Dell Data Guardian

Guía del usuario de Windows, Mac, dispositivos móviles y web v2.7

Identifier	GUID-5B8DE7B7-879F-45A4-88E0-732155904029
Status	Translated

Notas, precauciónes y advertencias

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

PRECAUCIÓN: Una PRECAUCIÓN indica un potencial daño al hardware o pérdida de datos y le informa cómo evitar el problema.

ADVERTENCIA: Una señal de ADVERTENCIA indica la posibilidad de sufrir daño a la propiedad, heridas personales o la muerte.

Identifier	GUID-8935090F-D61D-41F4-ABC8-F4654D88B0FA
Status	Translation Validated

Guía del usuario de Windows, Mac, aplicación Mobile y Web

2019 - 06

Rev. A01

Contenido

Identifier	**GUID-1E29C798-6A65-41FB-8102-6**
Status	**Translation Validated**

1 Introducción

La *Guía del usuario de Dell Data Guardian* proporciona la información necesaria para instalar y usar Data Guardian en Windows, Mac, dispositivos móviles o un portal web.

Identifier	**GUID-6EE59323-7410-43F4-AD47-C5B7B04044E8**
Status	**Translation Validated**

Descripción general

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

- 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, .pdf.
- Protección básica de archivos: aplicaciones y tipos de archivos adicionales, como el Bloc de notas.
- 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.

NOTA:
El administrador le informará si su empresa utiliza Data Guardian solo con documentos de Office, con el almacenamiento en la nube o con ambos. El administrador también indicará las aplicaciones y los tipos de archivos adicionales que se pueden proteger.

Puede utilizar Data Guardian en las plataformas siguientes:

- Windows
- iOS
- Android
- Mac
- Portal web de Data Guardian, si el administrador lo configuró

NOTA:
Con Data Guardian se pueden abrir archivos cifrados por otras plataformas. Es posible que algunos archivos sean de solo lectura. La mayoría de la información de usuario acerca de Data Guardian para Mac se encuentra dentro del software en el formato de ayuda en línea.

Identifier	**GUID-C9552E05-51A1-4C2D-AADE-C078B4639CD4**
Status	**In Translation**

Opciones de cifrado para Data Guardian

Según el nivel de seguridad establecido por su empresa, el administrador establece las políticas para proteger los datos en reposo y los datos en movimiento. El administrador le indicará qué políticas se aplican a la empresa.

Esta lista proporciona una descripción general de algunas opciones de cifrado y, para algunas plataformas, la ubicación de la configuración de la política.

- Documentos de Office y modos
- Documentos de Office: Windows
- Documentos de Office: Mac, dispositivos móviles y portal web
- Opciones adicionales
- Cifrado en la nube
- Configuración de la política

Documentos de Office y modos

Se puede establecer la política para proteger documentos de Office. El comportamiento de cifrado puede variar según la plataforma y el modo. Para Mac, consulte la Ayuda en línea.

Modos	Documentos de Office
Opciones del Modo para **Windows y Mac**: **Modo Opt-in:** dispone de varias opciones para elegir qué documentos de Office proteger. • **Windows** y **Mac:** una carpeta de **Documentos seguros** se agrega a la raíz de la carpeta Documentos. Esto proporciona otra forma para cifrar un archivo. **Modo Force-Protected:** la empresa requiere un nivel mayor de seguridad. Data Guardian realiza un barrido para cifrar los archivos. • **Windows** y **Mac**: otra política puede agregar una carpeta **Documentos no protegidos** a la raíz de la carpeta Documentos. Coloque los documentos protegidos de Office o los tipos de protección básica de archivos en esta carpeta para descifrarlos. • **Mac**: protege los archivos en **\Users**. Estas plataformas no se basan en modos: • Móvil • Portal web	**Documentos de Office que se utilizan en Windows, Mac, dispositivos móviles y portal web** • .docx • .pptx • .xlsx • .docm • .pptm • .xlsm • .pdf: si se protegen con Data Guardian, abra con Adobe Acrobat Reader DC o Microsoft Word, pero no desde la red.

Documentos de Office: Windows

El administrador puede establecer políticas adicionales de Data Guardian para controlar o evitar la pérdida de datos a través de estas opciones. El comportamiento de cifrado puede variar según el modo.

Opciones para documentos de Office protegidos en Windows	Descripción
• Guardar: si un documento de Office está protegido, puede guardar nuevo contenido. (**Guardar como** aparece atenuada), • Guardar como protegido • Si un documento de Office ya está protegido, **Guardar como** aparece atenuada.	Otra información para Windows: • Para documento **No protegido** de Office puede seleccionar **Guardar**, **Guardar como** o **Guardar como protegido**. • Se muestra un borde rojo en correos electrónicos y documentos protegidos de Office.
Copiar/pegar y portapapeles	Puede copiar y pegar desde un documento de Office protegido a otro documento de Office protegido. No puede pegar desde un documento protegido a un documento desprotegido.

Opciones para documentos de Office protegidos en Windows	Descripción
Imprimir	Según la política, la impresión de un documento de Office protegido puede que sea permitido, que tenga una marca de agua o que esté deshabilitada.
Exportar (Windows y Office 2013 y superior, dispositivos móviles)	Según la política, es posible que sea permitido, que tenga una marca de agua o que esté deshabilitada. **NOTA:** Si se establece la marca de agua, se pueden exportar los documentos de Office. Los PDF no se pueden exportar.
Imprimir pantalla	Según la política, es posible que sea permitido o que esté bloqueada.
Procesos bloqueados Ejemplo: herramienta Recortes	Según la política establecida por su empresa, algunos procesos se bloquean cuando está abierto un documento de Office protegido.
Marca de agua en pantalla	Cuando se abre un documento protegido de Office, la pantalla muestra una marca de agua con el nombre de la computadora y el nombre de usuario.
Clasificación TITUS (Windows con modo Opt-in)	Si la política está activada, puede hacer clic con el botón secundario en un documento de Office y seleccionar una clasificación TITUS. Esto proporciona otra forma en que los usuarios protejan un documento de Office.
Clasificación de datos (Windows con modo Opt-in)	Si la política está activada y configurada para proteger información confidencial, como números de seguro social o de tarjeta de crédito, se cifran los documentos de Office que contienen dichos datos.

Documentos de Office: Mac, dispositivos móviles y portal web

El comportamiento de cifrado puede variar según la plataforma y el modo. El administrador le informará qué se aplica a su empresa.

Opción de cifrado	Descripción
Mac: interfaz Dell Data Guardian	**Mac:** cargar un documento protegido para cifrar. Descargar un documento protegido para descifrar. Después de editar un documento protegido, los cambios se guardan en el archivo original, ya sea en la nube o localmente.
Móvil: dentro de la aplicación Data Guardian • Imprimir • Marca de agua en pantalla • Marca de agua oculta • Exportar	**Mobile:** basada en la política: • Están protegidos los documentos de Office dentro de la aplicación Data Guardian. • La impresión de un documento protegido de Office es posible que sea permitido, que tenga una marca de agua o que esté deshabilitada. • Cuando se abre un documento protegido de Office, la pantalla muestra una marca de agua con el nombre de la computadora y el nombre de usuario.
Portal web • Marca de agua en pantalla	**Portal web:** puede cargar documentos protegidos o no protegidos, pero cualquier archivo que se carga está protegido cuando se hace clic en Descargar.

Opción de cifrado	Descripción
	Cuando se abre un documento de Office protegido, en la pantalla se muestra una marca de agua con el nombre de usuario y el nombre de la computadora.

Opciones adicionales

El comportamiento de cifrado puede variar según la plataforma y el modo. El administrador le informará qué se aplica a su empresa.

Opción	Descripción (modos Opt-in y Force Protect)
Protección básica de archivos: permite que se protejan los tipos de aplicaciones y archivos adicionales. (Windows, Mac, dispositivos móviles y portal web) • Ejemplos: .txt o .png **NOTA:** Actualmente, no se muestra ningún borde rojo en estos tipos de archivos, incluso cuando están protegidos.	El administrador puede configurar una política para especificar los tipos de aplicaciones y archivos que se deben cifrar. **Windows, Mac y dispositivos móviles**: estos archivos se barren y se encriptan. • **Mac**: para extensiones de archivo establecidas por el administrador, cifra esos tipos de archivos en la carpeta */Users*. **Portal web:** también se basan en la política, estos archivos pueden ser de solo lectura o editables por el usuario.
Compartir documentos de Office protegidos con **usuarios externos**. (Windows, Mac, dispositivos móviles y portal web) En una portada, se incluyen los vínculos de registro e información de la instalación de Data Guardian.	• Usuarios externos y **Windows:** también puede agregar una **restricción de fecha (embargo)** en documentos de Office protegidos y archivos PDF. • **Portal Web:** puede cargar archivos compartidos al portal web. No puede compartir un archivo desde el portal web, pero puede compartirlo después de que lo descargue.
Manipulado archivo o portada (Windows, Mac, dispositivos móviles y web)	Para archivos de Office, Data Guardian puede escanear documentos protegidos y detectar distintas formas de manipulación.
Grupos de acceso (entorno local) (Windows, Mac, dispositivos móviles y portal web)	Cuando el administrador habilita esta función, solo las personas en su grupo de acceso pueden ver archivos cifrados. Puede otorgar a usuarios internos y externos acceso a archivos individuales y estos pueden solicitar acceso. Según la política adicional, puede hacer clic con el botón secundario en un correo electrónico de Outlook etiquetado como [PROTEGIDO] y eliminar el acceso para usuarios individuales.
Perimetraje (dispositivos móviles)	Solo los usuarios de un área determinada pueden acceder a los archivos desde sus teléfonos móviles.
Cifrado de correo electrónico de Outlook (Windows)	Según la política, un botón *Proteger* le permite cifrar el contenido de un mensaje de correo electrónico y de los archivos adjuntos. Cuando se envía a usuarios externos, en una portada se incluyen los vínculos de registro e información de instalación de Data Guardian.

Alojado o local

Si debe instalar Data Guardian, el administrador confirmará qué opción se debe emplear para su empresa.

NOTA:
En el caso de las aplicaciones móviles, si tiene Workspace ONE instalado, puede autenticarlo con Data Guardian con Single Sign On.

Dell Security Center alojado	Dell Management Server local
Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security. Si su empresa es de varios grupos de usuarios, el administrador proporcionará una ID de instalación. Cuando se muestra un usuario que aún no tiene acceso a un documento protegido, se incluye en la portada la información acerca de la ID de instalación. Todas las plataformas: si un grupo de usuarios no paga durante un período específico, se puede suspender a ese grupo de usuarios.	Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security. El administrador le proporcionará el nombre de la URL del servidor Dell.

Cifrado en la nube

El comportamiento de cifrado puede variar según la plataforma y el modo. El administrador le informará qué se aplica a su empresa.

Plataformas	Descripción
Móvil	Consulte Utilizar protección en la nube con dispositivos móviles.
Mac	Consulte la ayuda en línea.
Portal web	Consulte la ayuda en línea.
Windows	Actualmente, la protección del cifrado en la nube de Data Guardian se deshabilitó en Windows para evitar problemas de compatibilidad con las funciones más recientes de los proveedores de servicio en la nube. Para ver los archivos .xen ya protegidos con el cifrado en la nube, utilice la aplicación móvil de Data Guardian, el portal web o Data Guardian con Mac.

Configuración de la política

Algunas plataformas incluyen una lista parcial de configuración de la política en su dispositivo.

