Dell Data Guardian

Guía del usuario v1.2

Notas, precauciones y avisos

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

Guía del usuario de Dell Data Guardian

2017 - 04

Rev. A01

Tabla de contenido

1

Introducción a Dell Data Guardian

La *Guía del usuario de Dell Data Guardian* proporciona la información necesaria para instalar y usar Dell Data Guardian.

Descripción general

En función de las políticas establecidas por el administrador, Dell Data Guardian protege, por ejemplo, los siguientes datos:

- Sistemas de uso compartido de archivos basado en la nube: los equipos Windows o los dispositivos móviles capturan datos destinados al almacenamiento en la nube, los cifran y los cargan a la nube.
- Los documentos de Office se guardan en una ubicación local, se comparten con otros usuarios de varias formas o se almacenan en medios extraíbles. Pueden protegerse estos tipos de documentos de Office: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm.

> **NOTA:**
> El administrador le informará si su empresa utiliza Data Guardian con almacenamiento en la nube, documentos de Office o ambos.

Puede utilizar Data Guardian en las plataformas siguientes:

- Windows
- iOS
- Android
- Tanto este producto como Data Guardian para Mac pueden abrir archivos cifrados por el otro.
    - Este documento trata únicamente Dell Data Guardian para Windows.
    - Para obtener información de usuario acerca de Dell Data Guardian para Mac, consulte la ayuda en línea del software.

Soporte adicional

En caso de que necesite soporte adicional, póngase en contacto con su administrador.

2

Requisitos de Dell Data Guardian

En este capítulo se enumeran los requisitos de hardware y software.

NOTA:
No es compatible con IPv6.

Servidor

Data Guardian requiere que el cliente esté conectado a un Dell Enterprise Server o Dell Enterprise Server - VE, v. 9.6 o superior. A efectos del presente documento, ambos servidores se citan como servidor Dell, salvo que sea necesario mencionar una versión específica (por ejemplo, que un procedimiento sea diferente si se utiliza Dell Enterprise Server - VE).

Cliente Encryption

- Durante la implementación se deberán seguir las prácticas recomendadas para TI. Entre los que se incluyen, a modo de ejemplo, entornos de prueba controlados, para las pruebas iniciales e implementaciones escalonadas para los usuarios.
- La cuenta de usuario que realiza la instalación/actualización/desinstalación debe ser un usuario administrador local o de dominio, que puede ser designado temporalmente mediante una herramienta de implementación como Microsoft SMS o Dell KACE. No son compatibles los usuarios con privilegios elevados que no sean administradores.
- Realice copia de seguridad de todos los datos importantes antes de iniciar la instalación/desinstalación.
- Durante la instalación, no realice cambios en el equipo, incluida la inserción o extracción de las unidades (USB) externas.
- Aunque el cliente de Cifrado no es necesario, todos los clientes de Cifrado utilizados con Data Guardian deben ser v8.12 o posteriores.
- Data Guardian no es compatible con Microsoft Office 365.
- Para el cifrado en la nube, el equipo debe tener una unidad de disco (valor de letra) asignable disponible.
- Asegúrese de que los dispositivos de destino pueden conectarse a https://yoursecurityservername.domain.com:8443/cloudweb/register y a https://yoursecurityservername.domain.com:8443/cloudweb.
- Antes de implementar Data Guardian, es preferible que los dispositivos de destino no tengan configuradas cuentas de almacenamiento en nube.

  Si los usuarios desean mantener sus cuentas existentes, deben asegurarse de retirar todos los archivos que quieran conservar *sin cifrar* del cliente de sincronización antes de instalar Data Guardian.
- Los usuarios deberán estar preparados para reiniciar sus equipos una vez que se instale el cliente.
- Data Guardian no interfiere con el comportamiento de los clientes de sincronización. Por lo tanto, los administradores y usuarios finales deben familiarizarse con el funcionamiento de estas aplicaciones antes de implementar Data Guardian. Para obtener más información, consulte el servicio de asistencia de Box en https://support.box.com/home, el servicio de asistencia de Dropbox en https://www.dropbox.com/help o el servicio de asistencia de OneDrive en http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.
- Si se está ejecutando Office 2010: si las políticas se han definido para proteger documentos de Office y documentos habilitados para macros, los usuarios deben tener Office 2010 Service Pack 1 o superior (v14.0.6029 o superior). Consulte https://support.microsoft.com/en-us/kb/2121559 para determinar si se ha aplicado un Service Pack al conjunto de aplicaciones de Microsoft Office 2010. Sin esta actualización, no se puede tener acceso a los documentos protegidos. Independientemente de la política, los nuevos documentos de Office no estarán protegidos a menos que la funcionalidad de barrido esté activada. El siguiente barrido convierte los documentos de Office en archivos protegidos, pero los usuarios no pueden tener acceso a ellos sin una versión compatible de Office.
- Data Guardian no admite la herramienta de Restauración del sistema de Windows.

- Asegúrese de comprobar periódicamente www.dell.com/support para obtener la documentación y las recomendaciones técnicas más recientes.

Requisitos previos del cliente

Si no se ha instalado todavía, el instalador instala el paquete redistribuible Microsoft Visual C++ 2015 (x86 y x64).

NOTA:
Para los sistemas operativos Windows 7 y Windows 8.1, los equipos deben contar con todas las actualizaciones de Windows. Para obtener más información, consulte https://support.microsoft.com/en-us/help/2919355 y https://support.microsoft.com/en-us/help/2999226.

Se requiere Microsoft .Net 4.5.2 (o una versión posterior) para Data Guardian. Todos los equipos enviados desde la fábrica de Dell vienen con .Net 4.5.2 preinstalado. Sin embargo, si no está instalando en hardware de Dell o si está actualizando Data Guardian en hardware de Dell más antiguo, debería comprobar qué versión de .Net tiene instalada y, si fuera necesario, actualizar la versión antes de instalar Dell Data Guardian, con el fin de evitar errores durante la instalación/actualización. Para comprobar qué versión de .Net tiene instalada, siga estas instrucciones en el equipo en el que se va a realizar la instalación: http://msdn.microsoft.com/en-us/library/hh925568(v=vs.110).aspx. Para instalar Microsoft .Net Framework 4.5.2, acceda a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware del cliente de Windows

Los requisitos de hardware mínimos deben cumplir las especificaciones mínimas del sistema operativo. La tabla siguiente explica en detalle el hardware compatible con el cliente de Windows.

Hardware de Windows

- 200 MB de espacio libre en el disco, dependiendo del sistema operativo
- Tarjeta de interfaz de red 10/100/1000 o Wi-Fi
- Protocolo TCP/IP instalado y activado

Si su empresa cifra los datos para el almacenamiento en la nube, su equipo debe tener un carácter alfabético disponible para asignar a una unidad de disco.

Sistemas operativos

La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (32 bits y 64 bits)

- Windows 7 SP0-SP1
- Windows 8.1
- Windows 10

NOTA:
Windows 7 no es compatible con la política de geolocalización para los eventos de auditoría de Data Guardian.

Sistemas operativos Android

- 4.4 - 4.4.4 KitKat
- 5.0 -5.1.1 Lollipop
- 6.0-6.0.1 Marshmallow

- 7.0 Nougat

Sistemas operativos iOS

- iOS 8.x
- iOS 9.x
- iOS 10.x - 10.3

Clientes de sincronización en la nube

La siguiente tabla muestra los clientes de sincronización en la nube compatibles con Data Guardian. A menudo se publican actualizaciones de los clientes de sincronización. Dell recomienda probar nuevas versiones de clientes de sincronización con Data Guardian antes de introducirlas en el entorno de producción.

Clientes de sincronización en la nube

- Dropbox
- Dropbox for Business (solo para Windows)

  NOTA:
  En función de la versión de servidor de Dell que utilice su empresa, todos los archivos y las carpetas de cuentas personales de Dropbox vinculadas a cuentas empresariales podrían cifrarse.

- Box

  NOTA:
  Las herramientas y la edición de Box no son compatibles con Data Guardian. El uso de herramientas de Box puede provocar que la pantalla se vuelva azul.

- Google Drive
- OneDrive
- OneDrive para la Empresa
- Unified OneDrive

  NOTA:
  Unified OneDrive es un cliente de sincronización unificado tanto para OneDrive como para OneDrive para la Empresa.

Navegadores web

Puede utilizar Data Guardian > Cifrado en la nube con Internet Explorer, Mozilla Firefox y Google Chrome.

NOTA:
Data Guardian > El cifrado en la nube no es compatible con el explorador Microsoft Edge.

Tareas del usuario: cifrado en la nube y Office protegido

El administrador ya ha configurado las políticas para Data Guardian y le informará de si su empresa utiliza Data Guardian:

- Para administrar sus clientes de sincronización en la nube
- Para administrar sus clientes de sincronización en la nube además de ofrecer protección adicional en los documentos de Office: si su empresa solo protege los documentos de Office pero no administra un cliente de sincronización en la nube, siga los pasos del apartado Tareas del usuario: Office protegido sin cifrado en la nube.

Si su empresa utiliza Data Guardian con almacenamiento en la nube:

- Antes de implementar Data Guardian, consulte la ayuda en línea para el proveedor de almacenamiento en la nube/clientes de sincronización en la nube para comprender cómo funciona la aplicación de almacenamiento en la nube. Este documento explica principalmente cómo utilizar Data Guardian.
- Normalmente, instalará y trabajará con un cliente de sincronización en la nube. Es posible que su empresa haya optado por un cliente de sincronización en la nube preferido y haya establecido una política para permitirle utilizar solo ese cliente.

Descripción general de las tareas

Esta introducción resume la secuencia para instalar y utilizar Data Guardian.

Instalar Data Guardian y un cliente de sincronización en la nube

Tarea	Descripción	Para obtener más información
Si se instala un cliente de sincronización en la nube antes de Data Guardian	Las carpetas y archivos preexistentes sincronizados en la nube no están cifrados. **NOTA:** Las carpetas y archivos preexistentes sincronizados desde la nube están cifrados.	Consulte Carpetas preexistentes con archivos sin cifrar.
Instalar Data Guardian	Determine lo siguiente: El usuario debe instalar Data Guardian El administrador ya ha instalado Data Guardian; continúe con el siguiente paso.	El usuario es el encargado de instalar; consulte Instalar Data Guardian en Windows. Reinicie y continúe con el siguiente paso.
Confirme el estado de activación	Confirme en la bandeja del sistema que el icono de Data Guardian tiene una marca de verificación verde  .	Si el icono tiene un signo de exclamación naranja, consulte Posibles problemas de activación: nube y Office protegido.
Si la política protege documentos en la nube, instale un	Cliente de sincronización empresarial O bien	Cuentas de clientes de sincronización en la nube empresariales O bien

Tarea	Descripción	Para obtener más información
cliente de sincronización en la nube	Cliente de sincronización básico	Cuentas de clientes de sincronización en la nube básicas

NOTA:

Si abre un documento de Office y aparece una página de portada con información de activación o instalación, puede deberse a que el administrador haya definido políticas para proteger documentos de Office. Confirme que Data Guardian está instalado y activado. Consulte Posibles problemas de activación: nube y Office protegidos.

Usar Data Guardian

Tarea	Descripción	Para obtener más información
Ver el cliente de sincronización en la nube en el Explorador de archivos	Después de instalar Data Guardian y un cliente de sincronización en la nube, se muestra la Unidad virtual DDG VDisk en el Explorador de archivos.	Trabajar con carpetas y archivos Acceso a carpetas y archivos de clientes de sincronización en el equipo local
Trabajar con el cliente de sincronización en la nube en la Unidad virtual DDG VDisk	En la Unidad virtual DDG VDisk puede agregar subcarpetas al cliente de sincronización en la nube y arrastrar los archivos o crear archivos nuevos en esas subcarpetas. Después de sincronizar, los archivos se protegen en la nube: los archivos Office pueden abrirse pero solo se muestra una página de portada; los demás archivos están cifrados como archivos .xen. No obstante, en la unidad virtual local, se descifran y se visualizan en texto no cifrado. Para obtener más información, haga clic en el enlace correspondiente para su cliente de sincronización en la nube.	**Cuenta de empresa:** Dropbox for Business OneDrive for Business/OneDrive unificado **Cuenta básica:** Dropbox Box Google Drive OneDrive
Ver el menú de la bandeja del sistema	Ofrece información útil acerca de archivos, carpetas y solución de problemas.	Comprender los elementos del menú de la bandeja del sistema de Data Guardian
Proteger documentos Office habilitados para macros y PDF si la política está activada	Proteja un documento de Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm , .pdf) cuando lo cree. De este modo, serán seguros cuando los comparta con otros o los almacene en un medio extraíble.	Utilizar Documentos de Office con el Modo protegido de Data Guardian • Observar opciones del menú Archivo para determinar el nivel de seguridad de los documentos de Office • Trabajar con las opciones del menú Archivo
Compartir una carpeta en la nube con otros usuarios para colaborar en archivos	Comparta una carpeta con: Usuario interno (con una dirección de correo electrónico del dominio) Usuario externo (con una dirección de correo electrónico que no es del dominio); coordínese con su administrador.	Usuario interno: consulte la ayuda en línea para su proveedor de almacenamiento en la nube. Usuario externo: consulte Usar Data Guardian como usuario externo.

Instalar Data Guardian en la nube y en los documentos protegidos de Office

Carpetas preexistentes con archivos sin cifrar

Antes de implementar Dell Data Protection | Data Guardian (DDG VDisk), es preferible que los dispositivos de destino no tengan configurada una cuenta de proveedor de almacenamiento en la nube.

Si ya dispone de una cuenta de proveedor de almacenamiento en la nube con carpetas que se sincronizan con su equipo local y, a continuación, instala Data Guardian:

- Los archivos y carpetas preexistentes que se hayan sincronizado en la nube se mantendrán como texto no cifrado.
- Los archivos que agregue a estas carpetas preexistentes se mantendrán como texto no cifrado.
- Los archivos que sincronice desde la nube estarán cifrados

  Si desea cifrar los archivos existentes, navegue hasta la Unidad virtual DDG VDisk, cree una subcarpeta nueva en el cliente de sincronización en la nube y mueva los archivos existentes a esa carpeta.

  O bien

  Para contenidos de gran tamaño, un administrador puede solicitar temporalmente el Menú administrar carpetas.

Instalar Data Guardian en Windows

Para instalar Data Guardian, debe ser un administrador local en el equipo.

El equipo debe tener una letra alfabética disponible para asignarla a una unidad de disco.

Después de que se instale Data Guardian, esté preparado para reiniciar el equipo.

1 Para descargar el instalador de Data Guardian, vaya a la ubicación especificada por su administrador.
2 En función de su sistema operativo, seleccione el instalador de 32 bits o 64 bits, que normalmente aparece como **setup32.exe** o **setup64.exe**, y cópielo en el equipo local.
3 Haga doble clic en el archivo para iniciar el instalador.
4 Si se muestra un aviso de seguridad, haga clic en **Ejecutar**.
5 Seleccione un idioma y haga clic en **Aceptar**.
6 Si se le solicita que instale el Paquete redistribuible de Microsoft Visual C++ 2010 o Microsoft .Net Framework 4.0 Client Profile, haga clic en OK.
7 En la ventana de Bienvenida, haga clic en **Siguiente**.
8 Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.
9 En la pantalla Carpeta de destino, haga clic en **Siguiente** para instalar en la ubicación predeterminada de **C:\Archivos de programa\Dell \Dell Data Protection\Dell Data Guardian\.**

  En **C:**, no instale Data Guardian en las carpetas de los usuarios o de Windows ni en la raíz de cualquier unidad. Se mostrará un error.
10 En el campo *Nombre del servidor:*, introduzca el nombre del servidor con el que se comunicará este equipo, como, por ejemplo, servidor.dominio.com. No es necesario incluir www o http(s). Esta información la proporciona el administrador.

  No desmarque la casilla *Activar verificación de confianza en SSL* a menos que lo indique el administrador.
11 Haga clic en **Siguiente**.
12 En la pantalla Confirmar información del servidor de activación, confirme si la dirección URL del servidor es correcta. El instalador añade www o http(s) y el puerto. Haga clic en **Siguiente**.
13 En la ventana Tipo de administración, seleccione esta opción:

- Usuario interno: un usuario con una dirección de correo electrónico en el dominio de la empresa.

14 Haga clic en **Instalar** para comenzar la instalación.

Se mostrará una ventana de estado que muestra el progreso de la instalación.

