archivos según la política (página 12).

Para saber qué ubicaciones de un ordenador están cifradas, consulte Ver dónde se cifran los archivos (página 14).

Para conocer el estado de cifrado de uno o más archivos, haga clic con el botón derecho en los archivos y seleccione **SafeGuard File Encryption > Mostrar estado de cifrado**.

En Windows Explorer, los archivos cifrados están marcados con un símbolo de candado de color verde. Si el símbolo del candado no se muestra aunque el archivo esté cifrado, consulte el artículo de la base de conocimiento de Sophos 108784.

2.3 SafeGuard File Encryption (basado en ubicación)

El cifrado de archivos basado en la ubicación permite al responsable de seguridad definir las ubicaciones en las que se cifran los archivos, por ejemplo, **Documentos**.

Tras asignar a su ordenador una política de **File Encryption** del tipo **Basada en la ubicación**, los archivos en las ubicaciones especificadas por dicha política se cifrarán de forma transparente sin la intervención del usuario:

- Los archivos nuevos de una ubicación especificada para el cifrado se cifran automáticamente.
- 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 leer su contenido.
- Si accede a un archivo cifrado desde un ordenador en que File Encryption no está instalado, no podrá leer su contenido.

Para saber qué ubicaciones de su ordenador están cifradas, consulte Ver dónde se cifran los archivos (página 14).

Para conocer el estado de cifrado de uno o más archivos, haga clic con el botón derecho en los archivos y seleccione **SafeGuard File Encryption > Mostrar estado de cifrado**.

En Windows Explorer, los archivos cifrados están marcados con un símbolo de candado de color verde. Si el símbolo del candado no se muestra aunque el archivo esté cifrado, consulte el artículo de la base de conocimiento de Sophos 108784.

2.4 SafeGuard Cloud Storage

SafeGuard Cloud Storage ofrece cifrado basado en la ubicación para archivos almacenados en la nube. No afecta al modo en que trabaja con sus archivos, pero garantiza que las copias locales de sus datos almacenados en la nube se cifren de forma transparente y permanezcan cifrados al almacenarse en la nube.

SafeGuard Cloud Storage detecta automáticamente su proveedor de almacenamiento en la nube (si se admite) y aplica la política de cifrado a la carpeta de sincronización.

SafeGuard Cloud Storage no realiza un cifrado inicial de los archivos en la nube. Los archivos que se hayan guardado antes de que SafeGuard Cloud Storage se instalara o activara mediante una política permanecerán sin cifrar. Si desea cifrar estos archivos, primero debe quitarlos de la nube y luego volver a añadirlos.

Nota
No arrastre y suelte archivos en el icono de Dropbox del escritorio de Windows para añadirlos a la carpeta de Dropbox. Estos archivos se copiarán en la carpeta de Dropbox sin cifrar. Para asegurarse de que los archivos se cifran, cópielos directamente en su 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.

2.5 SafeGuard Data Exchange

SafeGuard Data Exchange ofrece cifrado basado en la ubicación para archivos almacenados en medios extraíbles para que pueda intercambiarlos con otros usuarios. Sólo los usuarios que dispongan de las claves apropiadas podrán acceder al contenido de los datos cifrados. Todos los procesos de cifrado y descifrado se ejecutan de forma transparente e implican una interacción mínima del usuario.

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.

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.

2.5.1 Iconos superpuestos

Los iconos superpuestos son pequeños iconos que aparecen en elementos del explorador de Windows. Su finalidad es proporcionar información rápida sobre el estado de cifrado de los archivos. El aspecto de los iconos depende del módulo que haya instalado.

Los iconos superpuestos de Data Exchange sólo se muestran en archivos y volúmenes.

- 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.

Nota
Si no aparece ningún icono superpuesto, consulte el artículo 108784 de la base de conocimiento de Sophos.

2.5.2 Cifrado transparente

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

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

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.