Plataforma	Ubicación de configuración de la política
Mac	Panel *Preferencias*
Móvil	Icono **Configuración** > **Acerca de**
Portal web	Icono **Configuración** > **Acerca de**

Identifier	**GUID-DEFFD392-F513-445E-A87C-2CE7250245A2**
Status	**Translation Validated**

Soporte adicional

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

Identifier	**GUID-1DE0401E-4073-46BA-95E3-**
Status	**Translation Validated**

2 Requisitos

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

Identifier	**GUID-7C606C28-5532-4F36-AFA3-03126F14A6EF**
Status	**Translation Validated**

Dell Server

Data Guardian para Windows, Mac y dispositivos móviles requiere Servidor de administración de seguridad o Servidor virtual de administración de seguridad v9.6 o una versión posterior. El cliente web de Data Guardian requiere Servidor de administración de seguridad o Servidor virtual de administración de seguridad v9.8 o una versión posterior. A efectos del presente documento, a ambos servidores se les denomina como Dell Server, salvo que sea necesario mencionar una versión específica (por ejemplo, que un procedimiento sea diferente si se utiliza Security Management Server Virtual).

Identifier	**GUID-198D0A89-3C37-4C12-87A4-1F801B60DB21**
Status	**In Translation**

Data Guardian para Windows

- 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.
- Data Guardian es compatible con versiones específicas de Microsoft Office 2016 y también con Microsoft Office 365 Empresa y Empresa Premium. No es compatible con Office 365 Empresa Essentials.
- Data Guardian para Windows es compatible con Workspace ONE. El instalador de Data Guardian para Workspace ONE y una instalación MSI tienen una extensión .msi.
- Data Guardian v2.4 y versiones superiores en Windows es compatible con los entornos Air Gap, pero con ciertas limitaciones. Actualmente, no se admiten los datos de geolocalización en los eventos de auditoría ni en los archivos de embargo. La baliza web requiere una configuración.
- 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 en el comportamiento de los clientes de sincronización. Por lo tanto, los administradores y los usuarios 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.

- Los documentos protegidos de Office son compatibles con Mozy, una solución complementaria de Data Guardian, también con otros productos de almacenamiento en NFS, correo electrónico y nube.
- Aunque Dell Encryption no es necesario, si se usa, el cliente Encryption debe ser v. 8.12 o posterior.
- Data Guardian no es compatible con la herramienta de Restauración del sistema de Windows ni con Windows Insider Preview.
- La redirección de carpetas de Microsoft no es compatible con Data Guardian.
- Asegúrese de revisar periódicamente dell.com/support para obtener la documentación y la asesoría técnica más recientes.

Requisitos previos

Requisitos previos para archivo .exe

Si no se instaló todavía, el instalador instala el paquete redistribuible Microsoft Visual C++ 2017 (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.

Requisitos previos para archivo .msi

Debe instalar el paquete redistribuible de Microsoft Visual Studio C++ 2017 (x86 y x64).

NOTA:
Además, si se está ejecutando MSI, también debe instalar Visual Studio 2010 Tools para Office Runtime (x86 y x64).

Requisito previo general

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 realizando la instalación en un hardware de Dell o está realizando la actualización de Data Guardian en un hardware más antiguo de Dell, debe comprobar qué versión de .Net tiene instalada y, si fuera necesario, actualizar la versión antes de instalar 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, vaya a https://www.microsoft.com/en-us/download/details.aspx?id=42643.

Hardware

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

Sistemas operativos

La tabla siguiente indica los sistemas operativos compatibles.

Sistemas operativos Windows (32 bits y 64 bits)

- Windows 7 SP1: Enterprise, Professional, Ultimate
- Windows 8.1 actualización 0-1: Enterprise Edition, Pro Edition
- Windows 10: Education, Enterprise, Pro versión 1703 (Creators Update/Redstone 2) mediante la versión 1809 (October 2018 Update/ Redstone 5)

NOTA:
El cliente debe contar con uno de estos sistemas operativos o el sistema se bloqueará. Si es necesario, un ajuste en una clave de registro le permite al administrador anular el bloqueo.

Para tener compatibilidad con Redstone 4, debe actualizar el agente antes de actualizar el sistema operativo. Consulte https://www.dell.com/support/article/us/en/04/sln307922.

NOTA:
Data Guardian no es compatible con la Protección contra vulnerabilidades de seguridad de Windows Defender (WDEG, por sus siglas en inglés) en Redstone 3 y versiones posteriores, o con el Kit de herramientas de experiencia de mitigación mejorada (EMET, por sus siglas en inglés) en Redstone 2 y versiones anteriores.

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

Data Guardian no admite varias versiones de Office en un equipo.

Microsoft Office

Data Guardian admite las siguientes versiones de Office. Sin embargo, debe tener solo una versión instalada de Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019
- Office 365 ProPlus: versiones 1705, 1708 y 1803 (canal semestral)

Identifier	**GUID-371FFDE5-7A34-4288-AA88-617E73C0F9A4**
Status	**In Translation**

Data Guardian para Mac

A continuación se indica el hardware compatible con el cliente Mac.

Hardware de Mac

- Procesadores Intel Core 2 Duo, Core i3, Core i5, Core i7 o Xeon
- 2 GB RAM
- 10 GB de espacio de disco libre

Sistemas operativos

A continuación se indican los sistemas operativos compatibles.

Sistemas operativos Mac

- macOS Sierra 10.12.6
- macOS High Sierra 10.13.6
- macOS Mojave 10.14.4 - 10.14.5

Proveedores del almacenamiento en la nube

Según la configuración de la política, pueden mostrarse los elementos siguientes en la interfaz de Data Guardian para Mac. El usuario no tiene que descargar ni instalar el cliente de sincronización en la nube.

Proveedores del almacenamiento en la nube

- Dropbox
- Box
- Google Drive

  NOTA:
  Google Backup and Sync no es compatible.

- OneDrive
- OneDrive for Business

Microsoft Office

Data Guardian para Mac admite las siguientes versiones de Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-70934847-A1D7-4AD3-8822-A1E474D4ECD6
Status	In Translation

Data Guardian para aplicación móvil

A continuación, se indican los sistemas operativos compatibles con Data Guardian para dispositivos móviles.

Sistemas operativos Android

- 5.0-5.1.1 Lollipop
- 6.0-6.0.1 Marshmallow
- 7.0-7.1.2 Nougat
- 8.0-8.1 Oreo
- 9.0 Pie

Sistemas operativos iOS

- iOS 10.x-10.3
- iOS 11.x-11.4.1
- iOS 12.x - 12.1.4

Sistema operativo del Chromebook

Se requiere Chrome OS versión M53 o posterior para ejecutar aplicaciones de Android en Chrome OS. Estos dispositivos se validan para ejecutar aplicaciones de Android en Chrome OS, pero se debe confirmar su opción al representante de ventas:

- https://www.chromium.org/chromium-os/chrome-os-systems-supporting-android-apps

Microsoft Office

La aplicación Data Guardian para móvil puede abrir archivos creados con las siguientes versiones de Office.

Microsoft Office

- Office 2013 SP1
- Office 2016
- Office 2019

Identifier	GUID-E0E57A65-225C-46FB-9E51-60FAC92BA57A
Status	In Translation

Data Guardian para web

Para habilitar el cliente web de Data Guardian, el administrador configura una máquina virtual que aloja al cliente web y lo comunica con Dell Server v9.8 o una versión posterior.

Los siguientes entornos virtualizados se pueden usar para implementar el cliente web Data Guardian.

Entornos virtualizados

- **VMware ESXi 6.7**
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - 8 GB de RAM como mínimo, recomendado
  - No es necesario un sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obtener una lista completa de sistemas operativos de host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
  - Consulte http://pubs.vmware.com/vsphere-67/index.jsp para obtener más información
- **VMWare ESXi 5.5**
  - CPU de 64 bits x86, necesario
  - Equipo host con un mínimo de dos núcleos
  - 8 GB de RAM como mínimo, recomendado
  - No es necesario un sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obtener una lista completa de sistemas operativos de host admitidos
  - El hardware debe cumplir con los requisitos mínimos de VMWare
  - 4 GB de RAM como mínimo, para el recurso de imágenes dedicado
  - Visite http://pubs.vmware.com/vsphere-55/index.jsp para obtener más información
- **Microsoft Hyper-V**
  - Procesador de 64 bits con Traducción de Direcciones de Segundo Nivel (SLAT)
  - 8 GB de RAM como mínimo, recomendado
  - Hardware que cumpla con los requisitos mínimos de Hyper-V
  - Consulte https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/reference/hyper-v-requirements para obtener más información.

NOTA:
Estos requisitos mínimos representan 25 (o menos) conexiones simultáneas a un único portal web.

Proveedores del almacenamiento en la nube

Según la configuración de la política, en el portal web de Data Guardian se puede acceder a estos proveedores de almacenamiento en la nube.

Proveedores del almacenamiento en la nube
• OneDrive for Business

Microsoft Office

Data Guardian para Web puede abrir archivos creados con las siguientes versiones de Office.

Microsoft Office
• Office 2013 SP1
• Office 2016
• Office 2019

Identifier	**GUID-F414365D-DE5B-4703-88AB-FCB73F3BD14D**
Status	**Translation Validated**

Otros requisitos

Actualmente, la autentificación multifactor (MFA) de Amazon Cognito no es compatible con ninguna plataforma Data Guardian.

Identifier	**GUID-E2815EA1-85AF-4049-B317-DF016FBA39EE**
Status	**Translation Validated**

Navegadores web

Puede utilizar Data Guardian con Internet Explorer, Mozilla Firefox, Google Chrome y Microsoft Edge.

En el caso de los dispositivos Mac, también es compatible el navegador Safari.

Identifier	**GUID-582A5665-D2A2-4B98-A51D-5F14376D98BA**
Status	**Translation Validated**

Adobe Acrobat

En el caso de los dispositivos Windows y Mac, los archivos .pdf protegidos se pueden abrir con Adobe Acrobat Reader DC.

NOTA:

Los siguientes no son compatibles: Adobe Acrobat *Standard* DC, Adobe Acrobat *Pro* DC y Adobe Acrobat DC.

Identifier	GUID-36045ECC-D303-4A63-9ABA
Status	In Translation

Instalar o desinstalar Data Guardian en Windows

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

Después de instalar Data Guardian, esté preparado para reiniciar el equipo.

Identifier	GUID-D0717325-F700-400C-BC03-5FD8190A81A9
Status	In Translation

Descripción general de las tareas de instalación para Windows

En esta descripción general se resume la secuencia para instalar 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 forma interactiva en Windows. Reinicie y continúe con el siguiente paso.
Confirme el estado de activación	Confirme en el área de notificaciones que el icono de Data Guardian tiene una marca de verificación verde  .	Si el ícono tiene un signo de exclamación naranja, consulte Posibles problemas de activación: nube y Office protegido. **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.

Opciones para Windows

Tarea	Descripción	Para obtener más información
Ver el menú del área de notificaciones	Ofrece información útil acerca de archivos, carpetas y solución de problemas.	Comprender los elementos del menú del área de notificaciones de Data Guardian

Identifier	GUID-B54EDFCA-AFBB-4BD0-8427-515A3E052962
Status	In Translation

Carpetas preexistentes con archivos sin cifrar

Antes de implementar Data Guardian, es preferible que los dispositivos de destino no tengan configurada una cuenta de almacenamiento en nube.