15 Cuando se muestre la pantalla Instalación completa, haga clic en **Finalizar**.

16 Haga clic en **Sí** para reiniciar.

La instalación de Data Guardian se ha completado.

17 Después de reiniciarlo, confirme en la bandeja del sistema que el icono de Data Guardian tiene una marca de verificación verde  .

Data Guardian y cifrado en la nube

Si su empresa define políticas para proteger los datos en la nube y ya tiene instalado y ha iniciado sesión en un cliente de sincronización, se mostrará una Unidad virtual DDG VDisk en el Explorador de Windows.

NOTA:
Data Guardian no admite el desmonte la unidad virtual.

Si debe instalar e iniciar sesión en un cliente de sincronización, consulte Instalar un cliente de sincronización en la nube.

Instalar un cliente de sincronización de nube

Descargar e instalar

Normalmente, una empresa sugiere que todos los usuarios instalen el mismo cliente de sincronización en la nube. Si procede, utilice el cliente de sincronización en la nube que prefiera su empresa.

NOTA:
El equipo debe tener una letra alfabética disponible para asignarla a una unidad de disco.

NOTA:
Actualmente, Data Guardian no admite un cliente de sincronización instalado en un punto de montaje.

1 Instale un cliente de sincronización en la nube empresarial o básico:

- **Cuentas de clientes de sincronización en la nube empresariales**

  Si su empresa ofrece una opción de cuenta empresarial, su administrador le proporcionará un enlace de descarga e instalación. Opciones disponibles:

  - **Dropbox for Business**: si instala Dropbox for Business, debe también Autenticar Dropbox for Business.
  - OneDrive for Business/OneDrive unificado: para obtener información sobre los pasos detallados, consulte https://support.microsoft.com/en-us/kb/2903984.
- **Cuentas de clientes de sincronización en la nube básicas**
  - **Dropbox**: consulte https://www.dropbox.com/install
  - **Sincronización de Box**: consulte https://www.box.com/box-for-devices
  - **Google Drive**: https://www.google.com/drive/download/
  - **OneDrive/Unified OneDrive (Windows 7 and 8)**: consulte https://onedrive.live.com/about/en-us/download/

    En Windows 8.1 y superior, OneDrive viene preinstalado. Si tiene Windows Update activado, OneDrive unificado reemplaza a OneDrive.

2 Después de instalar e iniciar sesión, le aparecerá la siguiente pantalla:

- En el Explorador de archivos, se ha agregado una Unidad virtual DDG VDisk. Se agrega la carpeta del cliente de sincronización en la nube a esta unidad virtual.

  Si instala más de un cliente de sincronización en la nube, cada cliente muestra una carpeta en esta unidad.

NOTA:
Data Guardian no admite el desmonte la unidad virtual.

- En Explorador de archivos > Favoritos, se agrega una carpeta para su cliente de sincronización en la nube.
- Se muestra el icono del cliente de sincronización en la bandeja del sistema.
- Dependiendo del proveedor de almacenamiento en la nube, puede agregarse automáticamente un acceso directo al cliente de sincronización en el escritorio.
- Únicamente con el Modo Opt-in (pero no con el modo Force-Protected) se añade una carpeta de Documentos seguros a la raíz de la carpeta Documentos. Consulte Documentos > Carpeta de documentos seguros.

Cambiar la letra de la unidad virtual o crear un acceso directo

Después de instalar Data Guardian y un cliente de sincronización en la nube, el icono de la Unidad virtual DDG VDisk se muestra en el Explorador de archivos. Se asigna a la unidad una letra disponible del final del alfabeto.

Para cambiar la letra de la unidad:

1 En la bandeja del sistema, haga clic en el icono de Data Guardian y, a continuación, seleccione **Configurar unidad**.

2 Seleccione una carta disponible de la lista *Corriente*.

3 Haga clic en **Aplicar** o **Aceptar**.
Para agregar el icono de la Unidad virtual DDG VDisk al escritorio, haga clic con el botón derecho del mouse en la unidad y seleccione **Crear acceso directo**.

Autenticar Dropbox for Business

Si instala Dropbox for Business, Data Guardian le solicitará que lleve a cabo la autenticación.

Para autenticar:

1 Tras instalar Data Guardian, quizá se abra la ventana Autenticación, o bien haga clic en el icono de Data Guardian y, a continuación, seleccione **Dropbox > Conectar**.
En la ventana Autenticación se le notificará que Data Guardian debe tener acceso a su cuenta de Dropbox y quizá incluya instrucciones sobre las cuentas de empresa y personales.

Para este usuario, esto proporciona opciones de menú contextual. Para la empresa y su administrador, esto es crucial ya que proporciona medidas de seguridad adicionales.

2 En la ventana Autenticación, haga clic en **Siguiente**.

3 Si se abre la ventana de protección contra amenazas de red, haga clic en **Sí**.

4 En la ventana Autenticación, introduzca el correo electrónico de su dominio y la contraseña de Dropbox.

5 Haga clic en **Iniciar sesión**.

6 Si ha vinculado sus cuentas de empresa y personales de Dropbox, se le indicará que seleccione una cuenta ahora. Debe seleccionar la cuenta de empresa.

7 Haga clic en **Finalizar** o espere a que la ventana se cierre.

Trabajar con carpetas y archivos

Data Guardian trabaja de manera transparente con el cliente de sincronización de la nube. Cuando su administrador establece una política para activar Data Guardian, los archivos están cifrados y protegidos en la nube si se han sincronizado desde su equipo local.

Siga las instrucciones que se indiquen en la ayuda del proveedor del almacenamiento en la nube para realizar las tareas siguientes:

- Crear carpetas
- Cargar/descargar carpetas y archivos

NOTA:
Para cargar archivos, copie o arrastre archivos a carpetas en la Unidad virtual DDG VDisk. Data Guardian no permite arrastrar los archivos desde el equipo local a la web ni crear archivos directamente en el sitio web del proveedor de almacenamiento en la nube.

- Utilizar sincronización selectiva de carpetas
- Compartir carpetas o archivos con usuarios internos que tengan Data Guardian. Consulte Compartir una carpeta con un usuario interno.
- Compartir carpetas o archivos con usuarios externos. Consulte Usar Data Guardian como usuario externo.
- Dejar de compartir carpetas

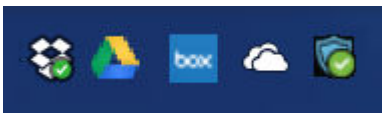
Visualización de carpetas y archivos en el equipo local y en la nube

Acceso a carpetas y archivos de clientes de sincronización en el equipo local

Para acceder a archivos y carpetas sincronizadas, haga clic en la **Unidad virtual DDG VDisk** en el explorador de archivos. Se muestra su cliente de sincronización en la nube.

A continuación se indican otras alternativas para acceder a su cliente de sincronización en la nube.

- En la bandeja del sistema, seleccione el icono del cliente de sincronización y abra la carpeta del cliente de sincronización. Para obtener más información, consulte la ayuda del proveedor de almacenamiento en la nube.



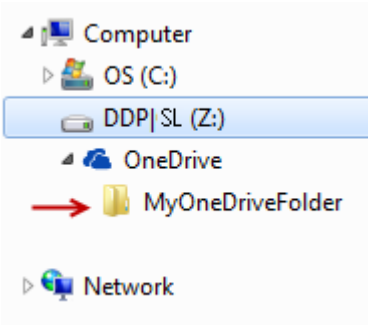
- En Favoritos, haga clic en el icono del cliente de sincronización.

  Al hacer clic en el icono del cliente de sincronización en la bandeja del sistema o en Favoritos, observe que se selecciona la Unidad virtual DDG VDisk. Data Guardian le redirige a esta unidad virtual, que le permite ver las carpetas locales sin cifrar y los archivos en texto no cifrado.

También puede acceder a los archivos y carpetas de la Unidad virtual DDG VDisk a través de un acceso directo de escritorio. Consulte Cambiar la letra de la unidad virtual o crear un acceso directo.

Agregar carpetas

Con Data Guardian, debe agregar subcarpetas en la carpeta sincronizada en la nube. No agregue archivos en la raíz de la Unidad virtual DDG VDisk.



Agregar archivos

Cuando se agrega un archivo a una carpeta, Data Guardian agrega automáticamente un archivo a la carpeta en la web. Data Guardian utiliza el archivo Cómo acceder a archivos seguros.html cuando se comparte una carpeta con usuarios externos. No se requiere abrir ni descargar este archivo. Consulte Usar Data Guardian como usuario externo.

Visualización de carpetas y archivos del cliente de sincronización en la nube

Data Guardian cifra los datos en la nube y los nombres de archivo tienen una extensión .xen. El icono junto al archivo puede cambiar para cada proveedor de almacenamiento en la nube, aunque no muestra el contenido. No es posible abrir archivos en la nube. Por lo tanto, aunque alguien consiga acceder a su cuenta de almacenamiento en la nube, no podrá abrir ni ver sus archivos. De esta manera aumenta la seguridad en la nube. Solo puede ver archivos en texto no cifrado en la Unidad virtual DDG VDisk.

Ocasionalmente, al descargar un archivo .xen en el escritorio y descifrarlo, permanece una copia del archivo con la extensión .xen. Puede eliminar la copia descargada del archivo .xen.

Si su empresa requiere protección adicional para carpetas y archivos en la nube, su administrador puede establecer una política para utilizar nombres de archivos confusos en la nube y al descargarlos. Aunque alguien consiga acceso a su cuenta de almacenamiento en la nube, no podrá abrir los archivos ni leer los nombres de los archivos.

Visualización de carpetas y archivos de cliente de sincronización en un equipo local con Data Guardian y una unidad virtual instalada

Para facilitar el uso de Data Guardian en su equipo local, cuando abra una carpeta en la Unidad virtual DDG VDisk, los archivos de la nube se descifran automáticamente y se muestran en texto no cifrado incluso si están protegidos como archivos cifrados en la nube.

Proteger archivos y carpetas en dispositivos que no disponen de Data Guardian

Si una persona no autorizada descarga un archivo protegido de la nube a un dispositivo que **no** dispone de Data Guardian instalado, la persona no puede tener acceso a los datos. En función de las políticas definidas por el administrador:

- Documentos de Office: el documento se abre, pero solo se muestra una página de portada con un mensaje específico para empresas.
- Documentos que no son de Office: el archivo se descarga como un archivo .xen. La persona no puede abrir el archivo.

> **NOTA:**
> Para los usuarios internos, si se descarga un archivo desde un equipo que dispone de Data Guardian a un dispositivo que no, no podrá ver ese archivo a menos que instale Data Guardian como usuario externo.

En ocasiones, puede mostrarse un archivo .xen en un equipo que tenga Data Guardian instalado. Por ejemplo, si se interrumpió la conexión a Internet antes de finalizar la descarga, es posible que la clave para abrir el archivo no esté disponible. Se muestra un cuadro de diálogo para informar de que no se puede descifrar el archivo.

Data Guardian no permite que se editen archivos sin extensiones. Esos archivos se tratan como archivos de solo lectura. Para editar un archivo sin extensión, descárguelo desde el sitio web del proveedor de almacenamiento en la nube, edítelo y, a continuación, súbalo mediante la Unidad virtual DDG VDisk.

Buscar nombres de archivo y contenido en la Unidad virtual DDG VDisk

Si desea buscar nombres de archivo o contenido en la Unidad virtual DDG VDisk, debe habilitar la indexación de Windows Search para esa unidad.

> **NOTA:**
> La Indización de búsqueda de Windows solo se habilita para las carpetas de Usuarios.

Para activar la indexación de Windows Search para la Unidad virtual DDG VDisk:

1 En Panel de control introduzca **Indexación de búsqueda** en el campo de búsqueda.

2 Seleccione **Opciones de indexación**.

3 En *Cambiar ubicaciones seleccionadas*, seleccione la casilla de verificación de la Unidad virtual DDG VDisk.

> **NOTA:**
> Los pasos restantes pueden variar dependiendo del sistema operativo.

4 Haga clic en **Aceptar**.

5 En Opciones de indexación, haga clic en **Cerrar**.

Ahora puede realizar una búsqueda en la Unidad virtual DDG VDisk.

Cómo compartir una carpeta con un usuario interno

Un usuario interno tiene una dirección de correo electrónico en el dominio de su empresa.

Para compartir una carpeta con un usuario interno, debe acceder al sitio web para su proveedor de almacenamiento en la nube y seleccionar **Compartir**. Consulte la ayuda en línea para el proveedor de almacenamiento en la nube.

Compartir una carpeta mediante Data Guardian y Box

En el sitio web de Box, seleccione una de estas opciones.

Opciones del sitio web de Box	Opciones	Descripción
Compartir	Disponible para archivos y carpetas Acceso de visualización	Cuando se abra la ventana Compartir, asegúrese de que está seleccionada la opción **Sí** en Permitir descarga. Después de descargar carpetas o archivos, las personas que lo han compartido deben extraer la carpeta comprimida y moverla con los archivos a la Unidad virtual DDG VDisk.
Invitar a colaboradores	Disponible para las carpetas Ver o Editar el acceso	Cuando se abra la ventana Invitar, puede seleccionar **Editor** o **Visor**. Las personas con las que comparte pueden sincronizar la carpeta con su equipo y esta se sincroniza con la Unidad virtual DDG VDisk.

Utilizar Documentos de Office con el Modo protegido de Data Guardian

Con el fin de mejorar la seguridad de empresa, el administrador puede habilitar una política para proteger archivos de estas aplicaciones de Office:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Si una persona no autorizada accede a un archivo protegido, el archivo permanece cifrado, por ejemplo, cuando:

- Se adjunta a un correo electrónico
- Se mueve a un navegador, en algunos clientes de sincronización en la nube puede hacer clic con el botón derecho del mouse en un nombre de archivo y seleccionar **Mover**.
- Se comparte en la red
- Se sube a un proveedor de almacenamiento en la nube
- Se almacena en un medio extraíble

Para documentos de Office, puede mostrarse una página de portada con instrucciones para la instalación o activación de Data Guardian, por ejemplo:

- Es necesario instalar Data Guardian.
- Es necesario activar Data Guardian.
- Abra un documento de Office protegido en la nube.
- Ha descargado un archivo Office desde su equipo que dispone de Data Guardian a un dispositivo personal que no lo tiene.
- Un usuario no autorizado accede a uno de los archivos de Office: la página de portada muestra un mensaje específico para empresas, pero el usuario no puede ver el contenido del archivo.

Si su empresa utiliza el Modo protegido de Data Guardian, consulte lo siguiente:

- Observar opciones del menú Archivo para determinar el nivel de seguridad de los documentos de Office
- Trabajar con las opciones del menú Archivo
- Determinar qué documentos Modo Opt -in están protegidos
- Opciones de menú adicionales para documentos de Office protegidos
- Usuarios externos y documentos de Office protegidos

Observar opciones del menú Archivo para determinar el nivel de seguridad de los documentos de Office

Para determinar si el administrador ha habilitado políticas de Data Guardian, abra un documento de Office y seleccione **Archivo**. Si se muestra *Guardar como protegido* en el panel izquierdo, significa que dispone de protección adicional en los documentos de Office.

Para determinar el nivel de seguridad, fíjese en las opciones que están activadas o desactivadas:

- **Modo Opt-in**: dispone de varias opciones para elegir qué documentos de Office proteger.
  - Las opciones *Guardar como* y *Guardar como protegido* están activadas: si decide proteger un documento de Office, seleccione **Guardar como protegido**.
  - Las opciones *Imprimir* y *Exportar* se pueden activar o desactivar en función de las políticas.
  - La opción *Compartir* (*Guardar y enviar* para Office 2010) está activada.
  - Carpeta **Documentos > Documentos seguros**: con el Modo Opt-in (pero no con el modo Force-Protected) se añade una carpeta de Documentos seguros a la raíz de la carpeta Documentos. Los documentos de Office incluidos en esta carpeta están cifrados. Si quita un documento de Office protegido de esta carpeta, sigue cifrado. Si cambia el nombre de la carpeta, todo su contenido sigue cifrado. Si elimina la carpeta, se vuelve a crear.
- **Modo Force-Protected**: la empresa requiere un nivel de seguridad mayor.
  - La opción *Guardar como* está desactivada y la opción *Guardar como protegido* está activada: debe guardar todos los documentos de Office en Modo protegido.
  - Las opciones *Imprimir* y *Exportar* se pueden activar o desactivar en función de las políticas.
  - La opción *Compartir* (*Guardar y enviar* para Office 2010) está desactivada.