2.5.3 Frase de acceso al soporte para medios extraíbles

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 soporte 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.

Para obtener instrucciones sobre cómo definir una frase de acceso al soporte, consulte Usar una frase de acceso al soporte (página 19).

La frase de acceso al soporte 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 soporte 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: Si les proporciona la frase de acceso al medio, obtendrán acceso a todos los archivos de los medios extraíbles con una única frase de acceso, independientemente de la clave utilizada para el cifrado de los archivos individuales.

También puede restringir el acceso a todos los archivos proporcionando al usuario externo sólo la 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.

No es necesario especificar una frase de acceso al soporte 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

No se admiten los discos Blu-ray ni los DVD de doble capa.

3 Bandeja del sistema de Sophos SafeGuard

Puede acceder a todas las funciones de Sophos SafeGuard en su ordenador a través del icono de la bandeja del sistema de Sophos SafeGuard de la barra de tareas de Windows. La disponibilidad de funciones específicas depende de los módulos que tenga instalados.

Haga clic con el botón derecho en el icono de la bandeja del sistema de Sophos SafeGuard para mostrar las siguientes opciones:

- **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 a su certificado.
  - **Certificado de empresa**: Muestra la información relativa a su certificado de empresa.
- **Restablecer credenciales de BitLocker**: Abre un cuadro de diálogo para cambiar el PIN de BitLocker.
- **Crear nueva clave**: Abre un cuadro de diálogo para crear una clave nueva que se utilice para SafeGuard Data Exchange (página 4) o SafeGuard Cloud Storage (página 3). Solo está disponible si alguno de los dos módulos está instalado en el equipo.
- **Cambiar frase de acceso al soporte**: Permite cambiar la frase de acceso del soporte, consulte SafeGuard Data Exchange (página 4).
- **Sincronizar**: Inicia la sincronización con el servidor de SafeGuard Enterprise. La información sobre herramientas muestra el progreso de la sincronización. También puede hacer doble clic en el icono de la bandeja del sistema para iniciar la sincronización.
- **Estado**: Muestra información sobre el estado actual del equipo protegido con SafeGuard Enterprise:

Campo	Información
Última directiva recibida	La fecha y la hora en que el equipo recibió una directiva nueva por última vez.
Última clave recibida	La fecha y la hora en que el equipo recibió una clave nueva por última vez.
Último certificado recibido	La fecha y la hora en que el equipo recibió un certificado nuevo por última vez.
Último contacto del servidor	La fecha y la hora del último contacto con el servidor.

Campo	Información
Estado del usuario SGN	El estado del usuario que tiene la sesión iniciada en el equipo (sesión de Windows): — **pendiente** La replicación del usuario en SafeGuard POA está pendiente. Esto significa que la sincronización inicial del usuario aún no se ha completado. 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 de 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. — **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. — **usuario no confirmado** Los usuarios no confirmados no tienen acceso al conjunto de claves debido a uno de estos motivos: – El usuario ha especificado unas credenciales incorrectas. – El usuario es un usuario local. – No se puede acceder al servidor de autenticación APN. – No se ha podido realizar la autenticación. – Consulte el artículo de la base de conocimiento

Campo	Información
Estado de equipo SGN	Indica el nivel de seguridad de la estación. — **no aplicable** La función relacionada no está activa. — **equipo seguro** El estado del sistema del equipo es seguro. — **equipo afectado** El estado del sistema del equipo no es seguro. Por lo tanto, se han revocado las claves y no puede acceder a los archivos cifrados.
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. Para más información, consulte la Ayuda de usuario de SafeGuard Enterprise.

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

4 Cómo...

4.1 Cifrar un ordenador 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, la unidad flash USB o TPM no está disponible o 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 de hardware satisfactoria, 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.