Si la cuenta de un proveedor de almacenamiento en la nube está configurada con carpetas sincronizadas con el equipo local antes de la instalación de 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

Identifier	GUID-7BBFA9B6-C19E-44E8-908C-F5AF181462C8
Status	In Translation

Instalación interactiva de Data Guardian en Windows

Debe ser un administrador local para instalar Data Guardian. Si los usuarios instalarán el producto, infórmeles la ubicación de los medios de instalación.

Antes de empezar

En función del entorno y del producto Data Guardian, determine cuál de los siguientes elementos necesita:

Dell Security Center alojado	Dell Management Server local
Si su ambiente alojado es para varios inquilinos, necesitará una ID de instalación.	Asegúrese de conocer el nombre del Dell Server.

Instalar Data Guardian

Después de instalar 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 y cópielo en la computadora local. A continuación, se incluyen los nombres de instalador de muestra:
   - Dell Security Center alojado: los nombres del instalador tienen una extensión .exe
   - local: los nombres del instalador tienen una
     - extensión .exe
     - extensión .msi para Workspace ONE y una instalación de MSI
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 Microsoft Visual C++ 2015 o el perfil de cliente Microsoft .NET Framework 4.5.2, haga clic en **Aceptar**.
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:\Program Files\Dell\Data Guardian\.

No instale Data Guardian en las carpetas C:\Users o C:\Windows ni en la raíz de cualquier unidad.

10 Seleccione una de estas opciones:

Dell Security Center alojado	Dell Management Server local
Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security.	Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security.
a Seleccione **Dell Security Center alojado**. b De manera opcional, si su empresa cuenta con varios inquilinos, ingrese una ID de instalación. **NOTA:** Si su empresa cuenta con varios inquilinos y no ingresa una ID de instalación, el administrador puede agregarla más tarde al registro. c Haga clic en **Continuar**. d Siga con el paso 11.	a Seleccione **Dell Management Server local**. b En el campo *Nombre de Dell Management Server:* ingrese el nombre del Dell Server con el que se comunicará esta computadora, como servidor.dominio.com. No es necesario incluir www o http(s). Esta información la proporciona el administrador. **NOTA:** No desmarque la casilla *Activar verificación de confianza en SSL* a menos que lo indique el administrador. c Haga clic en **Siguiente**. d En la pantalla Confirmar información de Dell Management Server, confirme si la dirección URL del Dell Server es correcta. El instalador agrega www o http(s) y el puerto. Haga clic en **Siguiente**. e Siga con el paso 11.

11 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.

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

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

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

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

La instalación de Data Guardian se ha completado.

15 Los usuarios deben confirmar la activación. El icono del área de notificaciones de Data Guardian debería tener una marca de verificación verde  .

NOTA:

En función de la manera en que se implemente Data Guardian dentro de la empresa, puede que la activación no sea inmediata. Sin embargo, si no se produce la activación, el usuario debe realizar una activación manual.

Identifier	**GUID-AF4BEC71-F3FB-43E9-A588-FA2C2BC7E4BD**
Status	**Translation Validated**

Posibles problemas de activación: nube y Office protegidos

Si ha instalado Data Guardian, pero el icono de Data Guardian del área de notificaciones 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:

Opción de Data Guardian	Posible problema
Office protegido	• 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.
Cifrado en la nube	• 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

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.

Identifier	**GUID-10DDD78A-61B2-4AE9-9DF4-0527FEE42D0D**
Status	**In Translation**

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 el área de notificaciones, se muestra el icono de un escudo con un signo de exclamación naranja.

2 Haga clic en el icono de **Data Guardian** en el área de notificaciones y seleccione **Activación de usuario**.

3 Ingrese 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 del área de notificaciones de Data Guardian  .

4 Confirme el estado de su modo de usuario. Haga clic en el icono del área de notificaciones 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 Utilizar Data Guardian como usuario externo.

> **NOTA:**
> Si el Modo de usuario indica **No registrado**, Data Guardian aún no está activado.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center alojado y grupo de usuarios suspendido

Con Dell Security Center alojado, si un grupo de usuarios no realiza pagos durante un período específico, se puede suspender a ese grupo de usuarios. Esto aplica para Windows, Mac, dispositivos móviles y portales web.

Los usuarios internos y externos de Data Guardian pueden experimentar lo siguiente:

- Todas las plataformas: si intenta instalar Data Guardian, activarlo o iniciar sesión, aparece un cuadro de diálogo en el que se indica que un grupo de usuarios está suspendido.
- Mac: si el grupo de usuarios se suspende mientras Data Guardian está abierto, aparece el diálogo de grupo de usuarios suspendido después de que cierra Explorer y todos los archivos e intenta abrir un archivo protegido.
- Portal web:
  - Si ya inició sesión y carga un archivo cifrado, aparece un mensaje que se indica que la carga falló.
  - Si se carga un archivo cifrado o no cifrado y, luego, se suspende el grupo de usuarios, aparece un mensaje en el que se indica que la descarga falló.
  - Si se cierra la sesión e intenta iniciar sesión otra vez, aparece un cuadro de diálogo que indica que el grupo de usuarios se encuentra suspendido.

Póngase en contacto con el administrador.

Identifier	**GUID-43BA606D-3F31-4E67-97B4-039DE9CEBC65**
Status	**In Translation**

Comprender los elementos del menú del Área de notificaciones 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 buscar un nombre de archivo, 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 con el botón secundario en el icono del área de notificaciones 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:** usuario con una dirección en este dominio

- **Usuario externo**: un usuario con una dirección fuera de este dominio
- **No registrado**: usuario interno o externo cuyo Data Guardian no está activado

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: Dell 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 que generó el Dell Server.

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

Nombre: nombre del archivo

Nube: esta función se deshabilitó por lo que ya no tiene datos.

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: esta función se deshabilitó.

Explorador creado: *Verdadero* o *Falso*.

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

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

Anteriormente, el cifrado en la nube de Data Guardian tenía un área de **Carpetas** en la pantalla Detalles. Actualmente, el cifrado en la nube está deshabilitado.

Identifier	**GUID-5726752F-D15C-479E-8E8E-6BBE27B23F90**
Status	**Translation Validated**

Comprobar si existen actualizaciones de políticas

Si el administrador modifica una política y le notifica una actualización de políticas, vaya al área de notificaciones de Windows, haga clic en el icono de **Dell 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.

Identifier	**GUID-62C18A73-A619-46BF-BE3A-76911412C43A**
Status	**Translation Validated**

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.

Identifier	**GUID-E67381E8-70C7-46BE-A822-9B5C48B0FFC3**
Status	**Translation Validated**

Actualizar Data Guardian

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

Identifier	**GUID-CC8C1B76-3E85-415F-AAE0-3C20521D70A6**
Status	**In Translation**

Desinstalar Data Guardian en Windows

Si el administrador ha sido el encargado de instalar Data Guardian, solo él debe 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.

Identifier	**GUID-FB8AEF07-F76C-4E52-9920-B56A973DB1E6**
Status	**In Translation**

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 esos archivos en su unidad local.

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. O bien puede verlos en el portal web de Data Guardian.

Desinstalar Data Guardian

1 Use el panel de control de Windows para desinstalar el programa.
2 Seleccione **Dell 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 Se muestra una advertencia para la desinstalación de Dell 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 Si un cuadro de diálogo indica que el usuario tiene un documento de Office abierto, haga clic en **Aceptar**, cierre el documento de Office e inicie de nuevo la desinstalación.
9 Haga clic en **Finalizar** cuando aparezca la pantalla Completado.
10 Haga clic en **Sí** para reiniciar.

La desinstalación de Data Guardian se ha completado.

Identifier	**GUID-05F5667F-C3BE-4C5E-B64D-5629C60C049D**
Status	**Translation Validated**

Proporcionar comentarios a Dell

Si el administrador habilitó los comentarios, puede proporcionar comentarios a Dell acerca de este producto. El breve formulario incluye dos preguntas sobre su nivel de satisfacción, con una escala de comentarios y una escala de clasificación (donde 10 indica el nivel de satisfacción más alto).

Para acceder, haga clic en el icono de Data Guardian del área de notificaciones y seleccione **Enviar comentarios**.

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

Identifier	GUID-E68E0B8D-7519-4C11-A918-
Status	In Translation

Utilizar Data Guardian con Windows

El administrador ya configuró las políticas para proteger los documentos y le indicará cuáles de estas opciones se aplicarán a la empresa.

Identifier	GUID-162A20CF-D1AD-4701-9A28-1000DB2FE1D4
Status	In Translation

Descripción general de opciones

En esta descripción general se resumen las opciones posibles para Data Guardian según la política establecida por el administrador. Estos documentos estarán seguros cuando los comparta con otros o los almacene en un medio extraíble.

Opción	Descripción	Para obtener más información
Documentos de Office y habilitados para macros	Estos incluyen .docx, .pptx, .xlsx, .docm, .pptm, .xlsm y .pdf.	Consulte Observar opciones del menú Archivo para determinar el nivel de seguridad de los documentos de Office. Tendrá uno de estos modos: • Opt-in • Force-Protected
Protección básica de archivos	Estas son aplicaciones y tipos de archivos adicionales que su empresa desea cifrar y que configuró el administrador.	Consulte Proteger los tipos de aplicaciones y archivos adicionales con protección básica de archivos.
Opciones adicionales	Es posible que se apliquen a documentos de Office, archivos básicos o ambos.	Consulte Opciones adicionales para Data Guardian.
Compartir un archivo con un usuario externo	Usuario que tiene una dirección de correo electrónico que no sea del dominio, ya sea alguien de otra empresa o un usuario interno, que desee acceder a archivos protegidos de una dirección de correo electrónico que no sea del dominio.	Consulte Utilizar Data Guardian como usuario externo.

Trabajar en línea con documentos protegidos

Al crear documentos protegidos, la práctica recomendada es trabajar en línea debido a que se generan claves para esos documentos. Si se recrean imágenes en su computadora y creó documentos protegidos sin conexión, notifíqueselo al administrador.

Propiedades del archivo > pestaña Dell Data Guardian

Con documentos de Office protegidos, puede hacer clic con el botón secundario y seleccionar **Propiedades**. Se muestra la pestaña **Dell Data Guardian** con información como la ID y la clave de acceso del archivo y los datos de embargo.

Íconos de superposición para Windows

En el caso de Data Guardian 2.2 y superior, se muestran íconos de superposición en los archivos protegidos en el Explorador de archivos. Si hace clic con el botón secundario en ese archivo protegido, se le proporciona más información en una pestaña de Dell Data Guardian.

Marca de agua oculta

En función de las políticas establecidas por el administrador, los documentos de Office protegidos pueden tener una marca de agua oculta que identifica al usuario. Si imprime o comparte el documento, la marca de agua persiste.

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.

Identifier	**GUID-E88C0771-29BE-4292-AD26-F913747EE0FC**
Status	**Translation Validated**

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
- .pdf

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 secundario 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.
- Abrió 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.

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.
  - *Recurso compartido* está activado.
  - Carpeta **Documentos > Documentos seguros**: con el Modo Opt-in (pero no con el modo Force-Protected) se agrega 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.
  - *Recurso compartido* está desactivado.

    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.
  - Carpeta **Documentos > No protegidos:** si se activa mediante la política en modo Force-Protected (pero no en modo Opt-in), se agrega una carpeta no protegida a la raíz de la carpeta Documentos. Los documentos de Office incluidos en esta carpeta están descifrados. Si elimina la carpeta, se vuelve a crear.

- 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 agregando 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.