    NOTA:
    Con el modo Force-Protected, la política también permite horas específicas para realizar un barrido de su equipo para localizar cualquier archivo de Office sin protección y cambiarlos al modo protegido. Debe haber iniciado sesión y estar conectado a la red para que Data Guardian realice el barrido de los archivos de Office sin protección.

- Si selecciona **Guardar como protegido**, la única opción en el campo *Guardar como tipo* es *Protegido de Office*.

- **Archivo > Información** difiere, por ejemplo:
  - Para los modos Opt-in y Force-Protected: *Añadir restricción de fecha* muestra si el administrador ha habilitado esta política. Consulte Mejorar la seguridad añadiendo restricciones de fecha.
  - Para los modos Opt-in y Force-Protected: la información de propiedades sobre este documento de Office, como el autor o la fecha, están ocultas para mayor seguridad.

- Estado de solo lectura: consulte el apartado siguiente para obtener más información.

  NOTA:
  La opción *Proteger documento* en Archivo > Información está relacionada con Microsoft Office y no con el modo protegido de Data Guardian.

Si abre un documento de Office que muestra el modo de solo lectura, compruebe lo siguiente:

- Si *Guardar como protegido* no aparece en el panel izquierdo, el modo de solo lectura no está relacionado con la política de Data Guardian.
- Si el administrador define políticas para el modo Force-Protected con un mayor nivel de seguridad, los documentos no protegidos de Office se abrirán en modo de solo lectura.

  NOTA:
  En el caso de OneDrive, si abre un documento de Office protegido a través de **Archivo > Abrir > OneDrive** y el documento es de solo lectura, confirme que tiene instalado y configurado el cliente de sincronización OneDrive.

Trabajar con las opciones del menú Archivo

Esta tabla muestra las opciones del menú Archivo para documentos de Office. En función del nivel de seguridad, algunas de las opciones se atenúan.

NOTA:
Actualmente, los documentos de Office incrustados no son compatibles con el modo protegido de Office.

Menú Archivo	Modo Opt-in y documentos de Office protegidos	Modo Force-Protected para protegido y no protegido
Abra el archivo	**Los archivos se abren como de costumbre**	**Los documentos no protegidos se abren en modo de solo lectura.**
Guardar	• Opciones: El documento ya está protegido: esta opción guarda el documento como protegido. No protegido: esta opción guarda el documento como no protegido. Para protegerlo, haga clic en **Guardar como protegido**. • Documento de solo lectura: un cuadro de diálogo le avisa de que no puede guardar un documento no protegido. Se abrirá la ventana Guardar como y deberá guardarlo con un nombre diferente. • Archivo .xen: puede abrirlo y guardarlo en Modo protegido, pero entonces el archivo .xen se quita de la nube. El documento de Office tiene su extensión habitual, pero está protegido. **NOTA:** **En la unidad virtual, si hace clic con el botón derecho del mouse para crear un documento de Office, se crea un archivo .xen. Se debe guardar manualmente como protegido.**	• El documento está protegido. • Documento de solo lectura: puede editarlo, pero no puede guardar el original. Cuando hace clic en Guardar, se abre la ventana Guardar como protegido y debe guardarlo en Modo protegido con un nuevo nombre. • Documentos remotos: si se abre un documento en una ubicación remota y no está protegido, debe guardar el archivo en la unidad local para modificarlo y guardarlo. No se puede guardar en la ubicación remota. **NOTA:** **Al hacer clic en Guardar se abre la ventana Guardar como, y la única opción en el campo Guardar como tipo es Protegido de Office (documentos, presentación o libro).** • Archivo .xen: puede abrirlo y guardarlo en Modo protegido, pero entonces el archivo .xen desaparece de la nube. El documento de Office tiene su extensión habitual, pero está protegido.
Guardar como	**Tiene las opciones estándar (pero no el Modo protegido)**	**Deshabilitado**
Guardar como protegido	**La única opción en el campo Guardar como tipo es Protegido de Office**	**La única opción en el campo Guardar como tipo es Protegido de Office**
Imprimir	**Se pueden habilitar o atenuar en función de las políticas definidas por el administrador. Si la opción de menú está activada, es posible que una política ponga una marca de agua, que contiene el nombre de usuario, el nombre de dominio y la ID. de equipo, en cada página al imprimir.**	**En función de la política, esta opción puede estar habilitada o atenuada.** **Si la opción de menú está activada, es posible que una política ponga una marca de agua, que contiene el nombre de usuario, el nombre de dominio y la ID. de equipo, en cada página al imprimir.**
Compartir	**Habilitado**	**Deshabilitado**
Guardar y enviar (Office 2010)	**Habilitado**	**Deshabilitado** **Si la opción Imprimir está activada, puede seleccionar Imprimir para imprimir el documento como un archivo PDF.**
Exportar (Office 2013 y superior)	**Se pueden habilitar o atenuar en función de las políticas definidas por el administrador.**	**Se pueden habilitar o atenuar en función de las políticas definidas por el administrador.**
Exportación protegida (Office 2013 y superior)	Si la opción de menú Exportar aparece atenuada y la opción Exportación protegida está activada, los documentos se exportan con una marca de agua que contiene el nombre de usuario, el nombre de dominio y el ID. de equipo en cada página. **NOTA:** Si exporta un documento en modo protegido a un usuario externo, puede abrirlo y verlo, pero no exportarlo ni imprimirlo.	Si la opción de menú Exportar aparece atenuada y la opción Exportación protegida está activada, los documentos se exportan con una marca de agua que contiene el nombre de usuario, el nombre de dominio y el ID. de equipo en cada página. **NOTA:** Si exporta un documento en modo protegido a un usuario externo, puede abrirlo y verlo, pero no exportarlo ni imprimirlo.

Trabajar en línea con documentos de Office protegidos

Al crear documentos de Office protegidos, lo más recomendable es trabajar en línea debido a que se generan claves para esos documentos. Si es necesario recrear imágenes en su equipo y ha creado documentos de Office protegidos fuera de línea, asegúrese de comunicárselo su administrador.

Trabajar en línea con documentos protegidos habilitados para macros

En un documento protegido habilitado para macros, la macro existe pero está bloqueada. Sin embargo, actualmente, Data Guardian solo puede controlar un documento habilitado para macros después de que el nuevo documento protegido (.docm, .pptm, .xlsm) se haya cerrado y vuelto a abrir. Además, si guarda un documento protegido con una macro como no protegido, debe cerrarlo y volver a abrirlo para que la macro se ejecute.

Adjuntar un documento de Office protegido a un correo electrónico de Outlook

Cuando adjunte un documento de Office protegido a un correo electrónico de Outlook, seleccione **Insertar** en lugar de *Insertar como texto*. *Insertar como texto* pega el contenido del documento directamente en el cuerpo del correo electrónico y, de este modo, el contenido ya no está protegido.

Solución de problemas para el modo Opt-in

En Archivo > Información, si la opción Imprimir aparece atenuada significa que una política de Data Guardian ha desactivado la impresión para los documentos de Office protegidos. Sin embargo, cuando hace clic con el botón derecho del mouse en un archivo de Office protegido en el Explorador de Windows, la opción Imprimir no está atenuada. Sin embargo, si selecciona Imprimir, se produce lo siguiente:

- Word: un cuadro de diálogo indica que Word ha dejado de funcionar.
- Excel: un cuadro de diálogo indica que la política ha deshabilitado la opción Imprimir.
- Powerpoint: un cuadro de diálogo indica que la política ha deshabilitado la opción Imprimir. Si hace clic en Aceptar, se imprime una página de portada que indica que el documento está protegido.

Determinar qué documentos Modo Opt -in están protegidos

Si tiene activado el modo Force-Protected, todos los documentos de Office están protegidos. Si tiene activado el modo Opt-in y desea confirmar si el documento está protegido o no, ábralo y la barra de título lo mostrará como protegido.

Opciones de menú adicionales para documentos de Office protegidos

El tipo de documento de Office, protegido o no, puede afectar a lo siguiente.

Clic con el botón derecho del mouse > Proteger

Puede hacer clic con el botón derecho del mouse en un documento de Office y seleccionar **Proteger**. Debe agregar contenido con las opciones de menú para mostrar. No puede proteger un documento en blanco.

Propiedades del archivo > pestaña Dell Data Guardian

En los documentos de Office protegidos, puede hacer clic con el botón derecho del mouse y seleccionar **Propiedades**, y se mostrará una pestaña de **Dell Data Guardian** con información como el Id. y la clave de acceso del archivo y los datos de embargo.

Pegar

Si el administrador define una política de protección de documentos de Office:

- Puede copiar y pegar datos en el documento protegido original.
- No puede copiar o pegar datos desde un documento protegido a un documento desprotegido. No aparece nada en el Portapapeles y un mensaje de texto específico para empresas indica que no puede pegarlo en el documento no protegido o no administrado.

> **NOTA:**
> Si corta texto de un documento protegido y le aparece el mensaje en un documento desprotegido, haga clic en **Deshacer** en el documento protegido para recuperar el texto.

Arrastrar y soltar en Modo protegido

Puede arrastrar y soltar contenido en un documento de Word protegido. Actualmente, la opción de arrastrar y soltar está desactivada para los archivos Power Point y Excel.

Imprimir sobres y etiquetas

Si el administrador ha definido una política para agregar una marca de agua al imprimir un documento de Office protegido, siga estos pasos para imprimir sobres o etiquetas:

1 En un documento de Word, seleccione la pestaña **Correspondencia**.
2 Seleccione la opción **Sobres** o **Etiquetas**.
3 Después de introducir la dirección o el remite, haga clic en **Imprimir**.

> **NOTA: Si utiliza otra opción para imprimir y el administrador ha definido una política para agregar una marca de agua en los documentos de Office impresos, aparecerá una marca de agua en los sobres o etiquetas.**

Documentos de Office protegidos y su manipulación

Data Guardian puede escanear documentos de Office protegidos para detectar distintas formas de manipulación.

Si un usuario interno manipula un documento de Office protegido:

- Data Guardian puede reparar o restaurar la manipulación.
- Si la manipulación no se puede reparar, aparece un cuadro de diálogo que le indica que el archivo ha sido manipulado y que debe ponerse en contacto con el administrador.

Si un usuario no autorizado abre un documento de Office protegido, solo se mostrará la página de portada. Si el usuario no autorizado modifica la página de portada, Data Guardian restaurará la página de portada cuando un usuario autorizado la vuelva a guardar como protegida.

Usuarios externos y documentos de Office protegidos

Mejorar la seguridad añadiendo restricciones de fecha

Con Data Guardian, carga un documento de Office protegido en la nube y lo comparte:

- Todos los usuarios internos de Data Guardian pueden verlo.
- Según cuál sea la política, los usuarios externos también pueden verlo.

De manera opcional, para mejorar la seguridad con los usuarios externos, puede agregar una restricción de fecha para limitar el tiempo que un usuario externo puede ver un documento de Office protegido.

1 Seleccione **Archivo > Información > Restricción de fecha**.
2 Desde las opciones de la lista desplegable, seleccione Fecha y hora de inicio y finalización para que un usuario externo vea el documento.

> **NOTA:**
> La Fecha y hora de inicio puede ser posterior si desea enviar el documento pero desea evitar que el usuario externo lo vea hasta la fecha y hora programadas.

3 Haga clic en **Aceptar**.
El documento se guardará, se protegerá, se cerrará y se volverá a abrir.

> **NOTA:**
> Aunque modifique las fechas para un documento de Office no protegido y haga clic en Cancelar, Data Guardian protegerá el archivo.

NOTA:
Actualmente, si agrega restricciones de fecha a un documento de Office protegido y quiere guardarlo a una unidad de red, primero debe guardar el archivo de forma local y, después, copiarlo a la red.

Si un usuario externo abre un archivo después del rango de fecha y hora establecido, aparece un cuadro de diálogo indicando que el archivo tiene restricciones de acceso y que el usuario externo debe ponerse en contacto con el autor. El cuadro de diálogo no muestra ninguna fecha al usuario externo.

Si define la fecha de inicio de un archivo en una fecha u hora posteriores y el usuario externo abre el archivo antes de tiempo, aparece un cuadro de diálogo que indica que el archivo no se puede abrir hasta la fecha y la hora indicadas debido a restricciones de acceso.

Cómo trabajar sin una conexión a Internet

Sin una conexión a Internet, puede ver los archivos sincronizados en la nube en su unidad local mediante el Explorador de archivos. No obstante, la Unidad virtual DDG VDiskno se muestra. Además, los cambios no se sincronizarán en la nube hasta que se conecte a Internet.

Límite de caracteres para los nombres de ruta de acceso de carpeta

Los nombres de ruta de acceso de Windows tienen un límite de 248 caracteres.

En la nube no existe este límite. Por lo tanto, puede crear carpetas y subcarpetas con un nombre de ruta de acceso que supere dicho límite. Sin embargo, localmente, en Windows, si hay un nombre de ruta de acceso que supere el límite, no se crearán las carpetas. Por lo tanto, asegúrese de limitar los nombres de ruta de acceso de las carpetas y subcarpetas a 248 caracteres.

Dropbox for Business

Dropbox for Business tiene requisitos específicos. Consulte Instalar un cliente de sincronización de nube.

Ayuda del proveedor del almacenamiento en la nube

Antes de utilizar Data Guardian, obtenga la información necesaria sobre el proveedor del almacenamiento en la nube. El servicio de soporte de Dropbox for Business se encuentra en:

https://www.dropbox.com/help.

Aunque pueda cargar archivos en el sitio web del proveedor de almacenamiento en la nube, la práctica recomendada es trabajar con carpetas y archivos en la Unidad virtual DDG VDisk.

Conectar Data Guardian y Dropbox for Business

Si su compañía utiliza Dropbox for Business, deberá permitir que Data Guardian permanezca conectado.

Para conectar:

1 En la bandeja del sistema, haga clic en el icono de Data Guardian y, a continuación, seleccione **Dropbox > Conectar**.
2 En la ventana Autenticación de Dropbox, lea la información que se ofrece y, a continuación, haga clic en **Siguiente**.
3 Si ha vinculado sus cuentas de empresa y personales de Dropbox, se le indicará que seleccione una cuenta ahora. Debe seleccionar la cuenta de empresa.

4 Cuando se le solicite permitir que Data Guardian acceda a sus archivos y carpetas de Dropbox, haga clic en **Permitir**.
5 Haga clic en **Finalizar**.

Configurar la sincronización selectiva para carpetas

Para sincronizar carpetas selectivamente:

1 En la bandeja del sistema, haga clic en el icono de **Dropbox for Business**.
2 Haga clic en el icono **Configuración** y seleccione **Preferencias**.
3 Haga clic en la pestaña **Cuenta** y, a continuación, en **Sincronización selectiva**.
4 Seleccione solo las carpetas o las subcarpetas que desee sincronizar en su equipo.
5 Haga clic en **Actualizar**.
6 En el diálogo de confirmación Actualizar, haga clic en **Aceptar**.
7 En la ventana Preferencias de Dropbox, haga clic en **Aceptar**.
Se mostrará un elemento emergente en la bandeja del sistema que indicará que las carpetas se están sincronizando.

Su empresa determinará si solo puede tener una cuenta de empresa o si puede usar tanto la carpeta personal como la de empresa. Si desea carpetas preexistentes, con archivos personales o datos que no requieren cifrado, anule la selección de estas carpetas antes de instalar Data Guardian. De lo contrario, sus datos personales podrían cifrarse.

Usar el icono de la bandeja del sistema de Dropbox for Business

En la bandeja del sistema, haga clic en el icono de Dropbox.

- Para el sitio web, seleccione el icono del globo.

  NOTA:
  Si utiliza Chrome o Firefox para abrir Dropbox.com, asegúrese de cerrarlos después de terminar de trabajar con archivos y carpetas. El contenido se cifrará incluso al abrir otra pestaña en el navegador. Podría incluir el correo electrónico, un archivo adjunto o los que archivos que se cargan mediante el navegador.

- Para la carpeta, seleccione el icono de la carpeta Dropbox. Esto le redirige a la Unidad virtual DDG VDisk.

Usar el menú contextual de Dropbox for Business

Cuando Data Guardian está instalado, Dropbox for Business tiene un menú contextual en el Explorador de Windows.

NOTA:
Deberá conectar Data Guardian con Dropbox.