4.1.1 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. Recomendamos utilizar una unidad flash USB sin cifrar para almacenar la clave. Las unidades de destino válidas para la clave de inicio se muestran en el cuadro de diálogo. Más adelante, deberá insertar el dispositivo de almacenamiento con la clave cada vez que inicie el equipo.

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

4.1.2 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. 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
Tenga cuidado al establecer un PIN o una contraseña. El entorno previo al arranque solo admite la distribución de teclado en inglés EE. UU. Si ahora establece un PIN o una contraseña con caracteres especiales, es posible que deba utilizar teclas distintas cuando los introduzca para iniciar sesión más adelante.

4.1.3 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
Tenga cuidado al establecer un PIN o una contraseña. El entorno previo al arranque solo admite la distribución de teclado en inglés EE. UU. Si ahora establece un PIN o una contraseña con caracteres especiales, es posible que deba utilizar teclas distintas cuando los introduzca para iniciar sesión más adelante.

4.1.4 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.

4.2 Restablecer una contraseña o un PIN de BitLocker olvidado

Si no puede iniciar sesión en su ordenador porque ha olvidado su PIN, contraseña o llave USB, necesitará una clave de recuperación. Para solicitar una clave de recuperación:

1. Reinicie el ordenador y pulse la tecla **Esc** en la pantalla de inicio de sesión de **BitLocker**.
2. En la pantalla **Recuperación de BitLocker**, busque el **ID de la clave de recuperación**.
   El **ID de la clave de recuperación** se muestra solo unos instantes. Para volver a verlo, es necesario reiniciar el ordenador.
3. Póngase en contacto con su administrador y proporciónele el **ID de la clave de recuperación**.
   El administrador debe buscar la clave de recuperación para su ordenador en Sophos SafeGuard Management Center y darle la clave.
4. En la pantalla **Recuperación de BitLocker**, introduzca la clave de recuperación.
   Ahora puede iniciar el ordenador.

Inmediatamente después de iniciar sesión en el sistema de nuevo, especifique credenciales de BitLocker nuevas. En función del sistema operativo, se muestra un cuadro de diálogo para el restablecimiento de credenciales. Si este cuadro de diálogo no aparece automáticamente, haga clic con el botón derecho en el icono Sophos SafeGuard de la barra de tareas, seleccione **Restablecer credenciales de BitLocker** y siga las instrucciones en pantalla.

4.3 Restablecer una contraseña o un PIN de BitLocker olvidado con Desafío/Respuesta

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. Mueva el ratón sobre los caracteres para mostrar una ayuda de deletreo o pulse **F1** varias veces para mostrar este cuadro de ayuda. El código caduca en 30 minutos, provocando el apagado automático del ordenador.
5. 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).
   - Tan pronto como un campo de texto se rellene completamente, el enfoque pasa al siguiente campo de texto de forma automática.
   - Si introduce un carácter erróneo por equivocación, el bloque se marcará en rojo.
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

Inmediatamente después de iniciar sesión en el sistema de nuevo, especifique credenciales de BitLocker nuevas. En función del sistema operativo, se muestra un cuadro de diálogo para el restablecimiento de credenciales. Si este cuadro de diálogo no aparece automáticamente, haga clic con el botón derecho en el icono Sophos SafeGuard de la barra de tareas, seleccione **Restablecer credenciales de BitLocker** y siga las instrucciones en pantalla.

4.4 Cifrar todos los archivos según la política

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.

Para iniciar el proceso de cifrado manualmente, haga clic con el botón derecho en el nodo **Este PC** en el Explorador de Windows y seleccione **SafeGuard File Encryption > Cifrar según directiva**.

El Asistente de cifrado de archivos de SafeGuard (página 13) cifra todos los archivos de las carpetas y subcarpetas cubiertas por las reglas de cifrado definidas.

4.4.1 Asistente de cifrado de archivos de SafeGuard

Para abrir el Asistente de cifrado de archivos de SafeGuard, haga clic con el botón derecho en el nodo **Este PC** o una carpeta del Explorador de Windows y seleccione **SafeGuard File Encryption > Cifrar según directiva**.