Identifier	**GUID-077EC2B6-61AD-4F13-95D0-CF91EF0143AF**
Status	**In Translation**

Utilizar el modo Opt-in para proteger documentos de Office

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

Trabajar con las opciones del menú Archivo para modo Opt-in

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
Abra el archivo	Los archivos se abren como de costumbre
Guardar	• Opciones: El documento ya está protegido: esta opción guarda el documento como protegido. No protegido: 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 abre la ventana *Guardar como* y debe guardarlo con un nombre de archivo diferente.
Guardar como	Tiene las opciones estándar (pero no el Modo protegido)
Guardar como protegido	La única opción en el campo Guardar como tipo es Protegido de Office
Imprimir	**Habilitado** Sin embargo, para documentos de Office protegidos, si un administrador inhabilita la opción Imprimir a través de la política, puede seleccionar Imprimir, pero se despliega un mensaje que indica que el documento protegido no se puede imprimir. Si su administrador le permite Imprimir, es posible que otra política ponga una marca de agua, que contenga el nombre de usuario, el nombre de dominio y la ID. de equipo en cada página cuando realice la impresión.
Compartir	**Habilitado** para documentos de Office protegidos. **Deshabilitado** para documentos desprotegidos.
Exportar (Office 2013 y superior)	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. 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 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 un macro como no protegido, debe cerrarlo y volver a abrirlo para que el macro se ejecute.

Clasificación TITUS y modo Opt-in

Si está activada la política, el administrador configura algunas clasificaciones TITUS para cifrar un documento con esa clasificación. Puede hacer clic con el botón secundario en un documento no protegido de Office y seleccionar la clasificación TITUS. Esto proporciona otra forma de proteger un documento de Office.

Clasificación de datos y modo Opt-in

Si está activada esta política, el administrador puede establecer clasificaciones de contenido específico, como Número de Seguro Social, número de tarjeta de crédito u otra información confidencial. El administrador le informará qué información se ha clasificado. Cuando guarda un documento que contiene información en función de dichas reglas de clasificación, se cifra el documento.

Si utiliza etiquetas en un documento de Office para generar una clasificación de datos utilizada en los metadatos de etiqueta del archivo de la política, la etiqueta que utiliza en el documento de Office distingue mayúsculas de minúsculas y debe coincidir con la mayúscula que utiliza el administrador en la política.

NOTA:

Si se habilita esta política, los archivos que cumplen con las reglas de clasificación se cifrarán en un barrido. No obstante, cuando cree el archivo, puede hacer clic con el botón secundario y seleccionar **Proteger archivo**.

Consulte también Cifrado de correo electrónico de Outlook con Data Guardian.

Solución de problemas para el modo Opt-in

Si la política de Data Guardian deshabilitó la impresión para documentos de Office protegidos, puede seleccionar Imprimir en **Archivo > Información** o hacer clic con el botón secundario en un archivo de Office protegido en el Explorador de Windows. 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 Opt-in y desea confirmar si el documento está protegido o no, ábralo y la barra de título lo mostrará como protegido.

NOTA:

Si tiene activado el modo Force-Protected, todos los documentos de Office están protegidos.

Identifier	**GUID-5E368002-F3BB-48A7-9A30-B4591019B21F**
Status	**In Translation**

Utilizar el modo Force-Protected para proteger documentos de Office

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

- Trabaje con opciones del menú Archivo para el modo Force Protected

Trabaje con opciones del menú Archivo para el modo Force Protected

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 Force-Protected para protegido y no protegido
Abra el archivo	Los documentos no protegidos se abren en modo de solo lectura.
Guardar	· 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).
Guardar como	**Deshabilitado**
Guardar como protegido	La única opción en el campo Guardar como tipo es Protegido de Office
Imprimir	**Habilitado** Sin embargo, para documentos de Office protegidos, si un administrador deshabilita la opción Imprimir a través de la política, aún puede seleccionar Imprimir, pero se despliega un mensaje que indica que el documento protegido no se puede imprimir. Si su administrador le permite Imprimir, es posible que otra política ponga una marca de agua, que contenga el nombre de usuario, el nombre de dominio y la ID. de equipo en cada página cuando realice la impresión.
Compartir	**Deshabilitado**
Exportar (Office 2013 y superior)	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.

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.

Identifier	GUID-669244A9-0658-46A3-A9EB-A5D349D7EDBC
Status	In Translation

Opciones adicionales para Data Guardian

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.

Pegar

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

- Puede copiar y pegar datos protegidos o desprotegidos en el documento original protegido o en un PDF protegido. Sin embargo, no es posible tener archivos .pdf sin protección abiertos en Acrobat Reader DC.
- 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.

Apertura y edición de un PDF protegido con Adobe Acrobat Reader DC

Cuando se utiliza Acrobat Reader DC:

- El usuario puede agregar anotaciones a un archivo .pdf protegido o completar un formulario. Cuando guarda el archivo, se crea un nuevo archivo .pdf protegido en el que se incluyen los cambios. Esto es una funcionalidad de Acrobat Reader DC.
- Para mejorar la seguridad, cuando se abre un archivo .pdf protegido con Acrobat Reader DC, se bloquea el acceso a Internet hasta que se cierre este programa.
- Para mejorar la seguridad, si un archivo .pdf está abierto, un usuario no puede enviar un correo electrónico desde esa instancia.

> **NOTA:**
> No puede abrir un archivo .pdf protegido desde la red. Puede utilizar Word para abrir un archivo .pdf protegido desde la red.

Imprimir sobres y etiquetas

Si el administrador ha definido una política para agregar una marca de agua cuando se imprime 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 ingresar 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.

Opciones adicionales

Procesos bloqueados

Según las políticas que define el administrador, es posible que se bloqueen algunos procesos, como la herramienta Recortes. El administrador le informará de esos procesos. Además, un cuadro de diálogo le informa que se bloqueó el proceso.

- **Modo Force-Protected:** si el administrador establece una política para bloquear el botón *PrtScr*, es posible que también se bloquee la capacidad de utilizar la pantalla táctil o tabletas para imprimir las pantallas.
- Windows con RS5 tiene una aplicación de anotación en captura de pantalla (anteriormente la herramienta Recortes). Con Data Guardian, el administrador puede activar una política que bloquea esta aplicación para mejorar la seguridad.

Adjuntar un documento protegido a un correo electrónico de Outlook

Cuando adjunte un documento 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.

Puede adjuntar un documento de Office protegido, un tipo de archivo protegido adicional basado en una política, o bien un archivo .xen.

Para Windows con Data Guardian, si adjunta un documento protegido, Data Guardian agrega información para acceder al archivo cifrado dentro de ese correo electrónico.

- Usuarios internos: la información se muestra con un vínculo para descargar un cliente.
- Usuarios externos: la información se muestra con un vínculo para el registro y la descarga de un cliente.

NOTA:
Para que se muestre la información agregada, debe enviar un correo electrónico desde Microsoft Office Outlook, no en la versión web de Outlook.

Cifrado de correo electrónico de Outlook con Data Guardian

En función de la política con Data Guardian versión 2.0.1 y versiones posteriores, los usuarios internos cuentan con la opción *Proteger* en la parte superior izquierda de Outlook para cifrar el correo electrónico y los archivos adjuntos. El emisor y el receptor deben tener Data Guardian instalado y activado.

El cifrado de correo electrónico de Outlook de Data Guardian es compatible con Office 2013 y versiones posteriores, pero no con el correo web.

Para utilizar la opción:

1 Haga clic en **Proteger** en la esquina superior izquierda.
2 En el caso de una dirección de correo electrónico externa, haga clic en **Sí** para confirmar el uso compartido de claves o **No** si decide no enviar el correo electrónico.

La práctica recomendada es tener un correo electrónico abierto a la vez. Si tiene más de uno abierto, asegúrese de hacer clic en el correo electrónico para enfocarlo antes de hacer clic en el botón Proteger. El botón Proteger debe atenuarse cuando no coloca el puntero sobre él.

Los datos en movimiento son seguros. En esta versión preliminar, la prevención de pérdida de datos (DLP) para los datos en reposo es parcialmente compatible. Las próximas versiones mejorarán la seguridad.

Para minimizar la DLP cuando se abre un correo electrónico cifrado, algunas acciones están desactivadas o bloqueadas:

- *Pasos rápidos* de Outlook
- *Mover*, *Mover a la carpeta* y acciones adicionales de la carpeta
- Flechas *Siguiente* y *Anterior*
- *Reenviar*
- Algunas opciones del botón secundario

Para minimizar la DLP cuando un correo electrónico cifrado está abierto, se controlan estas acciones:

- *Copiar/Pegar*
- *Imprimir* y *Exportar* datos
- Algunas opciones del botón secundario
- Carpeta de borrador y *Guardado automático*

Para destinatarios de correo electrónico de Outlook

Cuando abre un correo electrónico cifrado de Outlook, se muestra una advertencia que indica que el documento está protegido y el usuario debe hacer doble clic para abrir el archivo. No se muestra ningún contenido de correo electrónico en la vista previa, sino solo una portada. En la portada se indica el nombre para Dell Server local o una ID de instalación para ese grupo de usuarios específico si el Dell Security Center alojado es de varios grupos de usuarios. La portada también incluye vínculos para descargar el cliente Data Guardian.

Clasificación de correo electrónico

Informe local para documentos de Office protegidos cifrados con clasificación de datos (modo Opt-in)

Para proteger la información confidencial en documentos de Office y archivos PDF, el administrador puede establecer una política para barrer los archivos y luego cifrarlos en función de la clasificación de datos. Es posible que la información confidencial incluya números de seguro social, números de tarjeta de crédito, direcciones en Estados Unidos o datos específicos de la empresa. El administrador le informará de la información confidencial que causará que se cifren los archivos.

Para ver un informe local de archivos cifrados debido a la clasificación de datos y el motivo de aquel cifrado:

1 Vaya a **C:\Users\<nombre de usuario>\AppData\Local\Dell\Data Guardian**.

2 Abra el archivo **Classification Report.log**.

NOTA:
Si un archivo está en el proceso de cifrado, es posible que la entrada tenga varias líneas hasta que se complete el cifrado.

Identifier	**GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B**
Status	**In Translation**

Proteger los tipos de aplicaciones y archivos adicionales con protección básica de archivos

El administrador informará si las políticas permiten cifrar los tipos de aplicaciones y archivos adicionales. Si alguien abre un archivo cifrado con protección básica de archivos, pero no tiene instalado Data Guardian, el contenido será ilegible.

Descripción general de protección básica de archivos

Aplicaciones

Estos son ejemplos de aplicaciones que posiblemente el administrador necesite cifrar:

- Bloc de notas
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Algunas aplicaciones son solo parcialmente compatibles con Data Guardian y el administrador le informará sobre aquellas.

Tipos de archivos

Estos son ejemplos de tipos de archivos adicionales que se pueden configurar: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac y dispositivos móviles

Cuando está configurada la política de protección básica de archivos, Data Guardian realiza un barrido de las computadoras de los usuarios y cifra todos los archivos locales con dichas extensiones. Los archivos cifrados con protección básica de archivos solo se pueden ver y editar con la aplicación asociada con la extensión de archivo.

> **NOTA:**
> Los archivos en carpetas específicas del sistema no se cifran, por ejemplo, AppData. Además de las carpetas que se relacionan con documentos de Office protegidos, por ejemplo, la carpeta de documentos seguros.

Íconos de superposición para Windows

En el caso de Data Guardian 2.2 y superior, se muestran íconos de superposición en los archivos protegidos en el Explorador de archivos. Si hace clic con el botón secundario en ese archivo protegido, se le proporciona más información en una pestaña de Dell Data Guardian.