Para acceder al menú contextual, en el Explorador de Windows, abra una carpeta de Dropbox y haga clic con el botón derecho del mouse en un archivo. El icono de la nube tiene estas opciones:

- Enlace Compartir Dropbox seguro
- Ver en Dropbox.com
- Ver versiones anteriores

Usar las cuentas de empresa y personales de Dropbox

Si su empresa tiene Dropbox for Business y también permite que vincule una cuenta personal de Dropbox con la cuenta de empresa, asegúrese de que conoce y comprende las políticas que ha establecido su administrador para esas cuentas. Por ejemplo, una empresa puede establecer las políticas siguientes:

- Se cifran ambos, tanto los archivos personales como los de empresa.
  O bien
- Solo se cifran los archivos y las carpetas de empresa. Los archivos personales no se cifran.
  Por motivos de seguridad, su empresa puede contar con una política de auditoría. Los nombres de los archivos en la carpeta personal se registran y se envían al Dell Data Protection Server.

Si utiliza cuentas de empresa y personales de Dropbox, no guarde archivos de la empresa en su carpeta personal de Dropbox.

Descifrar carpetas en una cuenta personal

Si una cuenta personal se cifra accidentalmente, el administrador puede otorgar un acceso temporal para permitirle administrar el cifrado de sus carpetas. Anule la selección de las carpetas que deben descifrarse. Además, para quitar carpetas de la sincronización puede desvincularlas de la cuenta o desincronizar las carpetas personales que deben permanecer descifradas.

OneDrive for Business/OneDrive unificado

NOTA:
Data Guardian no es compatible con Microsoft Office 365.

NOTA:
OneDrive for Business no admite compartir datos.

Ayuda del proveedor del almacenamiento en la nube

Antes de utilizar Data Guardian, obtenga la información necesaria sobre el proveedor del almacenamiento en la nube. El servicio de soporte de OneDrive for Business se encuentra en:

http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Aunque pueda cargar archivos en el sitio web del proveedor de almacenamiento en la nube, la práctica recomendada es trabajar con carpetas y archivos en la Unidad virtual DDG VDisk.

Configurar la sincronización selectiva para carpetas

Para sincronizar carpetas selectivamente:

1. En la bandeja del sistema, haga clic con el botón derecho del mouse en el icono **OneDrive for Business/OneDrive unificado** y haga clic en **Sincronizar una nueva biblioteca**.
2. Introduzca la URL de la biblioteca.
3. Seleccione **Sincronizar ahora**.
4. Seleccione **Mostrar mis archivos**.

Usar el icono de la bandeja del sistema de OneDrive for Business

En la bandeja del sistema:

- Para el sitio web, haga clic con el botón derecho del mouse y seleccione **Ir a OneDrive.com**.
- Para la carpeta, haga clic con el botón derecho del mouse y seleccione **Abrir la carpeta de OneDrive for Business**. Esta acción le redirige a la Unidad virtual DDG VDisk.

Consideraciones de seguridad con Data Guardian y OneDrive o OneDrive for Business

Dell Data Guardian cifra archivos y carpetas para que los datos estén seguros. Como Data Guardian funciona con clientes de sincronización, tenga en cuenta estas consideraciones.

- Cuando descargue, no seleccione Cancelar. Esto provocará un error. Si desea eliminar el archivo, espere hasta que la descarga haya finalizado.
- Para Windows 8.1, Microsoft OneDrive dispone de archivos de marcador de posición que parecen existir en el cliente de sincronización aunque no se descargan realmente. Por lo tanto, Dell Data Guardian no puede cifrarlos. Si abre un archivo de marcador de posición, Data Guardian mostrará un cuadro de diálogo que indica que el archivo no estará protegido. Puede hacer clic con el botón derecho del mouse y seleccionar **Descargar** y, a continuación, **Data Guardian** lo convierte en un archivo .xen.

Dropbox

Ayuda del proveedor del almacenamiento en la nube

Antes de utilizar Data Guardian, obtenga la información necesaria sobre el proveedor del almacenamiento en la nube. La asistencia de Dropbox se encuentra en https://www.dropbox.com/help.

Aunque pueda crear archivos en la nube o cargar archivos en el sitio web del proveedor de almacenamiento en la nube, lo mejor es trabajar con carpetas y archivos en la Unidad virtual DDG VDisk.

NOTA:

Para Dropbox y Data Guardian, si crea un archivo de Office en la nube y lo sincroniza, se cifra como un archivo .xen. Por lo tanto, en la unidad virtual, se abre en modo de solo lectura. No se puede editar.

Si elimina todas las carpetas en la unidad virtual, los archivos se eliminan pero las carpetas pueden permanecer. Si es así, elimine las carpetas en la nube.

Configurar la sincronización selectiva para carpetas

Para sincronizar carpetas selectivamente:

1. En la bandeja del sistema, haga clic en el icono de **Dropbox**.
2. Haga clic en el icono **Configuración** y seleccione **Preferencias**.
3. Haga clic en la pestaña **Cuenta** y, a continuación, en **Sincronización selectiva**.
4. Seleccione solo las carpetas o las subcarpetas que desee sincronizar en su equipo.
5. Haga clic en **Actualizar**.
6. En el diálogo de confirmación Actualizar, haga clic en **Aceptar**.
7. En la ventana Preferencias de Dropbox, haga clic en **Aceptar**.
   Se mostrará un elemento emergente en la bandeja del sistema que indicará que las carpetas se están sincronizando.

Usar el icono de la bandeja del sistema de Dropbox

En la bandeja del sistema, haga clic en el icono de Dropbox.

- Para el sitio web, seleccione el icono del globo.

NOTA:
Si utiliza Chrome o Firefox para abrir Dropbox.com, asegúrese de cerrarlos después de terminar de trabajar con archivos y carpetas. El contenido se cifrará incluso al abrir otra pestaña en el navegador. Podría incluir el correo electrónico, un archivo adjunto o los que archivos que se cargan mediante el navegador.

- Para la carpeta, seleccione el icono de la carpeta Dropbox. Esto le redirige a la Unidad virtual DDG VDisk.

Consideraciones de seguridad con Data Guardian y Dropbox

Si la ejecución se realiza en una máquina virtual, no arrastre un archivo desde el escritorio del servidor al navegador. El archivo no estará protegido. Realizar una de estas acciones: en el navegador, utilice la opción Cargar o, en el escritorio, arrastre el archivo hasta la Unidad virtual DDG VDisk.

Preguntas más frecuentes de Dropbox

Pregunta

Mi cuenta de Dropbox tiene muchos archivos en conflicto. Cuando los borro de la nube, se siguen creando.

Respuesta

A veces, cuando ya se ha compartido una carpeta y se activan varias cuentas de Data Guardian al mismo tiempo, estos archivos se ven como si se hubieran creado al mismo tiempo. En un esfuerzo por conservar el original, Dropbox crea varios archivos con el mismo nombre y del mismo tipo, y los coloca en la nube. Por lo tanto, Data Guardian permite que se creen todos los archivos sin interferir.

Solución

1 Todas las personas que estén compartiendo el archivo deben colaborar anulando la selección de la carpeta de sincronización de la aplicación de Dropbox. Consulte Dropbox for Business.
2 Después de que se han eliminado todos los archivos y la carpeta de cada uno de los equipos locales, una persona debe acceder a la nube y eliminar los archivos duplicados.

Luego, cada persona puede utilizar la sincronización selectiva para volver a agregar la carpeta que desee sincronizar.

Box

Ayuda del proveedor del almacenamiento en la nube

Antes de utilizar Data Guardian, obtenga la información necesaria sobre el proveedor del almacenamiento en la nube. Puede encontrar la asistencia de Box en https://support.box.com/home.

Aunque pueda cargar archivos en el sitio web del proveedor de almacenamiento en la nube, la práctica recomendada es trabajar con carpetas y archivos en la Unidad virtual DDG VDisk.

NOTA:
Si usa Internet Explorer para cargar archivos al proveedor de almacenamiento en la nube de Box o abre un archivo, puede que la ventana del explorador de archivos tenga un retraso.

NOTA:
Box Tools y Box Edit no son compatibles con Data Guardian. Utilizar Box Tools puede causar un error de pantalla azul.

Configurar la sincronización selectiva para carpetas

Para sincronizar carpetas selectivamente:

1 En la bandeja del sistema, haga clic con el botón derecho del mouse en el icono de Box y seleccione **Abrir el sitio web de Box**.

2 En el sitio web del cliente de sincronización en la nube, haga clic con el botón derecho del mouse en una carpeta y seleccione **Sincronizar carpeta con el equipo**.

3 En la ventana Sincronizar carpeta, haga clic en **Sincronizar carpeta**.

El icono de la bandeja del sistema indica que se está aplicando la configuración. Esto puede tardar varios minutos.

4 Cuando haya finalizado, vaya a **Explorador de Windows** > **Sincronización de Box**. Las carpetas sincronizadas se muestran con una marca de verificación.

Usar el icono de la bandeja del sistema de Box

En la bandeja del sistema, haga clic con el botón derecho del mouse en el icono de Box.

- Para el sitio web: seleccione **Abrir sitio web de Box**.
- Para la carpeta: seleccione la carpeta **Abrir sincronización de Box**. Esta acción le redirige a la Unidad virtual DDG VDisk.

Preguntas más frecuentes del cliente de sincronización de Box

Pregunta

Estoy utilizando el cliente de sincronización de Box. Cree una nueva carpeta local y agregué algunos archivos. El cliente de sincronización parece estar funcionando, pero no se ha creado nada en la nube.

Respuesta

El cliente de sincronización de Box puede necesitar tiempo para recopilar información acerca de las nuevas carpetas y archivos. El proceso puede tardar varios minutos en comparación con otros clientes de sincronización. Asegúrese de esperar varios minutos para que el cliente de sincronización pueda completar el proceso antes de crear nuevas carpetas y archivos.

Pregunta

Estoy utilizando el cliente de sincronización de Box. Me quedé sin espacio en mi partición primaria, así que lo moví a otra unidad. Ahora la carpeta Mis archivos de Box tiene una o más carpetas creadas y con el nombre **Nueva carpeta**.

Respuesta

Actualmente, cuando se sincronizan archivos entre dos equipos con el mismo recurso compartido de archivos, si una persona mueve esa carpeta a otro lugar, cualquier carpeta nueva que otras personas creen en ese recurso compartido de archivos creará una carpeta vacía llamada **Nueva carpeta**.

Solución

Elimine la nueva carpeta directamente desde la nube. Se eliminará de todos los sistemas que comparten esa carpeta.

Consideraciones de seguridad con Data Guardian y Box

Si crea un archivo en el sitio web de Box Cloud, se sincronizará. No obstante, se descargará como un archivo cifrado.

Internet Explorer puede provocar retrasos cuando cargue o abra un archivo en Box.

Google Drive

Ayuda del proveedor del almacenamiento en la nube

Antes de utilizar Data Guardian, obtenga la información necesaria sobre el proveedor del almacenamiento en la nube. La asistencia de Google Drive se encuentra en https://support.google.com/drive/?hl=en#topic=14940.

Aunque pueda cargar archivos en el sitio web del proveedor de almacenamiento en la nube, la práctica recomendada es trabajar con carpetas y archivos en la Unidad virtual DDG VDisk.

Configurar la sincronización selectiva para carpetas

Para sincronizar carpetas selectivamente:

1 En la bandeja del sistema, haga clic en el icono de **Google Drive**.
2 Seleccione el icono Configuración.
3 Seleccione **Preferencias**.
4 Para sincronizar de forma selectiva, haga clic en **Solo estas carpetas**.
5 Borre la casilla de verificación para las carpetas que no deban estar protegidas en la nube.
6 Haga clic en **Aplicar**.
7 Para confirmar, haga clic en **Continuar**.

Usar el icono de la bandeja del sistema de Google Drive

En la bandeja del sistema, haga clic en el icono de Google Drive.

- Para el sitio web: seleccione **Visitar Google Drive en la web**.
- Para la carpeta: seleccione la carpeta **Abrir Google Drive**. Esta acción le redirige a la Unidad virtual DDG VDisk

Consideraciones de seguridad con Data Guardian y Google Drive

Data Guardian cifra archivos y carpetas para proteger los datos. Como Data Guardian funciona con clientes de sincronización, tenga en cuenta estas consideraciones.

- La política de seguridad corporativa prohíbe el uso de Google Docs con Data Guardian. Cuando instale Data Guardian, un cuadro de diálogo le informará de esta política. Para obtener más información, póngase en contacto con su administrador de TI.

  Google Drive contiene una aplicación de Google Docs que permite a los usuarios colaborar con documentos en tiempo real. No obstante, la colaboración se produce en un servidor de Google y los archivos no están cifrados. Para Windows y Data Guardian, cualquier Google Docs que cree se mostrará en las carpetas de clientes de sincronización de Google Docs.

  Sin embargo, si abre la carpeta, un cuadro de diálogo le advertirá de que Data Guardian no puede cifrar ese documento. Además, para asegurar la protección de los datos, es posible que su administrador ejecute informes para identificar Google Docs que están siendo sincronizados para ayudar a proporcionar seguridad.
- Google Drive tiene ambas opciones **Eliminar** (tira el documento a la papelera) y **Suprimir**. Google Drive con Data Guardian tiene únicamente la opción de Suprimir, para ser consistente con las otras funciones de Data Guardian.

NOTA:
Si elimina varios archivos de la unidad virtual de Data Guardian y continúan mostrándose algunos en el navegador o en la línea de comandos, elimínelos desde el navegador o desde la línea de comandos.

- En Google Drive es posible que le aparezca una advertencia que indique que se han quitado todas las propiedades cuando copie archivos a la Unidad virtual DDG VDisk. Estos son atributos de seguridad.

OneDrive

NOTA:
Data Guardian no es compatible con Microsoft Office 365.

Ayuda del proveedor del almacenamiento en la nube

Antes de utilizar Data Guardian, obtenga la información necesaria sobre el proveedor del almacenamiento en la nube. Asistencia de OneDrive en http://windows.microsoft.com/en-us/onedrive/onedrive-help#onedrive=other.

Aunque pueda cargar archivos en el sitio web del proveedor de almacenamiento en la nube, la práctica recomendada es trabajar con carpetas y archivos en la Unidad virtual DDG VDisk.

Configurar la sincronización selectiva para carpetas

Para sincronizar carpetas selectivamente:

1. En la bandeja del sistema, haga clic con el botón derecho del mouse en el icono de **OneDrive** y haga clic en **Configuración**.
2. Seleccione la pestaña **Elegir carpetas** y, a continuación, haga clic en **Elegir carpetas**.
3. Después, seleccione **Elegir carpetas para sincronizar**.
4. Se mostrará una lista de carpetas. Marque o desmarque las casillas para sincronizar las carpetas correspondientes. Haga clic en **Aceptar**.
5. Haga clic en **Aceptar**.
6. El icono de la bandeja del sistema indica que se está aplicando la configuración. Esto puede tardar varios minutos.
7. Cuando haya finalizado, vaya a **Explorador de Windows** > **OneDrive**. Las carpetas sincronizadas se muestran con una marca de verificación.

Usar el icono de la bandeja del sistema de OneDrive

En la bandeja del sistema:

- Para el sitio web, haga clic con el botón derecho del mouse y seleccione **Ir a OneDrive.com**.
- Para la carpeta, haga clic con el botón derecho del mouse y seleccione **Abrir la carpeta de OneDrive** . Esta acción le redirige a la Unidad virtual DDG VDisk.

Consideraciones de seguridad con Data Guardian y OneDrive o OneDrive for Business

Consulte Consideraciones de seguridad con Data Guardian y Clientes de sincronización.

Comprender los elementos del menú de la bandeja del sistema de Data Guardian

Pantalla Detalles

La pantalla Detalles de Data Guardian proporciona información muy útil como, por ejemplo:

- Para obtener soporte técnico, puede proporcionar información sobre el estado o la versión.
- Para ver un nombre de archivo sin texto confuso que esté asociado con un archivo .xen, seleccione **Archivos** > **Estado del archivo**.
- Para buscar un archivo por el nombre, seleccione Copiar en la parte inferior derecha y pegue el contenido en un archivo Word.
- Para ver quién es el propietario de la carpeta, seleccione Carpetas y desplácese hasta la columna PROPIETARIO DE LA CARPETA.