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 o procesados. 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.

4.5 Cifrar/Descifrar archivos de forma manual

SafeGuard File Encryption le permite cifrar o descifrar archivos individuales de forma manual. Haga clic con el botón derecho en un archivo y seleccione **Cifrado de archivos de SafeGuard**. Están disponibles las siguientes funciones:

- **Mostrar estado de cifrado**: Indica si el archivo está cifrado o no, así como la clave utilizada.
- **Cifrar según directiva**: Consulte Cifrar todos los archivos según la política (página 12).
- **Descifrar** (solo para el cifrado de archivos basado en la ubicación): Le permite descifrar un archivo que no está cubierto por una regla de File Encryption.
- **Descifrar el archivo seleccionado** (solo para el cifrado de archivos basado en la aplicación): Le permite descifrar el archivo y guardarlo en texto sin formato. Recomendamos descifrar el archivo solo en caso de no contener datos confidenciales.

- **Cifrar el archivo seleccionado** (solo para el cifrado de archivos basado en la aplicación): Le permite cifrar archivos de forma manual con la clave especificada en la política.
- **Crear archivo protegido con contraseña**: Aquí puede definir una contraseña para cifrar archivos individuales de forma manual. Esta opción le resultará útil si desea compartir archivos de manera segura con personas de fuera de su red corporativa. Consulte Enviar archivos cifrados por correo electrónico (página 15).

Si hace clic con el botón derecho en carpetas o unidades, están disponibles las siguientes funciones:

- **Mostrar estado de cifrado**: Muestra una lista de archivos incluidos con iconos que indican el estado de cifrado, así como la clave utilizada.
- **Cifrar según directiva**: Consulte Cifrar todos los archivos según la política (página 12).

Las siguientes opciones solo están disponibles para Cloud Storage y Data Exchange:

- **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. Si selecciona la opción **Recordar y no volver a mostrar este cuadro de diálogo**, el cuadro de mensaje no se volverá a mostrar para el medio en cuestión. En este caso, aparecerá el nuevo comando **Reactivar cifrado** en el menú contextual del dispositivo correspondiente en el Explorador de Windows. 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.

4.6 Ver dónde se cifran los archivos

Si quiere comprobar dónde se cifran los archivos en su ordenador y qué claves se utilizan para proteger sus archivos, puede utilizar la herramienta `FETool` de SafeGuard Enterprise.

Para abrir la herramienta `FETool` de SafeGuard Enterprise, abra una ventana de línea de comandos, vaya a `C:\Program Files (x86)\Sophos\SafeGuard Enterprise \FileEncryption` e introduzca `fetool rli -a`.

Este comando enumera todas las reglas de cifrado aplicables a su ordenador. La lista contiene el modo de cifrado, la ruta completa a las carpetas relevantes y las claves utilizadas.

4.7 Usar una contraseña para proteger un archivo

Al enviar correos electrónicos a destinatarios de fuera de su red corporativa, le recomendamos que cifre los archivos con una contraseña. Así los destinatarios pueden acceder a los archivos cifrados sin tener SafeGuard Enterprise instalado.

Siga estos pasos:

1. Haga clic con el botón derecho en el archivo que quiera enviar y seleccione **Crear archivo protegido con contraseña**.
2. Siga las instrucciones en pantalla para crear una contraseña. Recomendamos usar una contraseña segura y no incluirla en el mismo correo electrónico que los archivos.
   El archivo se cifra y guarda como archivo HTML. Ahora puede adjuntar el archivo HTML a los correos electrónicos de forma segura.

   Nota
   - Necesita espacio libre en disco para el cifrado.
   - El archivo HTML cifrado es mayor que el archivo original.
   - El tamaño máximo de archivo admitido es 50 MB.
   - Para enviar varios archivos a la vez, puede comprimirlos en un archivo .zip y luego cifrar el archivo .zip.