Excluir algunos archivos del barrido en Windows o Mac (antes de habilitar el barrido)

Si su empresa decide cifrar un tipo de archivo adicional, como. txt, es posible que no desee ni necesite que todos los archivos con esa extensión se barran y cifren.

Antes de habilitar la protección básica de archivos para esa extensión, el administrador puede configurar otra política que le permite agregar una carpeta a la computadora local, y los archivos de esa carpeta no se barren. El administrador puede establecer una política, crear un nombre de carpeta, proporcionar el nombre de la carpeta y sugerir dónde puede agregar esa carpeta. Estos pueden ser archivos necesarios para el sistema o archivos que no requieren protección.

> **IMPORTANTE:**
> Debe crear la carpeta antes de que el administrador habilite la política de protección básica de archivos.

1. Utilice el nombre de la carpeta y la ruta proporcionada por el administrador.
   - En el caso de Mac, vaya a **Panel de preferencias > Exclusiones de protección básica de archivos**. Aquí se muestra el nombre de la carpeta que se va a crear y la ruta.
2. Agregue archivos que no se deben cifrar con la extensión especificada, como .txt. De manera opcional, puede agregar subcarpetas con nombres creados por el usuario.

NOTA:
Si tiene archivos con esa extensión que se cifraron anteriormente, colocarlos en esa carpeta no los descifrará. Permanecen cifrados. Si tiene una carpeta de **Documentos no protegidos**, que el administrador puede crear a través de otra política, puede colocar tipos de protección básica de archivos en esta carpeta para descifrarlos.

3 Después de habilitar la protección básica de archivos, si tiene archivos no protegidos con esa extensión en una red o una unidad externa, puede copiarlos en la carpeta excluida. Permanecen sin cifrar. De lo contrario, se cifran.

Si la computadora tiene más de un usuario, solo el usuario que tenga la sesión iniciada actualmente puede colocar archivos en esa carpeta y excluirlos del barrido. Se barrerá o cifrará cualquier archivo que otro usuario coloque en la carpeta.

Eliminación de una extensión de archivo en Windows o Mac

El administrador puede optar por quitar una extensión de archivo. Si es así, se realiza un barrido en su computadora para descifrar esos tipos de archivo.

- La pestaña *Propiedades* > *Dell Data Guardian* del archivo cifrado deja de aparecer.
- Si tenía íconos superpuestos de archivo, estos dejarán de aparecer.
- El descifrado de archivos puede tardar varios minutos en completarse. Si un archivo con esa extensión sigue cifrado, es posible que se abriera durante el barrido o que esté almacenado en un servidor de archivos o en otra ubicación.

Comuníquese con el administrador para solicitar la recuperación de cualquier archivo con esa extensión que no esté descifrado.

Aplicaciones de Office

Puede utilizar una aplicación de Office para abrir un archivo cifrado con protección básica de archivos, pero el contenido es de solo lectura.

Portal web

En Configuración > Políticas, si la Protección básica de archivos está configurada en "True", el administrador agregó tipos de archivos que no son de Office, los cuales Data Guardian cifrará cuando se descarguen del portal web. El administrador debe indicarle los tipos de archivo.

NOTA:
Si carga un tipo de archivo que aún no es compatible, el contenido será ilegible en el portal web.

Puede cargar tipos de archivos que no sean de Office, sin importar si están cifrados o sin cifrar. Sin embargo, cuando descarga un archivo que no sea de Office, la extensión de archivo varía.

Archivos que no son de Office (como .txt o .png)	Descripción de la descarga
Cifrados antes de cargarlos Por ejemplo: archivos que no son de Office ya cifrados por Windows o Mac.	Cuando se descargan desde el portal web, mantienen la extensión de archivo, como .txt o .png.
Archivos no cifrados	Cuando se descargan desde el portal web, la extensión del archivo varía dependiendo de si el administrador agregó la extensión a una política. Sin embargo, están cifrados. Ejemplos de un archivo .txt descargado desde el portal web: • **nombredelarchivo.txt**: el administrador agregó el tipo de archivo .txt a una política. • **nombredelarchivo.txt.xen**: el tipo de archivo .txt no está incluido en la política. Se cifra el archivo, pero se agrega una extensión .xen.

Si está activada la política *Editar* en el portal web, los usuarios pueden editar los archivos que no son de Office.

Identifier	**GUID-801B897D-9A0F-48C0-B46C-A3726B8BD9E4**
Status	**Translation Validated**

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 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.

Identifier	**GUID-A8209D75-E380-4809-A55A-CF89E3FBE29A**
Status	**In Translation**

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

Si tiene una carpeta de cliente sincronizada en su computadora y Data Guardian la cifra, esos archivos se cifran en la nube.

Si utiliza el portal web de Data Guardian para cifrar los archivos, estos pueden cifrarse como archivos .xen. No puede abrir archivos .xen cifrados en Windows. Puede verlos en un dispositivo móvil con Data Guardian o el portal web.

Identifier	**GUID-7A2816C4-2882-4B5B-B2C6-A8032B1C4508**
Status	**Translation Validated**

Compartir documentos de Office protegidos con usuarios externos

Con Data Guardian, puede compartir un documento de Office protegido a través de correo electrónico, medios extraíbles, un recurso compartido de red o puede cargarlo en la nube y compartirlo:

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

Cuando adjunte el documento y haga clic en *Enviar*, aparece un cuadro de diálogo de confirmación para recordarle que la clave para ese documento protegido se compartirá con el usuario externo.

Mejorar la seguridad agregando restricciones de fecha

Si lo desea, 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 En el menú desplegable, seleccione una 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 guarda, se protege, se cierra y se vuelve 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, 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 establece el campo de *fecha de inicio* en una fecha u hora posterior y el usuario externo abre el archivo antes de tiempo, aparece un mensaje que explica que el archivo no se puede abrir hasta la fecha y la hora indicadas debido a restricciones de acceso.

Identifier	GUID-FFED5E16-B72A-4858-A64D-
Status	Translation Validated

Instalar y utilizar Data Guardian con Mac

Data Guardian para Mac tiene una ayuda integrada para pantallas específicas que proporcionan información sobre:

- Interfaz de Dell Data Guardian en la que los usuarios pueden cargar archivos para cifrarlos
- Cifrado en la nube
- Usuarios externos y restricciones de acceso
- Manipulación

En la interfaz de Dell Data Guardian para Mac, haga clic en el icono Ayuda.

Identifier	GUID-0DB59561-F614-4FEB-9265-6F2711737741
Status	Translated

Instalar cliente para Mac

Si el administrador lo agregó a su lista blanca de empresas, puede registrarse en: https://yoursecurityservername.domain.com:8443/cloudweb/register.

Tras registrarse, recibirá un correo electrónico que lo dirige a https://yoursecurityservername.domain.com:8443/cloudweb para que inicie sesión y descargue el cliente apropiado.

Debe ser un administrador local.

Para instalar Data Guardian para Mac:

1 Para el cliente de Data Guardian, localice el instalador en **Dell-Data-Guardian-Mac-0.x.x.xxxx.dmg.**
2 Utilice el archivo **.pkg** almacenado en Dell-Data-Guardian-0.x.x.xxxx.dmg para instalar o actualizar.
3 Haga doble clic en el paquete **Dell-Data-Guardian-x.x.x**.
4 Haga clic en **Continuar**.
5 En la ventana Introducción, haga clic en **Continuar**.
6 En la ventana Contrato de licencia de software, haga clic en **Continuar**.
7 Haga clic en **Aceptar** para continuar.
8 En la ventana Tipo de configuración, seleccione una de estas opciones:

Dell Security Center alojado	Dell Management Server local
Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security. a Seleccione **Dell Security Center alojado**. b Haga clic en **Continuar**. c Siga con el paso 9.	Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security. a Seleccione **Dell Management Server local**. b En el campo *Nombre de Dell Management Server:*, ingrese el nombre del servidor Dell con el que se comunicará esta computadora por ejemplo, servidor.dominio.com. No es necesario incluir www o http(s). Esta información la proporciona el administrador.

Dell Security Center alojado	Dell Management Server local
	c Haga clic en **Continuar**. d Siga con el paso 9.

9 En la ventana Tipo de instalación, realice una de estas acciones:
- Haga clic en **Instalar** y, luego, vaya al paso 10.
- Haga clic en **Cambiar ubicación de instalación**.
  1 En la ventana Seleccionar el destino, seleccione a todos los usuarios. Actualmente, esta es la única opción.
  2 Haga clic en **Continuar**.
  3 Haga clic en **Instalar** y, luego, vaya al paso 10.

10 En el diálogo, ingrese su nombre de usuario y contraseña y haga clic en **Instalar software**.

11 En la página Resumen, haga clic en **Cerrar**.

12 Cuando se le solicite, conserve el archivo .pkg o muévalo a la *papelera*.

13 Realice una de estas opciones:

Dell Security Center alojado	Dell Management Server local
La ventana Credenciales se abrirá automáticamente después de instalar. Si su empresa cuenta con varios inquilinos, necesitará una ID de instalación. 1 En la ventana Credenciales, ingrese el correo electrónico de su cuenta de inicio de sesión y haga clic en **Continuar**. 2 Realice una de estas opciones: • Si su empresa cuenta con varios grupos de usuarios, ingrese una ID de instalación, haga clic en **Continuar** y continúe con el paso 3. **NOTA:** Si se muestra un error, verifique sus credenciales. Si observa un ID de instalación o una dirección de correo electrónico incorrecta, haga clic en **Reiniciar inicialización** para volver a ingresar sus credenciales. • En el caso de un grupo de usuarios individual, continúe con el paso 3. 3 En la ventana de Microsoft, escriba su contraseña y haga clic en **Iniciar sesión**. 4 En la ventana Azure, escriba su contraseña. 5 Haga clic en **Inicio de sesión**. **NOTA:** Si se muestra un error, verifique sus credenciales. Si observa una dirección de correo electrónico incorrecta, haga clic en **Reiniciar inicialización** para volver a ingresar sus credenciales. 6 Se abre la interfaz de Dell Data Guardian. Consulte Aplicación Dell Data Guardian.	1 Cierre la ventana .dmg para abrir el Buscador. 2 Consulte Activación del usuario final.

NOTA:
Si una empresa actualiza de Cloud Edition a Data Guardian, debe autenticar y volver a vincular Data Guardian con su proveedor de almacenamiento en la nube. Para obtener más información acerca de la autenticación, consulte la ayuda en línea de Data Guardian.

Identifier	GUID-839E9A73-4125-4A28-84A6-4F5CC4D734AC
Status	In Translation

Activación de usuario final (local)

Activación para Dell Management Server local

En la variante local, después de abrir Dell Data Guardian por primera vez, debe iniciar sesión para activarlo:

1 En Finder, seleccione **Aplicaciones** y haga doble clic en **Dell Data Guardian**.

2 Cuando se abra la ventana Credenciales, ingrese la dirección del Dell Server, (por ejemplo, company.server.com). Esta información la proporciona el administrador. De manera predeterminada, el número de puerto es 8443. Si su empresa modifica el puerto predeterminado a un número de puerto personalizado, el administrador se lo informará.

> **NOTA:**
> No seleccione la casilla de verificación Errores de SSL, a menos que lo indique el administrador.

3 Ingrese su dirección de correo electrónico y contraseña.

4 Haga clic en **Iniciar sesión** para activar Data Guardian.

5 Consulte la sección *Aplicación Dell Data Guardian* más adelante.

Para obtener más información sobre la autenticación, consulte la ayuda en línea de Dell Data Guardian.