Para acceder a la pantalla Detalles:

Haga clic en el icono de la bandeja del sistema de **Data Guardian** y, a continuación, haga clic en **Detalles...**

La esquina superior izquierda de la pantalla Detalles mostrará la siguiente información:

Estado del servicio: estado del servicio de Windows de Data Guardian. Los valores posibles son: Detenido, InicioPendiente, DetenidoPendiente, En ejecución, ContinuarPendiente, EnPausaPendiente, En pausa

Estado de ejecución: el estado de activación del dispositivo. Los valores son: Activo, Reactivado, Suspendido, Suspendiendo

Modo de usuario: usuario interno; un usuario con una dirección en este dominio

Usuario externo: un usuario con una dirección fuera de este dominio

Correo electrónico de registro: para los usuarios internos, es el correo electrónico del dominio. Para los usuarios externos, este es el correo electrónico con el que se registraron.

URL del servidor: el DDP EE Server/VE Server que se comunica con este cliente.

Última modificación de la política: fecha y marca de tiempo de la última vez que el cliente usó y modificó la política.

Versión de la política: versión de la política generada por DDP EE Server/VE Server.

El área de **Archivos** de la pantalla Detalles muestra la información siguiente:

Nombre: nombre del archivo

Nube: enumera la ofuscación de nombres de archivos o si el archivo está *Desprotegido*.

Estado del archivo: este valor indica el propietario de la carpeta. El valor lo determina la Id. de clave.

Estado del proceso: indica si el archivo necesita una clave o si está *Completo*.

Empresa: indica el servidor predeterminado. Si se muestra el mensaje *Error: la clave no pertenece a su servidor* en esta columna, indica que la clave no pertenece a su servidor de empresa. La clave para un archivo cifrado debe pertenecer al servidor de su empresa.

Clave: id. de clave asignada a esta carpeta (los archivos nuevos usan esta clave para el cifrado).

Carpeta: el nombre de la ruta de acceso completo de la carpeta.

Última modificación: la fecha de modificación del archivo.

Estado de persistencia: esto indica si el archivo está en un disco.

Lectura de archivos XEN: *Verdadero* o *Falso*.

Explorador creado: *Verdadero* o *Falso*.

Para los archivos de registro, haga clic en **Ver registro** en la esquina inferior izquierda de la pantalla Detalles.

NOTA:
Los archivos de registro también se encuentran en **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.**

El área de **Carpetas** de la pantalla Detalles muestra la información siguiente:

Nombre: nombre de la carpeta

Clave: id. de clave asignada a esta carpeta (los archivos nuevos usan esta clave para el cifrado).

Cliente de sincronización: el último cliente de sincronización que sincronizó esa carpeta (Consulte Clientes de sincronización en la nube).

Propiedad de la carpeta: este valor indica el propietario de la carpeta. El valor lo determina la Id. de clave.

Reemplazar: las opciones son *Ninguno* y *Ya existente*. Los archivos preexistentes no están protegidos. También, si tiene acceso a Administración de carpetas y ha desprotegido algunos archivos, esta columna indica que no están protegidos.

Tipo de ofuscación: si su empresa administra el almacenamiento en la nube, se trata de una política definida en cada carpeta que indica qué tipo de archivos .xen se crearán en la nube. Esta es una política que establece su administrador. Si el administrador selecciona *Solo extensión*, se mostrará el propio nombre del archivo con la extensión ".xen". Si el administrador selecciona *Guid*, se mostrará el nombre del archivo codificado con la extensión ".xen". Esta es una configuración de la política que tiene efecto en carpetas nuevas solamente. El valor predeterminado es *Solo extensión*.

Menú Administrar carpetas

Es posible que algunos administradores necesiten compartir temporalmente carpetas de solución de problemas con más de un usuario. Puede solicitar permisos al administrador para la opción Administrar carpetas. Normalmente, se trata de una opción temporal.

Comprobar si existen actualizaciones de políticas

Si el administrador modifica una política y le notifica de una actualización de políticas, vaya a la bandeja del sistema de Windows, haga clic en el icono de **Dell Data Protection | Data Guardian** y seleccione **Comprobar si existen actualizaciones de políticas**.

Si el administrador modifica una directiva para proteger los archivos creados en Microsoft Word, debe cerrar el programa para que pueda aplicarse la actualización.

Localizar archivos de registro

Su administrador puede solicitar archivos de registro para solución de problemas.

Para localizar archivos de registro:

1 Navegue hasta
2 Seleccione **Xendow.service.log**.

NOTA:
Cuando Xendow.Service.log alcanza 3 MB, se guarda como Xendow.Service1.log y, a continuación, como Xendow.Service2.log.

Actualizar Data Guardian

La práctica recomendada es desinstalar la versión anterior y, a continuación, instalar la versión actual. Consulte Desinstalar Data Guardian.

Proporcionar comentarios a Dell

Si su administrador ha habilitado una política de comentarios, puede proporcionar comentarios a Dell acerca de este producto. El breve formulario incluye dos preguntas sobre su nivel de satisfacción, con escalas de clasificación (donde 10 indica el nivel de satisfacción más alto) y un campo para comentarios.

Para tener acceso al formulario, haga clic en el icono de Data Guardian de la bandeja del sistema y seleccione **Enviar retroalimentación**.

Si esta función no está habilitada por una política, la opción no se mostrará.

Posibles problemas de activación: nube y Office protegidos

Si ha instalado Data Guardian, pero el icono de Data Guardian de la bandeja del sistema no tiene una marca de verificación verde  , tenga en cuenta lo siguiente en función de si tiene cifrado en la nube, Office protegido o ambos:

- El acceso está bloqueado a los sitios web de sincronización en la nube
- La conexión de las aplicaciones de sincronización en la nube con sus servicios web está bloqueada
- Las carpetas locales sincronizadas no se actualizan durante este tiempo
- Data Guardian puede convertir los documentos de Office existentes en modo protegido antes de que lo active. Si es así, al abrir un documento de Office, se mostrará una página de portada con información para activarlo.

Realice una de estas opciones:

- Reinicie y vuelva a iniciar sesión con un sufijo UPN, por ejemplo, user_name@domain.com.
- Confirme con su administrador si debe seleccionar la casilla de verificación **Habilitar la verificación de confianza en SSL** cuando instale Data Guardian.
- Póngase en contacto con el administrador del sistema por si debe tener el equipo configurado para activarlo manualmente. Consulte Activar Data Guardian.

Activar Data Guardian

Normalmente, Data Guardian se activa automáticamente después de instalar y reiniciar. Si el administrador le pide que lo active manualmente, siga estos pasos:

1 Inicie sesión en Windows.

En la bandeja del sistema, se muestra el icono de un escudo con una marca de verificación naranja.

2 Haga clic en el icono de **Data Guardian** en la bandeja del sistema y, a continuación, seleccione **Activación de usuario**.

3 Introduzca el correo electrónico y la contraseña de su dominio y haga clic en **Activar**.

Si es un usuario interno (con una dirección de correo electrónico del dominio), ignore el botón Registrar. Únicamente deben registrarse los usuarios externos.

Cuando se complete la activación, se mostrará una marca de verificación verde en el icono  de la bandeja del sistema de Data Guardian.

4 Confirme el estado de su modo de usuario. Haga clic en el icono de la bandeja del sistema y seleccione **Detalles**.

5 En la parte superior, confirme el Modo de usuario:

Interno: un usuario con una dirección de correo electrónico en el dominio de la empresa.

Externo: un usuario con una dirección de correo electrónico que no es del dominio. Para obtener más información, consulte Usar Data Guardian como usuario externo.

Tareas del usuario: Office protegido sin cifrado en la nube

El administrador ya ha configurado las políticas de Data Guardian para proteger documentos de Office.

NOTA:
Si su empresa también administra su cliente de sincronización en la nube, consulte Tareas del usuario: cifrado en la nube y Office protegido.

Descripción general de las tareas

Esta introducción resume la secuencia para instalar y utilizar Data Guardian.

Instalar Data Guardian

Tarea	Descripción	Para obtener más información
Instalar Data Guardian	Determine lo siguiente: El usuario debe instalar Data Guardian El administrador ya ha instalado Data Guardian; continúe con el siguiente paso.	El usuario es el encargado de instalar; consulte Instalar Data Guardian en Windows. Reinicie y continúe con el siguiente paso.
Confirme el estado de activación	Confirme en la bandeja del sistema que el icono de Data Guardian tiene una marca de verificación verde  .	Si el icono tiene un signo de exclamación naranja, consulte Posibles problemas de activación: Office protegido.

Usar Data Guardian

Tarea	Descripción	Para obtener más información
Ver el menú de la bandeja del sistema	Ofrece información útil acerca de archivos, carpetas y solución de problemas.	Comprender los elementos del menú de la bandeja del sistema de Data Guardian
Proteja los documentos de Office y los documentos habilitados para macros si la política está activada	Proteja un documento de Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) cuando lo cree. De este modo, serán seguros cuando los comparta con otros o los almacene en un medio extraíble.	Utilizar Documentos de Office con el Modo protegido de Data Guardian • Observar opciones del menú Archivo para determinar el nivel de seguridad de los documentos de Office • Trabajar con las opciones del menú Archivo
Compartir una carpeta con otros usuarios para colaborar en archivos	Comparta una carpeta con: Usuario interno (con una dirección de correo electrónico del dominio)	Usuario interno: consulte la ayuda en línea para su proveedor de almacenamiento en la nube. Usuario externo: consulte Usar Data Guardian como usuario externo.

Tarea	Descripción	Para obtener más información
	Usuario externo (con una dirección de correo electrónico que no es del dominio); coordínese con su administrador.	

NOTA:

Si abre un documento de Office y aparece una página de portada con información de activación o instalación, puede deberse a que el administrador haya definido políticas para proteger documentos de Office. Confirme que Data Guardian está instalado y activado. Consulte Posibles problemas de activación: Office protegido.

Instalar Data Guardian para documentos Office protegidos

Instalar Data Guardian en Windows

Para instalar Data Guardian, debe ser un administrador local en el equipo.

El equipo debe tener una letra alfabética disponible para asignarla a una unidad de disco.

Después de que se instale Data Guardian, esté preparado para reiniciar el equipo.

1. Para descargar el instalador de Data Guardian, vaya a la ubicación especificada por su administrador.
2. En función de su sistema operativo, seleccione el instalador de 32 bits o 64 bits, que normalmente aparece como **setup32.exe** o **setup64.exe**, y cópielo en el equipo local.
3. Haga doble clic en el archivo para iniciar el instalador.
4. Si se muestra un aviso de seguridad, haga clic en **Ejecutar**.
5. Seleccione un idioma y haga clic en **Aceptar**.
6. Si se le solicita que instale el Paquete redistribuible de Microsoft Visual C++ 2010 o Microsoft .Net Framework 4.0 Client Profile, haga clic en OK.
7. En la ventana de Bienvenida, haga clic en **Siguiente**.
8. Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.
9. En la pantalla Carpeta de destino, haga clic en **Siguiente** para instalar en la ubicación predeterminada de **C:\Archivos de programa\Dell \Dell Data Protection\Dell Data Guardian\.**

   En **C:**, no instale Data Guardian en las carpetas de los usuarios o de Windows ni en la raíz de cualquier unidad. Se mostrará un error.
10. En el campo `Nombre del servidor:`, introduzca el nombre del servidor con el que se comunicará este equipo, como, por ejemplo, servidor.dominio.com. No es necesario incluir www o http(s). Esta información la proporciona el administrador.

    No desmarque la casilla *Activar verificación de confianza en SSL* a menos que lo indique el administrador.
11. Haga clic en **Siguiente**.
12. En la pantalla Confirmar información del servidor de activación, confirme si la dirección URL del servidor es correcta. El instalador añade www o http(s) y el puerto. Haga clic en **Siguiente**.
13. En la ventana Tipo de administración, seleccione esta opción:
    - Usuario interno: un usuario con una dirección de correo electrónico en el dominio de la empresa.
14. Haga clic en **Instalar** para comenzar la instalación.

    Se mostrará una ventana de estado que muestra el progreso de la instalación.
15. Cuando se muestre la pantalla Instalación completa, haga clic en **Finalizar**.
16. Haga clic en **Sí** para reiniciar.

    La instalación de Data Guardian se ha completado.
17. Después de reiniciarlo, confirme en la bandeja del sistema que el icono de Data Guardian tiene una marca de verificación verde  .

Utilizar Documentos de Office con el Modo protegido de Data Guardian

Con el fin de mejorar la seguridad de empresa, el administrador puede habilitar una política para proteger archivos de estas aplicaciones de Office:

- .docx, .pptx, .xlsx
- .docm, .pptm, .xlsm

Si una persona no autorizada accede a un archivo protegido, el archivo permanece cifrado, por ejemplo, cuando:

- Se adjunta a un correo electrónico
- Se mueve a un navegador, en algunos clientes de sincronización en la nube puede hacer clic con el botón derecho del mouse en un nombre de archivo y seleccionar **Mover**.
- Se comparte en la red
- Se sube a un proveedor de almacenamiento en la nube
- Se almacena en un medio extraíble

Para documentos de Office, puede mostrarse una página de portada con instrucciones para la instalación o activación de Data Guardian, por ejemplo:

- Es necesario instalar Data Guardian.
- Es necesario activar Data Guardian.
- Abra un documento de Office protegido en la nube.
- Ha descargado un archivo Office desde su equipo que dispone de Data Guardian a un dispositivo personal que no lo tiene.
- Un usuario no autorizado accede a uno de los archivos de Office: la página de portada muestra un mensaje específico para empresas, pero el usuario no puede ver el contenido del archivo.

Si su empresa utiliza el Modo protegido de Data Guardian, consulte lo siguiente:

- Observar opciones del menú Archivo para determinar el nivel de seguridad de los documentos de Office
- Trabajar con las opciones del menú Archivo
- Determinar qué documentos Modo Opt -in están protegidos
- Opciones de menú adicionales para documentos de Office protegidos
- Usuarios externos y documentos de Office protegidos

Observar opciones del menú Archivo para determinar el nivel de seguridad de los documentos de Office

Para determinar si el administrador ha habilitado políticas de Data Guardian, abra un documento de Office y seleccione **Archivo**. Si se muestra *Guardar como protegido* en el panel izquierdo, significa que dispone de protección adicional en los documentos de Office.

Para determinar el nivel de seguridad, fíjese en las opciones que están activadas o desactivadas:

- **Modo Opt-in**: dispone de varias opciones para elegir qué documentos de Office proteger.
  - Las opciones *Guardar como* y *Guardar como protegido* están activadas: si decide proteger un documento de Office, seleccione **Guardar como protegido**.
  - Las opciones *Imprimir* y *Exportar* se pueden activar o desactivar en función de las políticas.
  - La opción *Compartir* (*Guardar y enviar* para Office 2010) está activada.
  - Carpeta **Documentos > Documentos seguros**: con el Modo Opt-in (pero no con el modo Force-Protected) se añade una carpeta de Documentos seguros a la raíz de la carpeta Documentos. Los documentos de Office incluidos en esta carpeta están cifrados. Si

quita un documento de Office protegido de esta carpeta, sigue cifrado. Si cambia el nombre de la carpeta, todo su contenido sigue cifrado. Si elimina la carpeta, se vuelve a crear.

- **Modo Force-Protected**: la empresa requiere un nivel de seguridad mayor.
  - La opción *Guardar como* está desactivada y la opción *Guardar como protegido* está activada: debe guardar todos los documentos de Office en Modo protegido.
  - Las opciones *Imprimir* y *Exportar* se pueden activar o desactivar en función de las políticas.
  - La opción *Compartir* (*Guardar y enviar* para Office 2010) está desactivada.

    NOTA:
    Con el modo Force-Protected, la política también permite horas específicas para realizar un barrido de su equipo para localizar cualquier archivo de Office sin protección y cambiarlos al modo protegido. Debe haber iniciado sesión y estar conectado a la red para que Data Guardian realice el barrido de los archivos de Office sin protección.

- Si selecciona **Guardar como protegido**, la única opción en el campo *Guardar como tipo* es *Protegido de Office*.

- **Archivo > Información** difiere, por ejemplo:
  - Para los modos Opt-in y Force-Protected: *Añadir restricción de fecha* muestra si el administrador ha habilitado esta política. Consulte Mejorar la seguridad añadiendo restricciones de fecha.
  - Para los modos Opt-in y Force-Protected: la información de propiedades sobre este documento de Office, como el autor o la fecha, están ocultas para mayor seguridad.
  - Estado de solo lectura: consulte el apartado siguiente para obtener más información.