3. Comunique la contraseña a los destinatarios por teléfono o cualquier otro medio de comunicación. Los destinatarios pueden utilizar uno de estos navegadores para abrir el archivo adjunto protegido con contraseña:
   - Mozilla Firefox
   - Google Chrome
   - Microsoft Internet Explorer 11
   - Microsoft Edge
4. Indique a los destinatarios que hagan doble clic en el archivo y que sigan las instrucciones en pantalla para realizar una de las siguientes acciones:
   - Introduzca la contraseña y haga clic en **Introducir** para acceder al archivo.
   - Haga clic en **Proteger un nuevo archivo con contraseña** para proteger otro archivo con una contraseña.

Los destinatarios pueden acceder al archivo que haya protegido con una contraseña y pueden proteger el archivo con una contraseña cuando se lo vuelvan a enviar. Tienen la opción de utilizar la misma contraseña o una nueva. Incluso pueden proteger un archivo nuevo con una contraseña.

4.8 Enviar archivos cifrados por correo electrónico

Cuando envíe archivos sin cifrar a destinatarios de su red corporativa, no tendrá que preocuparse del cifrado o descifrado. Si el destinatario tiene la clave apropiada, podrá leer el archivo.

Para enviar correos electrónicos fuera de su red corporativa, SafeGuard Enterprise ofrece un complemento para Microsoft Outlook que permite cifrar fácilmente los archivos adjuntos de correo electrónico. Cuando envíe un correo con uno o más archivos adjuntos, el sistema le preguntará cómo quiere enviarlos. Las opciones disponibles pueden variar según el estado de cifrado de los archivos que ha adjuntado al correo.

Nota
Cuando envíe elementos incrustados como contactos (.vcf) o correos electrónicos (.msg) como adjuntos, no se le solicitará que los cifre. Se envían sin cifrar.

- **Protegidos con contraseña**

Seleccione esta opción si va a enviar archivos confidenciales a destinatarios fuera de su organización.

Después de definir una contraseña y pulsar Enviar, el archivo se cifra y guarda como archivo HTML. Si la contraseña protege varios archivos a la vez, cada archivo se cifra por separado con la misma contraseña. Los archivos que ya están cifrados se descifran automáticamente antes de protegerlos con contraseña.

Los destinatarios pueden abrir el archivo con su navegador web en cuanto les dé la contraseña. Recomendamos usar una contraseña segura y no incluirla en el mismo correo electrónico que los archivos. Recomendamos comunicar la contraseña a los destinatarios por teléfono o cualquier otro medio de comunicación.

Los destinatarios pueden utilizar uno de estos navegadores para abrir el archivo adjunto protegido con contraseña:

— Mozilla Firefox

— Google Chrome

— Microsoft Internet Explorer 11

— Microsoft Edge

Es posible que el descifrado funcione con otros navegadores, como los navegadores móviles, pero no se ofrece soporte de forma activa.

Los destinatarios pueden editar el archivo y devolverlo usando la misma contraseña o una nueva. Incluso pueden proteger un archivo nuevo con una contraseña. Un asistente de su navegador les guiará en el proceso. Para más información, consulte el artículo 124440 de la base de conocimiento de Sophos.

También puede proteger archivos con contraseña manualmente. Consulte Usar una contraseña para proteger un archivo (página 14).

- **Desprotegido**

  Seleccione esta opción solo si su archivo adjunto no contiene datos confidenciales. Su responsable de seguridad registrará y monitorizará los casos en los que envíe archivos adjuntos desprotegidos.

- **Adjuntos que se enviarán sin cambiarse**

  Si el correo electrónico contiene archivos adjuntos que no se pueden proteger con contraseña, puede enviarlos sin cambiar o suprimirlos del correo. El cuadro de diálogo contiene una lista de archivos que no pueden protegerse por una de las razones siguientes:

  — El archivo ya está protegido con contraseña. Puede descifrar el archivo primero y utilizar una contraseña nueva o bien enviar el archivo sin cambiar y comunicar la contraseña correspondiente al destinatario.