Aplicación Dell Data Guardian

Cuando se abre la aplicación Dell Data Guardian y se realiza correctamente la activación, el nombre del proveedor de almacenamiento en la nube aparecerá descolorido en el panel de la izquierda.

Si una empresa desea que todos los usuarios colaboren con el mismo proveedor de nube, el administrador puede establecer una política para permitir solo dicho proveedor y bloquear la visualización del resto.

Si se revoca la autenticación para Data Guardian o si esta caduca, también se desactivará el nombre del proveedor de almacenamiento en la nube.

1 En el panel de la izquierda, seleccione el proveedor de almacenamiento en la nube.

2 Se abrirá una ventana en la que se le solicitarán sus credenciales. Ingrese sus credenciales.

Cuando se autentica, se activa el nombre del proveedor de almacenamiento en la nube.

Identifier	GUID-8882A835-A7A8-4C7B-8330-3080F871A121
Status	Translation Validated

Dell Security Center alojado y grupo de usuarios suspendido

Con Dell Security Center alojado, si un grupo de usuarios no realiza pagos durante un período específico, se puede suspender a ese grupo de usuarios. Esto aplica para Windows, Mac, dispositivos móviles y portales web.

Los usuarios internos y externos de Data Guardian pueden experimentar lo siguiente:

- Todas las plataformas: si intenta instalar Data Guardian, activarlo o iniciar sesión, aparece un cuadro de diálogo en el que se indica que un grupo de usuarios está suspendido.
- Mac: si el grupo de usuarios se suspende mientras Data Guardian está abierto, aparece el diálogo de grupo de usuarios suspendido después de que cierra Explorer y todos los archivos e intenta abrir un archivo protegido.
- Portal web:
  - Si ya inició sesión y carga un archivo cifrado, aparece un mensaje que se indica que la carga falló.
  - Si se carga un archivo cifrado o no cifrado y, luego, se suspende el grupo de usuarios, aparece un mensaje en el que se indica que la descarga falló.
  - Si se cierra la sesión e intenta iniciar sesión otra vez, aparece un cuadro de diálogo que indica que el grupo de usuarios se encuentra suspendido.

Póngase en contacto con el administrador.

Identifier	**GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B**
Status	**In Translation**

Proteger los tipos de aplicaciones y archivos adicionales con protección básica de archivos

El administrador informará si las políticas permiten cifrar los tipos de aplicaciones y archivos adicionales. Si alguien abre un archivo cifrado con protección básica de archivos, pero no tiene instalado Data Guardian, el contenido será ilegible.

Descripción general de protección básica de archivos

Aplicaciones

Estos son ejemplos de aplicaciones que posiblemente el administrador necesite cifrar:

- Bloc de notas
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Algunas aplicaciones son solo parcialmente compatibles con Data Guardian y el administrador le informará sobre aquellas.

Tipos de archivos

Estos son ejemplos de tipos de archivos adicionales que se pueden configurar: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac y dispositivos móviles

Cuando está configurada la política de protección básica de archivos, Data Guardian realiza un barrido de las computadoras de los usuarios y cifra todos los archivos locales con dichas extensiones. Los archivos cifrados con protección básica de archivos solo se pueden ver y editar con la aplicación asociada con la extensión de archivo.

> **NOTA:**
> Los archivos en carpetas específicas del sistema no se cifran, por ejemplo, AppData. Además de las carpetas que se relacionan con documentos de Office protegidos, por ejemplo, la carpeta de documentos seguros.

Íconos de superposición para Windows

En el caso de Data Guardian 2.2 y superior, se muestran íconos de superposición en los archivos protegidos en el Explorador de archivos. Si hace clic con el botón secundario en ese archivo protegido, se le proporciona más información en una pestaña de Dell Data Guardian.

Excluir algunos archivos del barrido en Windows o Mac (antes de habilitar el barrido)

Si su empresa decide cifrar un tipo de archivo adicional, como. txt, es posible que no desee ni necesite que todos los archivos con esa extensión se barran y cifren.

Antes de habilitar la protección básica de archivos para esa extensión, el administrador puede configurar otra política que le permite agregar una carpeta a la computadora local, y los archivos de esa carpeta no se barren. El administrador puede establecer una política, crear un nombre de carpeta, proporcionar el nombre de la carpeta y sugerir dónde puede agregar esa carpeta. Estos pueden ser archivos necesarios para el sistema o archivos que no requieren protección.

IMPORTANTE:
Debe crear la carpeta antes de que el administrador habilite la política de protección básica de archivos.

1 Utilice el nombre de la carpeta y la ruta proporcionada por el administrador.
   - En el caso de Mac, vaya a **Panel de preferencias > Exclusiones de protección básica de archivos**. Aquí se muestra el nombre de la carpeta que se va a crear y la ruta.

2 Agregue archivos que no se deben cifrar con la extensión especificada, como .txt. De manera opcional, puede agregar subcarpetas con nombres creados por el usuario.

   NOTA:
   Si tiene archivos con esa extensión que se cifraron anteriormente, colocarlos en esa carpeta no los descifrará. Permanecen cifrados. Si tiene una carpeta de **Documentos no protegidos**, que el administrador puede crear a través de otra política, puede colocar tipos de protección básica de archivos en esta carpeta para descifrarlos.

3 Después de habilitar la protección básica de archivos, si tiene archivos no protegidos con esa extensión en una red o una unidad externa, puede copiarlos en la carpeta excluida. Permanecen sin cifrar. De lo contrario, se cifran.

Si la computadora tiene más de un usuario, solo el usuario que tenga la sesión iniciada actualmente puede colocar archivos en esa carpeta y excluirlos del barrido. Se barrerá o cifrará cualquier archivo que otro usuario coloque en la carpeta.

Eliminación de una extensión de archivo en Windows o Mac

El administrador puede optar por quitar una extensión de archivo. Si es así, se realiza un barrido en su computadora para descifrar esos tipos de archivo.

- La pestaña *Propiedades > Dell Data Guardian* del archivo cifrado deja de aparecer.
- Si tenía íconos superpuestos de archivo, estos dejarán de aparecer.
- El descifrado de archivos puede tardar varios minutos en completarse. Si un archivo con esa extensión sigue cifrado, es posible que se abriera durante el barrido o que esté almacenado en un servidor de archivos o en otra ubicación.

Comuníquese con el administrador para solicitar la recuperación de cualquier archivo con esa extensión que no esté descifrado.

Aplicaciones de Office

Puede utilizar una aplicación de Office para abrir un archivo cifrado con protección básica de archivos, pero el contenido es de solo lectura.

Portal web

En Configuración > Políticas, si la Protección básica de archivos está configurada en "True", el administrador agregó tipos de archivos que no son de Office, los cuales Data Guardian cifrará cuando se descarguen del portal web. El administrador debe indicarle los tipos de archivo.

NOTA:

Si carga un tipo de archivo que aún no es compatible, el contenido será ilegible en el portal web.

Puede cargar tipos de archivos que no sean de Office, sin importar si están cifrados o sin cifrar. Sin embargo, cuando descarga un archivo que no sea de Office, la extensión de archivo varía.

Archivos que no son de Office (como .txt o .png)	Descripción de la descarga
Cifrados antes de cargarlos Por ejemplo: archivos que no son de Office ya cifrados por Windows o Mac.	Cuando se descargan desde el portal web, mantienen la extensión de archivo, como .txt o .png.
Archivos no cifrados	Cuando se descargan desde el portal web, la extensión del archivo varía dependiendo de si el administrador agregó la extensión a una política. Sin embargo, están cifrados. Ejemplos de un archivo .txt descargado desde el portal web: • **nombredelarchivo.txt**: el administrador agregó el tipo de archivo .txt a una política. • **nombredelarchivo.txt.xen**: el tipo de archivo .txt no está incluido en la política. Se cifra el archivo, pero se agrega una extensión .xen.

Si está activada la política *Editar* en el portal web, los usuarios pueden editar los archivos que no son de Office.

Identifier	**GUID-FC539BCB-1939-4E0A-8A36-**
Status	**Translation Validated**

Instalar y 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. Para ver archivos cifrados o trabajar con ellos, debe tener instalada la aplicación Data Guardian en su dispositivo móvil.

Identifier	**GUID-116F412E-15BE-4E29-A886-5A308BA693ED**
Status	**Translated**

Requisito previo

Antes de utilizar la aplicación Data Guardian, determine cuál de estas opciones necesita según su entorno:

Dell Security Center alojado	Dell Management Server local
Si su ambiente alojado es para varios inquilinos, necesitará una ID de instalación.	Asegúrese de conocer el nombre del Dell Server, como server.domain.com. Esta información la proporciona el administrador.

Identifier	**GUID-A802F8F9-1B8F-47DD-8525-518A4C004221**
Status	**Translation Validated**

Introducción a Data Guardian Mobile

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

Tarea	Descripción	Consulte esta sección
Instalar Data Guardian - Determinar una opción:	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
Determinar qué políticas se aplican a dispositivos móviles	El administrador le indicará las políticas que se aplican.	Puede tener lo siguiente: • Documentos de Office protegidos • Protección en la nube

Tarea	Descripción	Consulte esta sección
		• Opciones adicionales
Explorar el Administrador de archivos	Consulte opciones de Data Guardian.	Explorar el Administrador de archivos
Si la política de protección de la nube está activada, acceda a su cuenta de proveedor de almacenamiento en la nube	En el dispositivo, vaya a la página principal del Administrador de archivos de la aplicación de Data Guardian y toque su proveedor de almacenamiento en la nube.	Consulte Acceder a su cuenta de proveedor de almacenamiento en la nube.

Según las políticas de Data Guardian, puede tener lo siguiente:

- Los archivos protegidos de Office (.docx, .pptx, .xlsx, .docm, .pptm, .xlsm, .pdf) conservan su extensión.
- Otras aplicaciones y tipos de archivos, por ejemplo, .txt.
- Los archivos que no son de Office en la nube tienen la extensión .xen.

En los dispositivos móviles con Data Guardian, usted puede:

- Crear carpetas y archivos
- Eliminar carpetas y archivos
- Compartir un documento con un usuario externo (si la política está activada para visores externos)

Identifier	**GUID-618A6EAF-794D-4077-A675-AC9ACA624CC3**
Status	**In Translation**

Instalación o desinstalación de Data Guardian en un dispositivo iOS mediante la App Store

Instalación en un dispositivo iOS

Requisito: si el dispositivo admite un escáner de huellas digitales de Touch ID y desea utilizarlo en lugar de un PIN, debe configurar el dispositivo para Touch ID antes de instalar Data Guardian.

1 En el dispositivo, toque **App Store** y busque **Data Guardian Mobile**.
2 Seleccione e instale la app de **Data Guardian**.
3 Toque la casilla de verificación para aceptar el acuerdo de licencia.
4 Seleccione una de estas opciones:

Dell Security Center alojado	Local
Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security. a Toque **Dell Security Center alojado**. b Ingrese su correo electrónico. c Toque **Enviar**.	Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security. a Toque **Local**. b En el campo Servidor de la pantalla de inicio de sesión, escriba el nombre del Dell Server de la empresa, como servidor.dominio.com. c Ingrese su nombre de usuario y contraseña. d Pulse **Iniciar sesión**.

Dell Security Center alojado	Local

> **NOTA:** Si su dirección de correo electrónico se encuentra en más de un grupo de usuarios, escriba su ID de instalación.

d En la ventana Microsoft Azure, ingrese la contraseña.

e Pulse **Iniciar sesión**.