    NOTA:
    La opción *Proteger documento* en Archivo > Información está relacionada con Microsoft Office y no con el modo protegido de Data Guardian.

Si abre un documento de Office que muestra el modo de solo lectura, compruebe lo siguiente:

- Si *Guardar como protegido* no aparece en el panel izquierdo, el modo de solo lectura no está relacionado con la política de Data Guardian.
- Si el administrador define políticas para el modo Force-Protected con un mayor nivel de seguridad, los documentos no protegidos de Office se abrirán en modo de solo lectura.

  NOTA:
  En el caso de OneDrive, si abre un documento de Office protegido a través de **Archivo > Abrir > OneDrive** y el documento es de solo lectura, confirme que tiene instalado y configurado el cliente de sincronización OneDrive.

Trabajar con las opciones del menú Archivo

Esta tabla muestra las opciones del menú Archivo para documentos de Office. En función del nivel de seguridad, algunas de las opciones se atenúan.

NOTA:
Actualmente, los documentos de Office incrustados no son compatibles con el modo protegido de Office.

Menú Archivo	Modo Opt-in y documentos de Office protegidos	Modo Force-Protected para protegido y no protegido
Abra el archivo	**Los archivos se abren como de costumbre**	**Los documentos no protegidos se abren en modo de solo lectura.**
Guardar	• Opciones: El documento ya está protegido: esta opción guarda el documento como protegido. No protegido: esta opción guarda el documento como no protegido. Para protegerlo, haga clic en **Guardar como protegido**. • Documento de solo lectura: un cuadro de diálogo le avisa de que no puede guardar un documento no protegido. Se abrirá la ventana Guardar como y deberá guardarlo con un nombre diferente. • Archivo .xen: puede abrirlo y guardarlo en Modo protegido, pero entonces el archivo .xen se quita de la nube. El documento de Office tiene su extensión habitual, pero está protegido. **NOTA:** **En la unidad virtual, si hace clic con el botón derecho del mouse para crear un documento de Office, se crea un archivo .xen. Se debe guardar manualmente como protegido.**	• El documento está protegido. • Documento de solo lectura: puede editarlo, pero no puede guardar el original. Cuando hace clic en Guardar, se abre la ventana Guardar como protegido y debe guardarlo en Modo protegido con un nuevo nombre. • Documentos remotos: si se abre un documento en una ubicación remota y no está protegido, debe guardar el archivo en la unidad local para modificarlo y guardarlo. No se puede guardar en la ubicación remota. **NOTA:** **Al hacer clic en Guardar se abre la ventana Guardar como, y la única opción en el campo Guardar como tipo es Protegido de Office (documentos, presentación o libro).** • Archivo .xen: puede abrirlo y guardarlo en Modo protegido, pero entonces el archivo .xen desaparece de la nube. El documento de Office tiene su extensión habitual, pero está protegido.
Guardar como	**Tiene las opciones estándar (pero no el Modo protegido)**	**Deshabilitado**
Guardar como protegido	**La única opción en el campo Guardar como tipo es Protegido de Office**	**La única opción en el campo Guardar como tipo es Protegido de Office**
Imprimir	**Se pueden habilitar o atenuar en función de las políticas definidas por el administrador. Si la opción de menú está activada, es posible que una política ponga una marca de agua, que contiene el nombre de usuario, el nombre de dominio y la ID. de equipo, en cada página al imprimir.**	**En función de la política, esta opción puede estar habilitada o atenuada.** **Si la opción de menú está activada, es posible que una política ponga una marca de agua, que contiene el nombre de usuario, el nombre de dominio y la ID. de equipo, en cada página al imprimir.**
Compartir	**Habilitado**	**Deshabilitado**
Guardar y enviar (Office 2010)	**Habilitado**	**Deshabilitado** **Si la opción Imprimir está activada, puede seleccionar Imprimir para imprimir el documento como un archivo PDF.**
Exportar (Office 2013 y superior)	**Se pueden habilitar o atenuar en función de las políticas definidas por el administrador.**	**Se pueden habilitar o atenuar en función de las políticas definidas por el administrador.**
Exportación protegida (Office 2013 y superior)	Si la opción de menú Exportar aparece atenuada y la opción Exportación protegida está activada, los documentos se exportan con una marca de agua que contiene el nombre de usuario, el nombre de dominio y el ID. de equipo en cada página. **NOTA:** Si exporta un documento en modo protegido a un usuario externo, puede abrirlo y verlo, pero no exportarlo ni imprimirlo.	Si la opción de menú Exportar aparece atenuada y la opción Exportación protegida está activada, los documentos se exportan con una marca de agua que contiene el nombre de usuario, el nombre de dominio y el ID. de equipo en cada página. **NOTA:** Si exporta un documento en modo protegido a un usuario externo, puede abrirlo y verlo, pero no exportarlo ni imprimirlo.

Trabajar en línea con documentos de Office protegidos

Al crear documentos de Office protegidos, lo más recomendable es trabajar en línea debido a que se generan claves para esos documentos. Si es necesario recrear imágenes en su equipo y ha creado documentos de Office protegidos fuera de línea, asegúrese de comunicárselo su administrador.

Trabajar en línea con documentos protegidos habilitados para macros

En un documento protegido habilitado para macros, la macro existe pero está bloqueada. Sin embargo, actualmente, Data Guardian solo puede controlar un documento habilitado para macros después de que el nuevo documento protegido (.docm, .pptm, .xlsm) se haya cerrado y vuelto a abrir. Además, si guarda un documento protegido con una macro como no protegido, debe cerrarlo y volver a abrirlo para que la macro se ejecute.

Adjuntar un documento de Office protegido a un correo electrónico de Outlook

Cuando adjunte un documento de Office protegido a un correo electrónico de Outlook, seleccione **Insertar** en lugar de *Insertar como texto*. *Insertar como texto* pega el contenido del documento directamente en el cuerpo del correo electrónico y, de este modo, el contenido ya no está protegido.

Solución de problemas para el modo Opt-in

En Archivo > Información, si la opción Imprimir aparece atenuada significa que una política de Data Guardian ha desactivado la impresión para los documentos de Office protegidos. Sin embargo, cuando hace clic con el botón derecho del mouse en un archivo de Office protegido en el Explorador de Windows, la opción Imprimir no está atenuada. Sin embargo, si selecciona Imprimir, se produce lo siguiente:

- Word: un cuadro de diálogo indica que Word ha dejado de funcionar.
- Excel: un cuadro de diálogo indica que la política ha deshabilitado la opción Imprimir.
- Powerpoint: un cuadro de diálogo indica que la política ha deshabilitado la opción Imprimir. Si hace clic en Aceptar, se imprime una página de portada que indica que el documento está protegido.

Determinar qué documentos Modo Opt -in están protegidos

Si tiene activado el modo Force-Protected, todos los documentos de Office están protegidos. Si tiene activado el modo Opt-in y desea confirmar si el documento está protegido o no, ábralo y la barra de título lo mostrará como protegido.

Opciones de menú adicionales para documentos de Office protegidos

El tipo de documento de Office, protegido o no, puede afectar a lo siguiente.

Clic con el botón derecho del mouse > Proteger

Puede hacer clic con el botón derecho del mouse en un documento de Office y seleccionar **Proteger**. Debe agregar contenido con las opciones de menú para mostrar. No puede proteger un documento en blanco.

Propiedades del archivo > pestaña Dell Data Guardian

En los documentos de Office protegidos, puede hacer clic con el botón derecho del mouse y seleccionar **Propiedades**, y se mostrará una pestaña de **Dell Data Guardian** con información como el Id. y la clave de acceso del archivo y los datos de embargo.

Pegar

Si el administrador define una política de protección de documentos de Office:

- Puede copiar y pegar datos en el documento protegido original.
- No puede copiar o pegar datos desde un documento protegido a un documento desprotegido. No aparece nada en el Portapapeles y un mensaje de texto específico para empresas indica que no puede pegarlo en el documento no protegido o no administrado.

> **NOTA:**
> Si corta texto de un documento protegido y le aparece el mensaje en un documento desprotegido, haga clic en **Deshacer** en el documento protegido para recuperar el texto.

Arrastrar y soltar en Modo protegido

Puede arrastrar y soltar contenido en un documento de Word protegido. Actualmente, la opción de arrastrar y soltar está desactivada para los archivos Power Point y Excel.

Imprimir sobres y etiquetas

Si el administrador ha definido una política para agregar una marca de agua al imprimir un documento de Office protegido, siga estos pasos para imprimir sobres o etiquetas:

1 En un documento de Word, seleccione la pestaña **Correspondencia**.
2 Seleccione la opción **Sobres** o **Etiquetas**.
3 Después de introducir la dirección o el remite, haga clic en **Imprimir**.

NOTA: Si utiliza otra opción para imprimir y el administrador ha definido una política para agregar una marca de agua en los documentos de Office impresos, aparecerá una marca de agua en los sobres o etiquetas.

Documentos de Office protegidos y su manipulación

Data Guardian puede escanear documentos de Office protegidos para detectar distintas formas de manipulación.

Si un usuario interno manipula un documento de Office protegido:

- Data Guardian puede reparar o restaurar la manipulación.
- Si la manipulación no se puede reparar, aparece un cuadro de diálogo que le indica que el archivo ha sido manipulado y que debe ponerse en contacto con el administrador.

Si un usuario no autorizado abre un documento de Office protegido, solo se mostrará la página de portada. Si el usuario no autorizado modifica la página de portada, Data Guardian restaurará la página de portada cuando un usuario autorizado la vuelva a guardar como protegida.

Usuarios externos y documentos de Office protegidos

Mejorar la seguridad añadiendo restricciones de fecha

Con Data Guardian, carga un documento de Office protegido en la nube y lo comparte:

- Todos los usuarios internos de Data Guardian pueden verlo.
- Según cuál sea la política, los usuarios externos también pueden verlo.

De manera opcional, para mejorar la seguridad con los usuarios externos, puede agregar una restricción de fecha para limitar el tiempo que un usuario externo puede ver un documento de Office protegido.

1 Seleccione **Archivo > Información > Restricción de fecha**.
2 Desde las opciones de la lista desplegable, seleccione Fecha y hora de inicio y finalización para que un usuario externo vea el documento.

NOTA:
La Fecha y hora de inicio puede ser posterior si desea enviar el documento pero desea evitar que el usuario externo lo vea hasta la fecha y hora programadas.

3 Haga clic en **Aceptar**.
El documento se guardará, se protegerá, se cerrará y se volverá a abrir.

NOTA:
Aunque modifique las fechas para un documento de Office no protegido y haga clic en Cancelar, Data Guardian protegerá el archivo.

NOTA:
Actualmente, si agrega restricciones de fecha a un documento de Office protegido y quiere guardarlo a una unidad de red, primero debe guardar el archivo de forma local y, después, copiarlo a la red.

Si un usuario externo abre un archivo después del rango de fecha y hora establecido, aparece un cuadro de diálogo indicando que el archivo tiene restricciones de acceso y que el usuario externo debe ponerse en contacto con el autor. El cuadro de diálogo no muestra ninguna fecha al usuario externo.

Si define la fecha de inicio de un archivo en una fecha u hora posteriores y el usuario externo abre el archivo antes de tiempo, aparece un cuadro de diálogo que indica que el archivo no se puede abrir hasta la fecha y la hora indicadas debido a restricciones de acceso.

Comprender los elementos del menú de la bandeja del sistema de Data Guardian

Pantalla Detalles

La pantalla Detalles de Data Guardian proporciona información muy útil como, por ejemplo:

- Para obtener soporte técnico, puede proporcionar información sobre el estado o la versión.
- Para ver un nombre de archivo sin texto confuso que esté asociado con un archivo .xen, seleccione **Archivos** > **Estado del archivo**.
- Para buscar un archivo por el nombre, seleccione Copiar en la parte inferior derecha y pegue el contenido en un archivo Word.
- Para ver quién es el propietario de la carpeta, seleccione Carpetas y desplácese hasta la columna PROPIETARIO DE LA CARPETA.

Para acceder a la pantalla Detalles:

Haga clic en el icono de la bandeja del sistema de **Data Guardian** y, a continuación, haga clic en **Detalles...**

La esquina superior izquierda de la pantalla Detalles mostrará la siguiente información:

Estado del servicio: estado del servicio de Windows de Data Guardian. Los valores posibles son: Detenido, InicioPendiente, DetenidoPendiente, En ejecución, ContinuarPendiente, EnPausaPendiente, En pausa

Estado de ejecución: el estado de activación del dispositivo. Los valores son: Activo, Reactivado, Suspendido, Suspendiendo

Modo de usuario: usuario interno; un usuario con una dirección en este dominio

Usuario externo: un usuario con una dirección fuera de este dominio

Correo electrónico de registro: para los usuarios internos, es el correo electrónico del dominio. Para los usuarios externos, este es el correo electrónico con el que se registraron.

URL del servidor: el DDP EE Server/VE Server que se comunica con este cliente.

Última modificación de la política: fecha y marca de tiempo de la última vez que el cliente usó y modificó la política.

Versión de la política: versión de la política generada por DDP EE Server/VE Server.

El área de **Archivos** de la pantalla Detalles muestra la información siguiente:

Nombre: nombre del archivo

Nube: enumera la ofuscación de nombres de archivos o si el archivo está *Desprotegido*.

Estado del archivo: este valor indica el propietario de la carpeta. El valor lo determina la Id. de clave.

Estado del proceso: indica si el archivo necesita una clave o si está *Completo*.

Empresa: indica el servidor predeterminado. Si se muestra el mensaje *Error: la clave no pertenece a su servidor* en esta columna, indica que la clave no pertenece a su servidor de empresa. La clave para un archivo cifrado debe pertenecer al servidor de su empresa.

Clave: id. de clave asignada a esta carpeta (los archivos nuevos usan esta clave para el cifrado).

Carpeta: el nombre de la ruta de acceso completo de la carpeta.

Última modificación: la fecha de modificación del archivo.

Estado de persistencia: esto indica si el archivo está en un disco.

Lectura de archivos XEN: *Verdadero* o *Falso*.

Explorador creado: *Verdadero* o *Falso*.

Para los archivos de registro, haga clic en **Ver registro** en la esquina inferior izquierda de la pantalla Detalles.

NOTA:
Los archivos de registro también se encuentran en **C:\ProgramData\Dell\Dell Data Protection\Dell Data Guardian.**

El área de **Carpetas** de la pantalla Detalles muestra la información siguiente:

Nombre: nombre de la carpeta

Clave: id. de clave asignada a esta carpeta (los archivos nuevos usan esta clave para el cifrado).

Cliente de sincronización: el último cliente de sincronización que sincronizó esa carpeta (Consulte Clientes de sincronización en la nube).

Propiedad de la carpeta: este valor indica el propietario de la carpeta. El valor lo determina la Id. de clave.

Reemplazar: las opciones son *Ninguno* y *Ya existente*. Los archivos preexistentes no están protegidos. También, si tiene acceso a Administración de carpetas y ha desprotegido algunos archivos, esta columna indica que no están protegidos.

Tipo de ofuscación: si su empresa administra el almacenamiento en la nube, se trata de una política definida en cada carpeta que indica qué tipo de archivos .xen se crearán en la nube. Esta es una política que establece su administrador. Si el administrador selecciona *Solo extensión*, se mostrará el propio nombre del archivo con la extensión ".xen". Si el administrador selecciona *Guid*, se mostrará el nombre del archivo codificado con la extensión ".xen". Esta es una configuración de la política que tiene efecto en carpetas nuevas solamente. El valor predeterminado es *Solo extensión*.

Menú Administrar carpetas

Es posible que algunos administradores necesiten compartir temporalmente carpetas de solución de problemas con más de un usuario. Puede solicitar permisos al administrador para la opción Administrar carpetas. Normalmente, se trata de una opción temporal.

Localizar archivos de registro

Su administrador puede solicitar archivos de registro para solución de problemas.

Para localizar archivos de registro:

1 Navegue hasta
2 Seleccione **Xendow.service.log**.

NOTA:
Cuando Xendow.Service.log alcanza 3 MB, se guarda como Xendow.Service1.log y, a continuación, como Xendow.Service2.log.

Comprobar si existen actualizaciones de políticas

Si el administrador modifica una política y le notifica de una actualización de políticas, vaya a la bandeja del sistema de Windows, haga clic en el icono de **Dell Data Protection | Data Guardian** y seleccione **Comprobar si existen actualizaciones de políticas**.