  — El archivo se ha cifrado con una clave que no está disponible actualmente en su juego de claves. Es posible que la clave se haya revocado de forma temporal debido a un problema de seguridad o que no tenga la propiedad de la clave utilizada para cifrar el archivo. En ese caso, póngase en contacto con el responsable de seguridad.

Al enviar un correo electrónico a destinatarios internos y externos, el sistema lo gestiona como si se enviase solamente a dominios externos.

4.9 Crear una clave local

Las claves locales pueden utilizarse para cifrar archivos en ubicaciones especificadas en un dispositivo extraíble o un proveedor de almacenamiento en la nube. Estas ubicaciones ya deben estar incluidas en una política de cifrado.

Para crear una clave local:

1. Haga clic con el botón derecho en el icono de la bandeja del sistema de Sophos SafeGuard de la barra de tareas de Windows o haga doble clic 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 también tiene que cumplir las políticas 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 de SafeGuard > Cifrar según directiva** 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.

4.9.1 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 de SafeGuard > Importar clave desde archivo**.
2. Introduzca la frase de acceso.

La clave se importará y tendrá acceso al archivo.

4.10 Intercambiar 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 tengan SafeGuard Enterprise instalado en su ordenador pueden utilizar SafeGuard Portable para acceder a archivos cifrados. SafeGuard Portable no es compatible con Mac. Para más información, consulte:

  — Intercambiar datos en medios extraíbles sin SafeGuard Enterprise (página 20)

  — Editar archivos con SafeGuard Portable (página 24)

4.10.1 Cifrar medios extraíbles con SafeGuard Data Exchange

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 si se deben cifrar los archivos de los medios extraíbles, se le preguntará si desea hacerlo al conectar los medios extraíbles al ordenador.

Para iniciar el cifrado de forma manual:

1. Seleccione **SafeGuard File Encryption > Cifrar según directiva** en el menú contextual del Explorador de Windows. Si no se ha definido ninguna clave específica, se mostrará un cuadro de diálogo para la selección de claves.
2. Seleccione una clave y haga clic en **Aceptar**. Se cifrarán todos los datos que contengan los medios extraíbles.

   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 medios 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 soporte, el cifrado inicial comenzará automáticamente cuando conecte otro dispositivo al equipo.

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

4.10.2 Usar una frase de acceso al soporte

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.

Tenga en cuenta que no se puede utilizar una frase de acceso al soporte en ordenadores Mac.

Cambiar/restablecer una frase de acceso al soporte

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.

Sincronizar una frase de acceso al soporte

La frase de acceso a medios en sus dispositivos y su equipo se sincronizarán automáticamente. Si cambia la frase de acceso al soporte en su equipo y conecta un dispositivo que aún utiliza la frase de acceso al soporte 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. Tenga en cuenta que no se puede utilizar una frase de acceso al soporte en ordenadores Mac.

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).

4.10.3 Intercambiar datos en medios extraíbles sin SafeGuard Enterprise

SafeGuard Portable le permite intercambiar datos cifrados en medios extraíbles con destinatarios que no tienen SafeGuard Enterprise.

Nota
SafeGuard Portable no es compatible con ordenadores Mac ni con ordenadores que tengan instalado Sophos SafeGuard.

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.

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.

Los destinatarios pueden descifrar datos cifrados y volver a cifrarlos en cuanto les proporcione la frase de acceso al soporte necesaria o la frase de acceso de una clave local. Pueden 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 esté instalado en el ordenador del destinatario. Permanece en el medio extraíble.

Para obtener más información, consulte Editar archivos con SafeGuard Portable (página 24).