5 Cuando se le solicite, toque el sensor de huellas digitales o cree un PIN.

Entonces se activó su cuenta y aparece la pantalla del Data Guardian Data Guardian.

Desinstalar la app de Data Guardian

1 En el menú de aplicaciones de iOS, pulse y mantenga pulsado el ícono de **Data Guardian**.

2 Toque **x**.

3 Toque **Eliminar**.

Identifier	GUID-7247F5B1-D730-4DE6-97BA-7E88AD40B7E4
Status	In Translation

Instalación o desinstalación de Data Guardian en un dispositivo iOS con Workspace ONE

Si tiene Workspace ONE instalado, puede autenticarlo con Data Guardian con Single Sign On. Estos pasos son los mismos para el Dell Security Center alojado o para el Dell Management Server local.

El administrador enviará la aplicación Data Guardian a su dispositivo.

1 Cuando se le pregunte si desea instalar la aplicación **Data Guardian**, toque **Aceptar**.

2 Inicie la aplicación **Data Guardian**.

3 En el contrato de licencia, toque **Aceptar**.

4 En la opción de selección de Workspace ONE o Data Guardian, toque **Workspace ONE** para tener un inicio de sesión único.

5 Ingrese su contraseña.

6 Cuando se le indique, cree un PIN.

> **NOTA:** Si inicia sesión en Workspace ONE, solo deberá ingresar el PIN de Data Guardian.

Entonces se activó su cuenta y aparece la pantalla del Data Guardian Data Guardian.

Identifier	GUID-D045F8A7-9124-4843-BAF6-E0BB27CE1046
Status	In Translation

Instalación o desinstalación de Data Guardian en un dispositivo Android mediante Google Play

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 Toque la casilla de verificación para aceptar el acuerdo de licencia.

4 Seleccione una de estas opciones:

Dell Security Center alojado	Dell Management Server local
Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security. a Toque **Alojado**. b Ingrese su correo electrónico. c Toque **Enviar**. **NOTA:** Si su dirección de correo electrónico se encuentra en más de un grupo de usuarios, escriba su ID de instalación. d En la ventana Microsoft Azure, ingrese la contraseña. e Pulse **Iniciar sesión**.	Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security. a Toque **Local**. b En el campo Servidor de la pantalla de inicio de sesión, escriba el nombre del Dell Server de la empresa, como servidor.dominio.com. c Ingrese su nombre de usuario y contraseña. d Pulse **Iniciar sesión**.

5 Cuando se le indique, cree un PIN.

Entonces se activó su cuenta y aparece la pantalla del Data Guardian Data Guardian.

Desinstalar la app de Data Guardian

1 En el menú de aplicaciones de Android, pulse **Configuración**.

2 En **Configuración**, toque **Aplicaciones**.

3 Mantenga presionado el ícono de **Data Guardian**.

4 Arrastre el ícono hasta la opción Desinstalar.

5 Pulse **Aceptar**.

Identifier	**GUID-37A6FDB2-CD4D-4EB3-BDE1-EC151BC08814**
Status	**In Translation**

Instalación o desinstalación de Data Guardian en un dispositivo Android con Workspace ONE

Si tiene Workspace ONE instalado, puede autenticarlo con Data Guardian con Single Sign On. Estos pasos son los mismos para el Dell Security Center alojado o para el Dell Management Server local.

1 En el dispositivo, toque **Concentrador**.

2 Toque **Catálogo de aplicaciones**.

3 En la aplicación Dell Data Guardian, toque **Instalar**.

4 En *Confirmar instalación*, toque **Instalar**.

5 En *Google Play Protect*, toque **Permitir**.

6 En el mensaje de la aplicación instalada, toque **Listo**.

7 Toque **Abrir** para iniciar la aplicación Data Guardian.

8 En la opción de autenticación con Workspace ONE o Data Guardian, toque **Workspace ONE** para tener un inicio de sesión único.

9 En el contrato de licencia, toque la casilla de verificación.

10 Toque **Single Sign On**.

11 Cuando se le indique, cree un PIN.

NOTA: Si inicia sesión en Workspace ONE, solo deberá ingresar el PIN de Data Guardian.

Entonces se activó su cuenta y aparece la pantalla del Data Guardian Data Guardian.

Desinstalar la app de Data Guardian

1 En el menú de aplicaciones de Android, pulse **Configuración**.
2 En **Configuración**, toque **Aplicaciones**.
3 Mantenga presionado el ícono de **Data Guardian**.
4 Arrastre el ícono hasta la opción Desinstalar.
5 Pulse **Aceptar**.

Identifier	**GUID-5B8DFEFC-DC7C-42AE-A662-627068964BC8**
Status	**In Translation**

Explore el Administrador de archivos

En el Administrador de archivos de Data Guardian, puede usar el almacenamiento local o la nube. Se abre el Administrador de archivos al abrir Data Guardian.

Pantalla de administrador de archivos

Las carpetas predeterminadas para la pantalla del administrador de archivos incluyen:

- Documentos
- Descargas
- Fotos

Pantalla Crear nuevo

Toque el icono Agregar (**+**) y aparece la pantalla *Crear nuevo* con estas opciones:

- Documento
- Hoja de cálculo
- Presentación (PowerPoint)
- Foto
- Carpeta
- Servicio de nube

Opciones del menú de navegación

Toque el icono del menú de navegación. Las opciones incluyen:

- **Navegador**
- **Administrador de archivos**
- Icono **Configuración**:
  - Botón **Cambiar PIN** (si la función está activada por política)
  - **Navegador**
  - **Administrador de archivos (Configuración):** utilice estas opciones

    - **Intervalo de actualización:** con qué frecuencia Data Guardian sincroniza los servicios en la nube. Dell recomienda *Manual* o *Diariamente*. Otras opciones son *Cada hora* o *Semanalmente*.
    - **Advertencia de descarga de 10 MB:** habilitar o deshabilitar. Utilice esta opción si no se encuentra conectado a Wi-Fi y el tamaño de la descarga supera los 10 MB.
    - **Borrar caché:** borra archivos temporales.
  - (iOS): **Touch ID** o **Face ID**, según la versión de iOS y si tiene preconfigurados los reconocimientos de huella digital o reconocimiento facial. Toque para habilitar o deshabilitar cuando utiliza Data Guardian.
  - **Acerca de:** consulte Las políticas y la versión de Data Guardian
  - Botón **Salir de Data Guardian**
  - **Cuentas de servicios en la nube:** indica si están vinculadas o desvinculadas.
- **Navegador**
- **Administrador de archivos:** para volver a la pantalla Administrador de archivos.
- **Bloquear Data Guardian**

Opciones adicionales

- Agregar un archivo a Favoritos
  - Para iOS, consulte el menú de navegación.
  - Para Android, mantenga pulsado el nombre de archivo.

Identifier	**GUID-8826272C-679E-40FF-B0A9-D1C9888AF6E5**
Status	**Translation Validated**

Determinar políticas para Data Guardian Mobile

El administrador le indicará cuál de estas políticas se establecieron para su empresa.

Identifier	**GUID-4C1E2DAD-C0CA-4E6F-96D4-0297C01CE8B2**
Status	**Translation Validated**

Ver las políticas y la versión de Data Guardian

Algunas políticas de Data Guardian se indican en **Acerca de**. Para ver estas políticas o la versión de Data Guardian:

1 En el menú de navegación de Data Guardian, toque **Configuración > Acerca de**.

2 Toque **Política**.

Teniendo en cuenta las políticas establecidas por su administrador, la lista incluye:

- Longitud del PIN
- Fin del tiempo de espera por inactividad
- Error de inicio de sesión
- Copiar y pegar: permite copiar desde un documento protegido a un documento protegido.

Versión

3 Determinar las opciones adicionales de las políticas.

Estas pueden incluir:

- Documentos de Office protegidos
- Protección en la nube
- Políticas adicionales

Identifier	**GUID-3613C9F0-10DE-4A67-9158-1964C8D2D77E**
Status	**Translation Validated**

Utilizar documentos protegidos de Office con dispositivos móviles

El administrador le indicará las opciones que están activadas para la empresa. Cuando haya instalado Data Guardian y haya abierto un documento de Office protegido, se muestra un mensaje que indica que el documento se está descifrando.

Opciones de Data Guardian para documentos de Office

Aparecen estas opciones de Data Guardian.

- **Crear:** según la configuración de la política, el documento está protegido al momento de crearlo. En el encabezado de este archivo aparece *Documento protegido*.
- **Copiar/pegar:** con un documento de Office protegido, solo puede copiar a otro documento de Office protegido.
- **Imprimir:** según la configuración adicional de la política, es posible que tenga una marca de agua cuando imprima.
- **Exportar:** según la configuración adicional de la política, es posible que tenga una marca de agua cuando exporte.

Cuando un documento de Office esté abierto, toque el icono que aparece en la parte superior izquierda para estas opciones:

- **Guardar**
- **Guardar como**
- **Exportar**
- **Salir**

Opciones adicionales de Office según la política:

- **Editar:** puede editar archivos de Office .docx y .ppt.

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

- **Marca de agua oculta:** según la política, es posible que los documentos de Office protegidos tengan una marca de agua oculta que identifica al usuario. Si imprime o comparte el documento, la marca de agua persiste.
- **Marca de agua en pantalla:** cuando un documento de Office protegido esté abierto, aparece una marca de agua en la pantalla del cliente.

Información adicional para documentos de Office

Documentos de Office protegidos sin conexión

Cuando crea un documento de Office protegidoo 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.

Solución de problemas para documentos de Office protegidos

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.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Proteger los tipos de aplicaciones y archivos adicionales con protección básica de archivos

El administrador informará si las políticas permiten cifrar los tipos de aplicaciones y archivos adicionales. Si alguien abre un archivo cifrado con protección básica de archivos, pero no tiene instalado Data Guardian, el contenido será ilegible.

Descripción general de protección básica de archivos

Aplicaciones

Estos son ejemplos de aplicaciones que posiblemente el administrador necesite cifrar:

- Bloc de notas
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Algunas aplicaciones son solo parcialmente compatibles con Data Guardian y el administrador le informará sobre aquellas.

Tipos de archivos

Estos son ejemplos de tipos de archivos adicionales que se pueden configurar: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac y dispositivos móviles

Cuando está configurada la política de protección básica de archivos, Data Guardian realiza un barrido de las computadoras de los usuarios y cifra todos los archivos locales con dichas extensiones. Los archivos cifrados con protección básica de archivos solo se pueden ver y editar con la aplicación asociada con la extensión de archivo.

> **NOTA:**
> Los archivos en carpetas específicas del sistema no se cifran, por ejemplo, AppData. Además de las carpetas que se relacionan con documentos de Office protegidos, por ejemplo, la carpeta de documentos seguros.

Íconos de superposición para Windows

En el caso de Data Guardian 2.2 y superior, se muestran íconos de superposición en los archivos protegidos en el Explorador de archivos. Si hace clic con el botón secundario en ese archivo protegido, se le proporciona más información en una pestaña de Dell Data Guardian.

Excluir algunos archivos del barrido en Windows o Mac (antes de habilitar el barrido)

Si su empresa decide cifrar un tipo de archivo adicional, como. txt, es posible que no desee ni necesite que todos los archivos con esa extensión se barran y cifren.

Antes de habilitar la protección básica de archivos para esa extensión, el administrador puede configurar otra política que le permite agregar una carpeta a la computadora local, y los archivos de esa carpeta no se barren. El administrador puede establecer una política, crear un nombre de carpeta, proporcionar el nombre de la carpeta y sugerir dónde puede agregar esa carpeta. Estos pueden ser archivos necesarios para el sistema o archivos que no requieren protección.