Si el administrador modifica una directiva para proteger los archivos creados en Microsoft Word, debe cerrar el programa para que pueda aplicarse la actualización.

Actualizar Data Guardian

La práctica recomendada es desinstalar la versión anterior y, a continuación, instalar la versión actual. Consulte Desinstalar Data Guardian.

Proporcionar comentarios a Dell

Si su administrador ha habilitado una política de comentarios, puede proporcionar comentarios a Dell acerca de este producto. El breve formulario incluye dos preguntas sobre su nivel de satisfacción, con escalas de clasificación (donde 10 indica el nivel de satisfacción más alto) y un campo para comentarios.

Para tener acceso al formulario, haga clic en el icono de Data Guardian de la bandeja del sistema y seleccione **Enviar retroalimentación**.

Si esta función no está habilitada por una política, la opción no se mostrará.

Posibles problemas de activación: Office protegido

Si ha instalado Data Guardian, pero el icono de Data Guardian de la bandeja del sistema no tiene una marca de verificación verde  , tenga en cuenta lo siguiente:

- Data Guardian puede convertir los documentos de Office existentes en modo protegido antes de que lo active. Si es así, al abrir un documento de Office, se mostrará una página de portada con información para activarlo.

Realice una de estas opciones:

- Reinicie y vuelva a iniciar sesión con un sufijo UPN, por ejemplo, user_name@domain.com.
- Confirme con su administrador si debe seleccionar la casilla de verificación **Habilitar la verificación de confianza en SSL** cuando instale Data Guardian.
- Póngase en contacto con el administrador del sistema por si debe tener el equipo configurado para activarlo manualmente. Consulte Activar Data Guardian.

Activar Data Guardian

Normalmente, Data Guardian se activa automáticamente después de instalar y reiniciar. Si el administrador le pide que lo active manualmente, siga estos pasos:

1 Inicie sesión en Windows.
En la bandeja del sistema, se muestra el icono de un escudo con una marca de verificación naranja.
2 Haga clic en el icono de **Data Guardian** en la bandeja del sistema y, a continuación, seleccione **Activación de usuario**.
3 Introduzca el correo electrónico y la contraseña de su dominio y haga clic en **Activar**.

Si es un usuario interno (con una dirección de correo electrónico del dominio), ignore el botón Registrar. Únicamente deben registrarse los usuarios externos.

Cuando se complete la activación, se mostrará una marca de verificación verde en el icono  de la bandeja del sistema de Data Guardian.

4 Confirme el estado de su modo de usuario. Haga clic en el icono de la bandeja del sistema y seleccione **Detalles**.

5 En la parte superior, confirme el Modo de usuario:

Interno: un usuario con una dirección de correo electrónico en el dominio de la empresa.

Externo: un usuario con una dirección de correo electrónico que no es del dominio. Para obtener más información, consulte Usar Data Guardian como usuario externo.

Utilizar Data Guardian Mobile con iOS o Android

Esta sección describe la información básica sobre la utilización de Data Guardian Mobile con iOS o Android. Cuando su administrador establece una política para habilitar Data Guardian, los archivos están cifrados y seguros en la nube. Sin embargo, puede utilizar la aplicación Data Guardian Mobile para visualizarlos en su dispositivo móvil.

Requisito previo

Antes de utilizar la app de Data Guardian, necesita el nombre del Servidor de Dell Data Protection de su empresa, como por ejemplo servidor.dominio.com. Esta información la proporciona el administrador.

Introducción a Data Guardian Mobile

Siga la secuencia a medida que vaya utilizando Data Guardian Mobile.

Tarea	Descripción	Consulte esta sección
Instalar Data Guardian	Determine lo siguiente: El administrador ya ha instalado El usuario debe instalar	El administrador ya ha instalado: toque la app de Data Guardian e inicie sesión. El usuario es el encargado de instalar; consulte uno de estos dos apartados: Instalación en un dispositivo iOS Instalación en un dispositivo Android
Acceder a su cuenta de proveedor de almacenamiento en la nube	En el dispositivo, vaya a la página principal de la app de Data Guardian y toque su proveedor de almacenamiento en la nube.	Consulte una de las opciones siguientes: Acceder a su proveedor de almacenamiento en la nube cuenta en iOS Acceder a su proveedor de almacenamiento en la nube cuenta en Android

La aplicación Data Guardian Mobile enumera el cliente de sincronización en la nube utilizado con su compañía y le permite descargarlo.

NOTA:
Si descarga la app del cliente de sincronización en la nube a su dispositivo, Data Guardian no cifrará las carpetas ni los archivos que haya cargado directamente de la aplicación. Para cifrar y proteger archivos debe utilizar la aplicación de Data Guardian para cargarlos.

Para proteger sus datos en la nube, Data Guardian los cifra. Por lo tanto, para ver archivos cifrados, debe tener instalada la aplicación de Data Guardian en su dispositivo móvil.

- Los archivos de Office protegidos, (.docx, .pptx, .xlsx) conservan su extensión.
- Los archivos que no son de Office en la nube tienen la extensión .xen.

Si una persona no autorizada accede a su cuenta de almacenamiento en la nube y descarga un archivo a un dispositivo móvil que **no** dispone de Data Guardian instalado, no podrá abrir ni ver los archivos. Si abre un archivo de Office protegido, solo le aparecerá una página de portada que le indicará que no puede ver el documento sin Data Guardian. Esto ofrece más seguridad a sus datos.

En dispositivos móviles, puede:

- Crear carpetas
- Cargar y descargar archivos

  NOTA:
  Con Data Guardian debe iniciar la carga y descarga en el dispositivo. Para cifrar los archivos al cargarlos en la nube, debe cargarlos desde la pantalla de inicio de Data Guardian, no desde una aplicación cliente de sincronización en la nube. Cuando toca un archivo, Data Guardian lo descifra automáticamente y lo muestra como texto no cifrado en la aplicación. No obstante, en la nube, el archivo se mantiene seguro como un archivo .xen.

- Agregar un archivo a Favoritos
  - Para iOS, consulte el menú de navegación. Para Android, pulse y mantenga pulsado el nombre de archivo.
- Eliminar carpetas y archivos
- Aceptar una carpeta compartida de un usuario interno

  NOTA:
  Si un usuario interno comparte una carpeta con usted mediante Data Guardian, debe ir al sitio web del almacenamiento en la nube y moverlo a la carpeta raíz o descargar la carpeta compartida para poder verlo en el dispositivo.

- Compartir un documento con un usuario externo (si la política está habilitada para visores externos): para dispositivos iOS, consulte Ver las políticas de almacenamiento en la nube de Data Guardian para su dispositivo iOS.
- Editar archivos Office .docx y .ppt.

  NOTA:
  Actualmente, los archivos .csv y .csv .xen no se pueden editar en dispositivos móviles.

Documentos de Office protegidos sin conexión

Cuando crea un documento de Office protegido o un documento habilitado para macros protegido y está sin conexión, se crea una clave para ese documento. Cuando el dispositivo está en línea, las claves se cargan al Servidor Dell. Si un dispositivo está sin conexión durante tres días, una notificación indica que Data Guardian no puede ponerse en contacto con el Servidor Dell. La notificación se muestra diariamente hasta que se conecte a la red. Para ver los archivos cifrados, el dispositivo móvil debe estar en línea.

Protección adicional mediante el perimetraje

En función de las políticas establecidas por el administrador, los dispositivos móviles puede tener protección adicional en documentos de Office protegidos y los archivos .xen no pueden abrirse fuera de la región especificada. Debe estar en una región aprobada para abrir los archivos protegidos. Actualmente, las regiones son Estados Unidos y Canadá. Debe activar los servicios de ubicación del dispositivo para que funcione el perimetraje. Si su administrador ha habilitado la función de perimetraje y los servicios de ubicación están desactivados, se le denegará el acceso a los archivos.

Uso de PIN

El administrador puede establecer una política que requiera un PIN.

Data Guardian en un dispositivo iOS

Instalación en un dispositivo iOS

1. En el dispositivo, toque **App Store** y busque **Data Guardian Mobile**.
2. Seleccione e instale la app de **Data Guardian**.
3. En el campo Servidor de la pantalla de conexión, escriba el nombre de host del Dell Data Protection Server de la empresa, por ejemplo, servidor.dominio.com.
4. Introduzca su nombre de usuario y contraseña.
5. Toque **Iniciar sesión**.

Acceder a su proveedor de almacenamiento en la nube cuenta en iOS

Después de iniciar sesión en Data Guardian, una política de Data Guardian determina los proveedores de almacenamiento en la nube que se visualizan en la pantalla de inicio. Su administrador puede designar un proveedor de almacenamiento en la nube específico para utilizarlo en la empresa.

El menú de navegación ofrece opciones adicionales.

Para acceder a una cuenta:

1 En la página de inicio de Data Guardian, pulse el proveedor de almacenamiento en la nube.
2 Realice una de las siguientes acciones siguiendo las instrucciones en línea:
   - Cree una cuenta con el proveedor de almacenamiento en la nube.
   - Inicie sesión en una cuenta de proveedor de almacenamiento en la nube existente.

> **NOTA:**
> Para obtener más información, consulte la ayuda de su proveedor de almacenamiento en la nube.

Desvincular un proveedor de almacenamiento en la nube

Si tiene más de una cuenta con el mismo proveedor de almacenamiento en la nube, no puede iniciar en ambas simultáneamente. Debe borrar la casilla de verificación para desvincular y cerrar sesión en la cuenta actual y, a continuación, iniciar sesión con otras credenciales.

1 Abra el menú de navegación de Data Guardian y toque **Configuración**.
2 Toque **Desvincular**.

Ver las políticas de almacenamiento en la nube de Data Guardian para su dispositivo iOS

1 En el menú de navegación de Data Guardian, toque **Configuración**.
2 Toque **Política**.
   La lista puede incluir:
   - Revisión: número de políticas que se han revisado
   - Ofuscación de nombres de archivos: el valor predeterminado se establece en **No**
   - Cliente de sincronización en la nube: la política debe establecerse en **Cifrar**
   - Visores externos: la política de uso compartido está activada si se establece en **Sí**. Cuando abra un documento en la aplicación, una opción de menú le permitirá compartir el archivo.

Desinstalar la app de Data Guardian

1 En el menú de aplicaciones de iOS, pulse y mantenga pulsado el icono de **Data Guardian**.
2 Toque **x**.
3 Toque **Eliminar**.

Solución de problemas de iOS y Data Guardian

En un dispositivo iOS, si abre un documento de Office protegido de más de 25 MB y aparece un cuadro de diálogo que indica que hay poca memoria, la advertencia proviene de Polaris Office, no de Data Guardian. Si el dispositivo tiene memoria suficiente, cierre el archivo y vuelva a abrirlo.

En Dropbox for Business, si marca un archivo como disponible sin conexión y le cambia el nombre en el sitio web de Dropbox, el archivo no se abrirá en el dispositivo iOS que disponga de la app de Data Guardian.

Data Guardian en un dispositivo Android

Instalación en un dispositivo Android

1 En el dispositivo, acceda a **Google Play** y busque **Data Guardian Mobile**.

2 Seleccione e instale la app de **Data Guardian**.
3 En el campo Servidor de la pantalla de conexión, escriba el nombre del Dell Data Protection Server de la empresa, por ejemplo, servidor.dominio.com.
4 Introduzca su nombre de usuario y contraseña.
5 Toque **Iniciar sesión**.

Su cuenta ya está activada.

Acceder a su proveedor de almacenamiento en la nube cuenta en Android

Después de iniciar sesión en Data Guardian, una política de Data Guardian determina los proveedores de almacenamiento en la nube que se visualizan. Su administrador puede designar un proveedor de almacenamiento en la nube específico para utilizarlo en la empresa y bloquear otros.

Para acceder a una cuenta:

1 En la página de inicio de Data Guardian, pulse el proveedor de almacenamiento en la nube.
2 Realice una de las siguientes acciones siguiendo las pantallas en línea:
   - Cree una cuenta con el proveedor de almacenamiento en la nube.
   - Inicie sesión en una cuenta de proveedor de almacenamiento en la nube existente.

   NOTA:
   Para obtener más información, consulte la ayuda de su proveedor de almacenamiento en la nube.
3 Después de acceder a su cuenta, abra el menú de navegación y pulse **Configuración**. Cuando otorgue acceso a un proveedor de almacenamiento en la nube, se mostrará una marca de selección en la casilla de verificación.

NOTA:
Si tiene más de una cuenta con el mismo proveedor de almacenamiento en la nube, no puede iniciar en ambas simultáneamente. Debe borrar la casilla de verificación para desvincular y cerrar sesión en la cuenta actual y, a continuación, iniciar sesión con otras credenciales.

NOTA:
Para OneDrive y Dropbox, si no puede compartir un archivo desde las aplicaciones y el archivo comparte un vínculo con la app de Data Guardian, comparta el archivo desde la aplicación del navegador de archivos del dispositivo.

Desinstalar la app de Data Guardian

1 En el menú de aplicaciones de Android, pulse **Configuración**.
2 En **Configuración**, toque **Aplicaciones**.
3 Pulse el icono de **Data Guardian**.
4 Arrastre el icono hasta la opción Desinstalar.
5 Haga clic en **Aceptar**.

Consideraciones de seguridad con Data Guardian y Clientes de sincronización

Data Guardian cifra archivos y carpetas para que los datos estén seguros. Como Data Guardian funciona con clientes de sincronización, tenga en cuenta estas consideraciones.

Google Drive

Google Drive contiene una aplicación de Google Docs que permite a los usuarios colaborar con documentos en tiempo real. No obstante, la colaboración se produce en un servidor de Google, no en Dell Data Protection EE Server/VE Server. Por lo tanto, los archivos no están

cifrados. Para dispositivos Android e iOS con Data Guardian, el acceso a Google Docs está bloqueado. Difiere ligeramente dependiendo de la plataforma:

- Android
- iOS: se muestra un mensaje.

OneDrive y OneDrive for Business

Con OneDrive for Business, si descarga varios archivos y cancela la descarga, OneDrive for Business cancelará aquellos que no se hayan descargado aunque continuará con el que se encuentre en proceso de descarga. Se trata de un problema de Microsoft. Por lo tanto, permita que los archivos se descarguen completamente antes de cancelar.

Registros

Por motivos de seguridad, no hay ningún archivo de registro disponible en dispositivos móviles.

Enviar comentarios a Dell

Si su administrador ha habilitado una política de comentarios, puede proporcionar comentarios a Dell acerca de este producto. Si esta función no está habilitada por una política, la opción no se mostrará.

Para enviar comentarios:

1 En el menú de navegación de Data Guardian, toque **Retroalimentación**.
2 Las preguntas breves le permiten clasificar su nivel de satisfacción (10 indica el nivel de satisfacción más alto) e introducir un comentario.

Usar Data Guardian como usuario externo

Un usuario externo que tenga una dirección de correo electrónico que no sea de dominio también puede usar Data Guardian. He aquí algunos ejemplos.

- Ha instalado y activado Data Guardian como parte de su empresa, pero necesita compartir archivos protegidos o colaborar en archivos protegidos con un usuario fuera de su empresa.
- Su dirección de correo electrónico está dentro del dominio de la empresa, pero desea también instalar y activar Data Guardian en un equipo o dispositivo móvil con su dirección de correo electrónico personal, no de dominio. Esto le permite interactuar con sus archivos protegidos desde una dirección de correo electrónico que no sea de dominio de empresa.

Para los usuarios externos, consulte Requisitos del servidor. Además, el dominio o usuario no debe estar en la lista negra de la empresa.

NOTA:
Los usuarios externos que se registraron con Secure Lifecycle 1.0 o superior migrarán si la empresa se actualiza.

Tareas del usuario interno

Para compartir archivos seguros con un usuario externa, puede enviar un documento de Office protegido o un archivo .xen a través de un correo electrónico de Outlook. Una petición de confirmación le recuerda que se compartirá la clave del archivo compartido.

NOTA:
Si un usuario externo envía por correo electrónico un archivo protegido, las claves no se comparten.

También puede utilizar la opción Conceder acceso para compartir archivos seguros con un usuario externo. Debe hacer lo siguiente:

- Poner a disposición del usuario externo uno o más archivos seguros.
  - Documentos de Office protegidos: conceda acceso a uno o más archivos seguros mediante:
    - Carpeta local o una unidad de red
    - Correo electrónico
    - Medios extraíbles
    - Recurso compartido de red
  - Archivos .xen que no son de Office: cree una carpeta para compartir el en cliente de sincronización y añada archivos.
- Conceda el acceso de usuarios externos a uno o varios archivos.