4.10.4 Grabar archivos en CD/DVD con SafeGuard Data Exchange

SafeGuard Data Exchange permite grabar archivos cifrados en un CD/DVD con el asistente de grabación de Windows. El responsable de seguridad debe definir una regla de cifrado para la unidad

de grabación de CD. Si no se ha especificado ninguna regla de cifrado para la unidad de grabación de CD, los archivos se grabarán siempre sin cifrar.

La extensión de grabación de disco de SafeGuard para el asistente de grabación de CD solo está disponible para grabar CD/DVD en formato **Mastered**. 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 un CD/DVD.

En el asistente de grabación de CD, puede especificar la forma en que se grabarán los archivos en el CD (cifrados o no cifrados). 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.

Cifrar archivos 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.

Grabar 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.

Copiar SafeGuard Portable en 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.

4.11 Intercambiar datos en la nube sin SafeGuard Enterprise

SafeGuard Portable le permite intercambiar datos cifrados en la nube con destinatarios que no tienen SafeGuard Enterprise.

SafeGuard Portable le permite acceder a datos cifrados en su almacenamiento en la nube desde ordenadores sin SafeGuard Enterprise. 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. 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 obtener más información sobre cómo utilizar SafeGuard Portable, consulte Editar archivos con SafeGuard Portable (página 24).

Al hacer doble clic en un archivo o seleccionar el comando Abrir, no se descifra el archivo in situ. Esto se debe a que los archivos descifrados en las carpetas de sincronización del almacenamiento en la nube se sincronizan automáticamente con la nube. Al hacerlo, se mostrará un cuadro de diálogo donde podrá seleccionar una ubicación segura para el archivo. 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

4.12 Usar claves predeterminadas

Al definir 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.

El responsable de seguridad debe permitir explícitamente el uso de claves predeterminadas para Cloud Storage. Si se permite, el usuario podrá seleccionar una clave predeterminada de un grupo predefinido de claves y utilizarla para cifrar carpetas en su almacenamiento en la nube.

Puede definir una clave predeterminada desde el menú contextual en las siguientes ubicaciones:

- medios extraíbles
- archivos en medios extraíbles
- carpetas o subcarpetas de sincronización de Cloud Storage
- archivos en una carpeta o subcarpeta de sincronización de Cloud Storage
- Además, puede definir una clave como predeterminada inmediatamente después de crear una nueva clave local en el cuadro de diálogo **Crear clave**.

Para definir una clave predeterminada, seleccione **SafeGuard File Encryption > Establecer clave predeterminada**.

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.

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

Para leer archivos cifrados en dispositivos Android e iOS con Sophos Secure Workspace es necesario usar claves locales para el cifrado. Para obtener más información, consulte la Ayuda de usuario de Sophos Secure Workspace.

Ejemplo

Desea utilizar Dropbox para proporcionar datos protegidos a varios partners y dar acceso a cada partner a una subcarpeta únicamente. Para ello, solo tiene que establecer una clave predeterminada aparte para cada subcarpeta. SafeGuard Enterprise añadirá SafeGuard Portable a cada subcarpeta para que los partners 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, podrán 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.

4.13 Recuperar archivos cifrados

Si un archivo está cifrado con una clave que no está disponible en el conjunto de claves, no podrá abrir el archivo. Esto quizá se deba a que no debe acceder al archivo según la política de la empresa. Sin embargo, en algunos casos, es posible que tenga permiso de acceso al archivo pero simplemente no tenga la clave necesaria. En ese caso, debe averiguar qué clave se utilizó y pedir a su responsable de seguridad que la asigne a su conjunto de claves. Proceda de la siguiente forma:

1. Haga clic con el botón derecho en el archivo y pulse **Cifrado de archivos de SafeGuard > Mostrar estado de cifrado**.
   Se mostrará la clave que se utilizó para cifrar el archivo.
2. Póngase en contacto con su responsable de seguridad e facilítele el nombre de la clave.
3. Pídale que asigne la clave a su conjunto de claves.
4. Cuando su responsable de seguridad le confirme que se ha actualizado su política de usuario, haga clic con el botón derecho en el icono de Sophos SafeGuard en la barra de tareas del equipo.
5. Haga clic en **Sincronizar**.
6. De nuevo, haga clic en el icono en la bandeja del sistema y pulse **Estado**.
   Aparecerá un diálogo con la fecha en la que se transfirió la última clave a su equipo. La fecha actual se muestra en **Última clave recibida** cuando se ha añadido la clave solicitada al conjunto de claves.

Ahora puede acceder al archivo.

4.14 Comprobar la conexión con el servidor de SafeGuard Enterprise

Si tiene problemas para sincronizar su estación de trabajo con el servidor, puede utilizar la herramienta Client/Server Connectivity Check para averiguar por qué falla la comunicación entre la estación de trabajo y el servidor de SafeGuard Enterprise.

Para abrir la herramienta SafeGuard Enterprise Client/Server Connectivity Check, vaya a `C:\Archivos de programa (x86)\Sophos\SafeGuard Enterprise\Client` y ejecute la aplicación `SGNCSCC.exe`.

Para más información, consulte el artículo 109662 de la base de conocimiento de Sophos.

4.15 Editar archivos con SafeGuard Portable

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

Ha recibido 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 y después volver a cifrarlos.

   Además de los detalles de los archivos, 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. Sólo se pueden descifrar aquellos archivos de los que se conozca la frase de contraseña correspondiente a la clave utilizada.
2. Para editar un archivo, haga clic con el botón derecho y seleccione uno de los siguientes 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 con la última clave utilizada.
Descifrar	Abre el cuadro de diálogo **Introducir frase de acceso** para introducir la frase de acceso que permite descifrar el archivo seleccionado.
Estado de cifrado	Muestra el estado de cifrado del archivo.
Copiar a	Copia el archivo a la carpeta que elija y lo descifra.
Eliminar	Elimina el archivo seleccionado.

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

4.15.1 Establecer claves de cifrado para SafeGuard Portable

Para establecer una clave de cifrado para SafeGuard Portable:

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.
3. Confirme la frase de acceso y haga 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.

4.15.2 Cifrar archivos con SafeGuard Portable

1. En SafeGuard Portable, haga clic con el botón derecho y seleccione **Cifrar**.

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

Al guardar archivos nuevos con el procedimiento de arrastrar y soltar, se le preguntará si desea cifrarlos.

Si no se ha establecido ninguna clave predeterminada, se abrirá un cuadro de diálogo para hacerlo. Introduzca el nombre de la clave y la frase de acceso, confirme esta última y haga clic en **Aceptar**.

2. Para cifrar más archivos con la clave que acaba de establecer, seleccione **Cifrar** en el menú contextual o en el menú **Archivo**.
   La última clave que SafeGuard Portable haya utilizado se usará para todos los procesos de cifrado posteriores, hasta que seleccione otra diferente.

4.15.3 Descifrar archivos con SafeGuard Portable

1. En SafeGuard Portable, haga clic con el botón derecho y seleccione **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 soporte le da acceso a todos los archivos cifrados, sin que importe la clave local de cifrado. Si solo dispone de la frase de acceso de una clave local, únicamente 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.

Después de descifrar los archivos e introducir la frase de acceso de la clave, no es necesario especificarla de nuevo la próxima vez que cifre o descifre los archivos que se han cifrado con la misma clave.

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.

Los archivos que se hayan descifrado se cifrarán de nuevo al cerrar SafeGuard Portable.

5 Soporte

Versión completa

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

- Visitar el foro Sophos Community 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.aspx.
- Abrir un ticket de incidencia con nuestro equipo de soporte en https://secure2.sophos.com/es-es/support/contact-support/support-query.aspx.

6 Aviso legal