Si tiene pensado compartir archivos .xen que no son de Office, debe añadirlos a una carpeta de cliente de sincronización y, a continuación, concederle acceso. Para los archivos Office protegidos, debe conceder acceso. Los pasos pueden variar según el método que utilice o el cliente de sincronización utilizado.

Compartir una carpeta en el cliente de sincronización para compartir archivos .xen

1 En el Explorador de Windows, acceda al cliente de sincronización, cree una carpeta y cargue un archivo para compartir con un usuario externo. Consulte Visualización de carpetas y archivos en el equipo local y en la nube.

Los documentos de Office protegidos pueden estar en la Unidad virtual DDG VDisk, en la carpeta de Data Guardian o en el escritorio.

NOTA:
Con los archivos de Office protegidos, no puede seleccionar una carpeta.

Se abrirá la página *Compartir acceso a documentos protegidos* con una columna que muestra los archivos seleccionados.

2 En el sitio web del cliente de sincronización, confirme que la carpeta y el archivo se han creado y cifrado.

Cuando agrega un archivo .xen a una carpeta nueva en la Unidad virtual DDG VDisk, Data Guardian agrega un documento, *How to access secure files.html*, a la carpeta del sitio web. Este archivo solo se utiliza cuando se comparte la carpeta con un usuario externo.

3 En el sitio web del cliente de sincronización, haga clic con el botón derecho del mouse en la carpeta que ha creado y haga clic en **Compartir**.

Se abrirá una ventana, que le permite especificar la cuenta de correo electrónico para un usuario externo. Los pasos variarán en función del cliente de sincronización utilizado. Para obtener vínculos con información sobre el cliente de sincronización, consulte Trabajar con clientes de sincronización en la nube en la unidad virtual DDG VDisk.

4 Conceda acceso a los archivos individuales en esa carpeta que desea compartir.

Conceda acceso a uno o más archivos de Office protegidos

Debe conceder acceso a todos los archivos que comparta con usuarios externos.

1 Haga clic con el botón derecho del mouse en un archivo seguro y seleccione **Conceder acceso a archivos protegidos**. Puede seleccionar hasta 50 archivos a la vez.
2 En el campo *Correo electrónico para compartir*, introduzca la dirección de correo electrónico del usuario que no sea del dominio y haga clic en **Agregar**.
3 Repita este paso para agregar hasta diez direcciones de correo electrónico.
4 Haga clic en **Aceptar**.

Un cuadro de diálogo indica si se ha compartido con éxito o si la dirección de correo electrónico no está autorizada para recibir los archivos protegidos.

5 Lo mejor que puede hacer es informar al usuario externo de que recibirá un correo electrónico con las instrucciones que le permitirán registrarse a un Servidor Dell, descargar y activar Dell Data Protection | Data Guardian y ver los archivos protegidos compartidos.

Aprobar o denegar el acceso cuando un usuario externo lo solicita

Un usuario externo que tiene Data Guardian instalado puede solicitar acceso a un documento protegido si no tiene una clave para el documento.

1 Si recibe un correo electrónico de un usuario externo que solicita acceso a un documento protegido, puede ver el nombre del usuario externo y el archivo solicitado.
2 Seleccione **Aprobar** o **Denegar**.

Se envía un mensaje de correo electrónico al usuario externo. Si aprueba, se comparte la clave del documento protegido.

Si no está disponible, el administrador también tiene la opción de aprobar o denegar el acceso.

Tareas del usuario externo

Para abrir y ver un documento de Data Guardian, el usuario externo debe:

- Registrarse en Data Guardian

- Instalar Data Guardian: el usuario externo debe tener derechos de administrador en su equipo
- Si el usuario interno comparte una carpeta a través de un cliente de sincronización, el usuario externo debe tener una cuenta de cliente de sincronización. Consulte Instalar clientes de sincronización en la nube y, a continuación, Trabajar con clientes de sincronización en la nube en la unidad virtual DDG VDisk.

Registrarse en Data Guardian

La primera vez que un usuario interno comparte un archivo, el usuario externo debe registrarse.

Para registrarse en Data Guardian:

1 En el correo electrónico de verificación de la cuenta de Dell Enterprise Server, haga clic en el hipervínculo.
2 Avance por la página web.
3 En la página de confirmación, haga clic en **Continuar para iniciar sesión**.
4 En la página de inicio de sesión, haga clic en **¿Ha olvidado la contraseña?**

> **NOTA:**
> El Servidor Dell tiene asignada una contraseña aleatoria que debe restablecer.

5 En la página Restablecer contraseña, introduzca y confirme la contraseña nueva y, a continuación, haga clic en **Registrar**.
Aparecerá un diálogo de confirmación de registro y se enviará un correo electrónico a la dirección que haya introducido el usuario interno.
6 Abra el correo electrónico de activación de la cuenta y haga clic en el vínculo.
El correo electrónico también muestra el nombre del servidor que debe utilizar cuando instale Data Guardian.
7 En la página Inicio de sesión, escriba la dirección de correo electrónico y la contraseña que ha utilizado para registrarse.
8 Haga clic en **Inicio de sesión**.
Se abre una página de descarga de Data Guardian.
9 Descargue e instale Data Guardian.
Se abre una página de descarga con diferentes opciones para Windows, iOS, Android y Mac OS X. Se abre la página Descargar para un Enterprise Server. En Dell Enterprise Server - VE, hacer clic en Windows le lleva al sitio dell.com/support.

Estos pasos describen cómo instalar Data Guardian en Windows. Consulte también Tareas del usuario: Office protegido sin cifrado en la nube.

> **NOTA:**
> La lista de descargas también muestra el nombre del servidor que necesitará en estos pasos.

10 En Windows, haga clic en **Descargar (32 bits)** o **Descargar (64 bits)**, según el sistema operativo de su equipo.
11 Descargue el archivo de configuración en un directorio de su equipo.
12 Haga doble clic en el archivo de configuración para iniciar el instalador.
13 Seleccione un idioma y haga clic en **Aceptar**.
14 Si se le solicita que instale el paquete redistribuible Microsoft Visual C++ 2010, haga clic en **Aceptar**.
15 En la ventana de Bienvenida, haga clic en **Siguiente**.
16 Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.
17 En la pantalla Carpeta de destino, haga clic en **Siguiente** para instalar en la ubicación predeterminada de **C:\Archivos de programa\Dell \Dell Data Protection\Dell Data Guardian\.**
18 En el campo *Nombre del servidor:*, introduzca el nombre del servidor con el que se comunicará este equipo. Este nombre está en el correo electrónico de activación que haya recibido o en la parte superior de la página de descargas.
19 Haga clic en **Siguiente**.
20 En la pantalla Confirmar servidor de activación, confirme que la dirección URL del servidor es correcta. El instalador añade www o http(s) y el puerto. Haga clic en **Siguiente**.
21 En la ventana Tipo de administración, seleccione esta opción:
- Usuario externo: un usuario con una dirección de correo electrónico que no es del dominio de la empresa.

22 Haga clic en **Instalar** para comenzar la instalación.

Se mostrará una ventana de estado que muestra el progreso de la instalación.

23 Cuando se muestre la pantalla Instalación completa, haga clic en **Finalizar**.

24 Haga clic en **Sí** para reiniciar.

La instalación de Data Guardian se ha completado.

25 Consulte Activar Data Guardian.

Activar Data Guardian

Una vez que Data Guardian se ha instalado y el equipo se ha reiniciado, siga estos pasos para activar:

1 Inicie sesión en Windows.

En la bandeja del sistema, se muestra el icono de una nube con un signo de exclamación naranja.

2 Cuando se muestre un cuadro de diálogo en la bandeja del sistema, haga clic en **Haga clic aquí para activar**.

Si no ve el cuadro de diálogo, haga clic en el icono de **Data Guardian** que aparece en la bandeja del sistema y seleccione **Activación de usuario**.

3 Introduzca la dirección de correo electrónico y la contraseña que haya utilizado para registrase y haga clic en **Activar**.

Cuando se complete la activación, se mostrará una marca de verificación verde en el icono  de la bandeja del sistema de Data Guardian.

4 Confirme el estado de su modo de usuario. Haga clic en el icono de la bandeja del sistema y seleccione **Detalles**.

En la parte superior, Modo de usuario es:

Externo: un usuario con una dirección de correo electrónico que no es del dominio.

Si ya ha instalado y ha iniciado sesión en un cliente de sincronización, la Unidad virtual DDG VDisk se muestra en el Explorador de Windows.

Solicitar el acceso de un usuario interno

Con Windows y Mobile, si un usuario externo ha instalado y activado Data Guardian, puede solicitar el acceso a un archivo de un usuario interno. El usuario externo debe realizar una solicitud por separado para cada archivo.

1 Si abre un archivo de Office protegido y se indica que es necesario solicitar el acceso, haga clic en **Sí** o **No**.

Un cuadro de diálogo indica que la solicitud se ha enviado correctamente. El usuario interno puede autorizar o denegar el acceso y el usuario externo recibe un correo electrónico con el resultado. Si el usuario externo abre el archivo protegido antes de que el usuario interno apruebe el acceso, aparece un mensaje que indica que la solicitud está pendiente.

2 Después de 48 horas, el usuario externo puede solicitar el acceso de nuevo.

En la bandeja de sistema, el usuario externo puede hacer clic con el botón derecho del mouse en el icono de Data Guardian y seleccionar la página **Detalles**. Haga clic en la pestaña **Seguridad**. Cuando la hora de una solicitud regresa a *Ninguna*, el usuario externo puede solicitar acceso de nuevo.

Ver un documento de Office protegido

Si una empresa activa una política de protección de documentos de Office y un usuario interno envía un archivo protegido a un usuario externo, el usuario externo debe estar conectado al Servidor Dell cuando abra el documento por primera vez. Después de eso, se podrá abrir y ver el documento sin conexión durante un período de tiempo especificado, por ejemplo, una semana. A continuación, el usuario externo debe conectarse al Servidor y volver a abrir el documento protegido.

Por motivos de seguridad, un usuario externo no podrá realizar las siguientes acciones con un documento de Office protegido.

- Imprimir
- Exportar

- Guardar como
- Compartir

Desinstalar un cliente de sincronización o Data Guardian

Si el administrador ha sido el encargado de instalar Data Guardian, solo él podrá desinstalar el producto. Un usuario externo al que se haya invitado a compartir una carpeta y tenga derechos de administrador en un equipo externo también podría desinstalar Data Guardian desde ese equipo externo.

Desinstalar un cliente de sincronización en la nube

Si desinstala el cliente de sincronización en la nube pero aún dispone de Data Guardian en su equipo, todavía puede ver los archivos en texto no cifrado en la Unidad virtual DDG VDisk.

Sin embargo, si vuelve a instalar el mismo cliente de sincronización en la nube, necesitará una nueva clave para abrirlo en la Unidad virtual DDG VDisk y deberá descargarse los archivos del sitio web del cliente de sincronización.

Desinstalar Data Guardian

Debe ser un administrador local en el equipo para desinstalar Data Guardian.

Copiar archivos en su unidad local

Si desinstala Data Guardian de su equipo o dispositivo, los archivos que haya en el sitio web del cliente de sincronización tendrán que ser seguros por lo que permanecerán cifrados.

1 Antes de desinstalar, determine si necesita acceder a algún archivo.
2 Copie estos archivos de la Unidad virtual DDG VDisk a su unidad local.

Estos archivos que ha copiado de la Unidad virtual DDG VDisk se mostrarán como texto no cifrado. Las carpetas y archivos en el sitio web del cliente de sincronización estarán cifrados, incluso si los descarga. Para verlos, debe volver a instalar Data Guardian.

Desinstalar Data Guardian

1 Use el panel de control de Windows para desinstalar el programa.
2 Seleccione Dell Data Protection | Data Guardian y haga clic en **Cambiar** en el menú superior.
3 Haga clic en **Siguiente** cuando aparezca la pantalla de Bienvenida.
4 Seleccione **Eliminar** y haga clic en **Siguiente**.
5 Aparecerá una advertencia para confirmar si desea desinstalar Dell Data Protection | Data Guardian. Si es así, haga clic en **Siguiente**.
6 En la pantalla Quitar el programa, haga clic en **Eliminar**.
Se indicará el progreso en una ventana de estado.
7 Si se muestra un diálogo de error del cliente de sincronización, haga clic en **Continuar**.
8 Haga clic en **Finalizar** cuando aparezca la pantalla Completado.
9 Haga clic en **Sí** para reiniciar.

La desinstalación de Dell Data Protection | Data Guardian ha finalizado.

Preguntas más frecuentes

Preguntas más frecuentes sobre diversos temas

Pregunta

Moví la carpeta de sincronización del proveedor de nube a Archivos de programa y ahora no puedo descifrar los archivos que se descargan a mi carpeta de sincronización desde la nube.

Respuesta

Por diseño, la carpeta Archivos de programa u otras carpetas excluidas están desprotegidas, conforme a la política correspondiente. Data Guardian no descifra los archivos descargados a esta carpeta ni a sus subcarpetas.

Solución

Desvincule o desinstale el cliente de sincronización y mueva la carpeta de sincronización de nuevo a su ubicación predeterminada o a una ubicación alternativa administrada.

NOTA:
Para obtener una lista de las ubicaciones administradas y no administradas, póngase en contacto con su administrador.

Pregunta

Tenía algunos archivos .xen archivados, y los copié a mi escritorio. Algunos de ellos se descifraron, pero otros no.

Respuesta

Durante una sincronización, Data Guardian está diseñado para descifrar directamente a la unidad virtual o descifrar cuando se descarga a través de un navegador web. Para archivos que se han copiado desde otra ubicación, utilice el Explorador de Windows y mueva el archivo .xen a la unidad virtual para que se descifre.

Solución

Mueva los archivos .xen a la carpeta de la unidad virtual para que se carguen en la nube. De esta forma, se descifrarán localmente.

Pregunta

Cambié el nombre de mi equipo. Ahora ya no recibo las actualizaciones de políticas y no puedo cifrar en la nube.

Respuesta

Actualmente, el servidor reconoce solo el extremo que utilizó originalmente para la activación. Si cambia el nombre del extremo, el servidor no reconocerá la ubicación para el envío de la política y Data Guardian no funcionará como se espera.

Solución

1 Detenga la sincronización de archivos en el equipo local.

NOTA:
Si no detiene la sincronización antes de la desinstalación, los datos valiosos podrían dejar de estar protegidos en la nube o, posiblemente, eliminarse.

2 Desinstale Data Guardian y, a continuación, vuelva a instalarlo. Para desinstalar, debe tener derechos de administrador.

Pregunta

En dispositivos suspendidos de Windows, no sucede nada cuando trato de cargar archivos en la nube. Si cierro las ventanas que ya estaban abiertas, aparece un mensaje de error de acceso denegado.

Respuesta

El mensaje de error no procede de Data Guardian. Puede acceder a los archivos localmente, pero no obtendrá futuras actualizaciones a los archivos.

Preguntas frecuentes sobre los Documentos Office y el Modo protegido

Pregunta

He intentado abrir un documento Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm) y ha aparecido una página de portada.

Respuesta

Si el administrador ha definido una política de protección de documentos de Office, deberá instalar Data Guardian. Confirme que el icono de Data Guardian de la bandeja del sistema tiene una marca de comprobación verde que indica que está activado.

Solución

Determine si es necesario instalar o activar Data Guardian. Consulte Instalar Data Guardian o Posibles problemas con la activación.

Pregunta

No puedo abrir un documento protegido de Office (Word, PowerPoint o Excel).

Respuesta

Compruebe lo siguiente:

- Configuración del bloqueo de archivos: si el administrador define políticas para proteger documentos de Office, no utilice esta configuración en **Archivo > Opciones**.

Solución

Para verificar la configuración del bloqueo de archivos:

1 En un documento de Office, seleccione **Archivo > Opciones**.
2 Seleccione el **Centro de confianza** de la lista.
3 En la derecha, haga clic en **Configuración del centro de confianza.**
4 Seleccione **Configuración del bloqueo de archivos** de la lista.
5 Para *documentos y plantillas Word/Excel/PowerPoint 2007 y posteriores*, asegúrese de que la casilla *Abrir* no está seleccionada.
6 Haga clic en **Aceptar**.