IMPORTANTE:

Debe crear la carpeta antes de que el administrador habilite la política de protección básica de archivos.

1 Utilice el nombre de la carpeta y la ruta proporcionada por el administrador.
   - En el caso de Mac, vaya a **Panel de preferencias > Exclusiones de protección básica de archivos**. Aquí se muestra el nombre de la carpeta que se va a crear y la ruta.

2 Agregue archivos que no se deben cifrar con la extensión especificada, como .txt. De manera opcional, puede agregar subcarpetas con nombres creados por el usuario.

   NOTA:

   Si tiene archivos con esa extensión que se cifraron anteriormente, colocarlos en esa carpeta no los descifrará. Permanecen cifrados. Si tiene una carpeta de **Documentos no protegidos**, que el administrador puede crear a través de otra política, puede colocar tipos de protección básica de archivos en esta carpeta para descifrarlos.

3 Después de habilitar la protección básica de archivos, si tiene archivos no protegidos con esa extensión en una red o una unidad externa, puede copiarlos en la carpeta excluida. Permanecen sin cifrar. De lo contrario, se cifran.

Si la computadora tiene más de un usuario, solo el usuario que tenga la sesión iniciada actualmente puede colocar archivos en esa carpeta y excluirlos del barrido. Se barrerá o cifrará cualquier archivo que otro usuario coloque en la carpeta.

Eliminación de una extensión de archivo en Windows o Mac

El administrador puede optar por quitar una extensión de archivo. Si es así, se realiza un barrido en su computadora para descifrar esos tipos de archivo.

- La pestaña *Propiedades > Dell Data Guardian* del archivo cifrado deja de aparecer.
- Si tenía íconos superpuestos de archivo, estos dejarán de aparecer.
- El descifrado de archivos puede tardar varios minutos en completarse. Si un archivo con esa extensión sigue cifrado, es posible que se abriera durante el barrido o que esté almacenado en un servidor de archivos o en otra ubicación.

Comuníquese con el administrador para solicitar la recuperación de cualquier archivo con esa extensión que no esté descifrado.

Aplicaciones de Office

Puede utilizar una aplicación de Office para abrir un archivo cifrado con protección básica de archivos, pero el contenido es de solo lectura.

Portal web

En Configuración > Políticas, si la Protección básica de archivos está configurada en "True", el administrador agregó tipos de archivos que no son de Office, los cuales Data Guardian cifrará cuando se descarguen del portal web. El administrador debe indicarle los tipos de archivo.

NOTA:

Si carga un tipo de archivo que aún no es compatible, el contenido será ilegible en el portal web.

Puede cargar tipos de archivos que no sean de Office, sin importar si están cifrados o sin cifrar. Sin embargo, cuando descarga un archivo que no sea de Office, la extensión de archivo varía.

Archivos que no son de Office (como .txt o .png)	Descripción de la descarga
Cifrados antes de cargarlos Por ejemplo: archivos que no son de Office ya cifrados por Windows o Mac.	Cuando se descargan desde el portal web, mantienen la extensión de archivo, como .txt o .png.
Archivos no cifrados	Cuando se descargan desde el portal web, la extensión del archivo varía dependiendo de si el administrador agregó la extensión a una política. Sin embargo, están cifrados. Ejemplos de un archivo .txt descargado desde el portal web: • **nombredelarchivo.txt**: el administrador agregó el tipo de archivo .txt a una política. • **nombredelarchivo.txt.xen**: el tipo de archivo .txt no está incluido en la política. Se cifra el archivo, pero se agrega una extensión .xen.

Si está activada la política *Editar* en el portal web, los usuarios pueden editar los archivos que no son de Office.

Identifier	**GUID-36644E42-9324-479F-8128-F89D438E8F17**
Status	**Translation Validated**

Utilizar protección en la nube con dispositivos móviles

Si el administrador activa la nube protección, necesitará dos aplicaciones:

- Aplicación cliente de sincronización en la nube: consulte la ayuda para ese cliente de sincronización en la nube.
- La aplicación Data Guardian Mobile indica el cliente de sincronización en la nube utilizado con su empresa y permite descargarlo.

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 se abre un documento de Office protegido, solo aparecerá una portada que indicará que no se puede ver el documento sin Data Guardian. Esto ofrece más seguridad a sus datos.

Acceder a su cuenta de proveedor de almacenamiento en la nube

Para acceder a su cuenta de proveedor de almacenamiento en la nube:

1 En la pantalla del Administrador de archivos, toque el icono Agregar (**+**).

2 Presione **Servicio en la nube**.
La política de Data Guardian determina qué proveedores de almacenamiento en la nube se mostrarán. Su administrador puede designar uno o varios proveedores específicos de almacenamiento en la nube para utilizarlos en la empresa y bloquear otros.

3 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.

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

Utilizar protección en la nube

En los dispositivos móviles con Data Guardian, usted 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.

- 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.

- **Archivo > Copiar:** según la política establecida por el administrador, puede copiar un archivo de un proveedor de nube a otro.
- Para Android con OneDrive o Dropbox, si no puede compartir un archivo desde las aplicaciones y el archivo comparte un vínculo con la aplicación Data Guardian, comparta el archivo desde la aplicación del navegador de archivos del dispositivo.

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> Administrador de archivos > Servicio en la nube**. Cuando otorgue acceso a un proveedor de almacenamiento en la nube, se mostrará una marca de selección en la casilla de verificación.

2 Realice una de estas opciones:

Android

a Toque **Vinculado**.

b Toque **Sí**.

iOS

a Toque **Desvinculado**.

Esto elimina el acceso a los archivos y los archivos de Data Guardian. Sin embargo, esto no elimina los archivos desde la nube.

Solución de problemas de la protección en la nube

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.

Identifier	**GUID-19337C15-12E9-4E8D-B908-29416128B500**
Status	**Translation Validated**

Utilizar las políticas adicionales con dispositivos móviles

El administrador le indicará cuál de estas políticas se estableció para su empresa.

Uso de PIN

El administrador puede establecer una política que exija un PIN y la configuración de su longitud.

Manipulación

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

Protección adicional mediante el perimetraje

En función de las políticas establecidas por el administrador, los dispositivos móviles pueden 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.

Identifier	**GUID-21086952-1999-4F9B-A47C-C57073C7C715**
Status	**Translation Validated**

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 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.

NOTA:
Google Backup and Sync no es compatible.

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.

Identifier	**GUID-46C6144D-AF30-4559-96AC-39DB1738D2D8**
Status	**Translation Validated**

Registros

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

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center alojado y grupo de usuarios suspendido

Con Dell Security Center alojado, si un grupo de usuarios no realiza pagos durante un período específico, se puede suspender a ese grupo de usuarios. Esto aplica para Windows, Mac, dispositivos móviles y portales web.

Los usuarios internos y externos de Data Guardian pueden experimentar lo siguiente:

- Todas las plataformas: si intenta instalar Data Guardian, activarlo o iniciar sesión, aparece un cuadro de diálogo en el que se indica que un grupo de usuarios está suspendido.
- Mac: si el grupo de usuarios se suspende mientras Data Guardian está abierto, aparece el diálogo de grupo de usuarios suspendido después de que cierra Explorer y todos los archivos e intenta abrir un archivo protegido.
- Portal web:
  - Si ya inició sesión y carga un archivo cifrado, aparece un mensaje que se indica que la carga falló.
  - Si se carga un archivo cifrado o no cifrado y, luego, se suspende el grupo de usuarios, aparece un mensaje en el que se indica que la descarga falló.
  - Si se cierra la sesión e intenta iniciar sesión otra vez, aparece un cuadro de diálogo que indica que el grupo de usuarios se encuentra suspendido.

Póngase en contacto con el administrador.

Identifier	**GUID-66FB1CE0-6669-4DDD-80E8-BCBAA27D4E13**
Status	**Translation Validated**

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 ingresar un comentario.

Identifier	GUID-BDAC1DD8-21C2-4ED1-B0A
Status	In Translation

Ver o editar los archivos protegidos en un cliente Web

Si el administrador configura un portal web Data Guardian, puede establecer un vínculo a una URL para ese cliente web y ver los archivos cifrados sin instalar un cliente Data Guardian. En función de política, también puede editar un archivo.

Según la política establecida por el administrador, es posible que vea lo siguiente:

- Documentos protegidos de Office: .docx, .pptx, .xlsx, .docm, .pptm, .xlsm y .pdf.
- Archivos .xen: archivos de Office o que no son de Office que cifró Data Guardian cuando se cargaron en la nube.
- Tipos de archivos adicionales, como el Bloc de notas.

Según la política establecida por el administrador, puede acceder a un proveedor de almacenamiento en la nube.

Identifier	GUID-C468D78F-0ADF-45FC-B5A2-44B933EB2497
Status	Translation Validated

Acceder al portal web para Data Guardian

Los pasos varían ligeramente según el navegador que utilice.

1 En administrador, obtenga la URL para acceder al portal web.
2 Haga clic en URL.
Si se muestra un aviso de seguridad, haga clic en **Continuar** o **Proseguir**.
3 En la pantalla de acuerdo de licencia, haga clic en **Aceptar**.
Si se muestra un aviso de seguridad, haga clic en **Continuar** o **Proseguir**.
4 Ingrese sus credenciales de dominio.
5 Haga clic en **Inicio de sesión**.
6 Si se le indica que rastree su ubicación, seleccione una opción.
7 Para ver o editar archivos, consulte la ayuda en línea, disponible en el portal web de Data Guardian.

NOTA:
Para Mac, debe configurar Safari para permitir elementos emergentes.

Identifier	GUID-D11E8451-72A7-4179-8693-28D0FAFF9B8B
Status	In Translation

Proteger los tipos de aplicaciones y archivos adicionales con protección básica de archivos

El administrador informará si las políticas permiten cifrar los tipos de aplicaciones y archivos adicionales. Si alguien abre un archivo cifrado con protección básica de archivos, pero no tiene instalado Data Guardian, el contenido será ilegible.

Descripción general de protección básica de archivos

Aplicaciones

Estos son ejemplos de aplicaciones que posiblemente el administrador necesite cifrar:

- Bloc de notas
- Wordpad
- Visio
- MS Paint

> **NOTA:**
> Algunas aplicaciones son solo parcialmente compatibles con Data Guardian y el administrador le informará sobre aquellas.

Tipos de archivos

Estos son ejemplos de tipos de archivos adicionales que se pueden configurar: .txt, .rtf, .csv, .odt, .vsdx, .png, .jpg, .jpeg, .jpe, .jfif, .gif, .tif, .tiff, .bmp

Windows, Mac y dispositivos móviles

Cuando está configurada la política de protección básica de archivos, Data Guardian realiza un barrido de las computadoras de los usuarios y cifra todos los archivos locales con dichas extensiones. Los archivos cifrados con protección básica de archivos solo se pueden ver y editar con la aplicación asociada con la extensión de archivo.

> **NOTA:**
> Los archivos en carpetas específicas del sistema no se cifran, por ejemplo, AppData. Además de las carpetas que se relacionan con documentos de Office protegidos, por ejemplo, la carpeta de documentos seguros.

Íconos de superposición para Windows

En el caso de Data Guardian 2.2 y superior, se muestran íconos de superposición en los archivos protegidos en el Explorador de archivos. Si hace clic con el botón secundario en ese archivo protegido, se le proporciona más información en una pestaña de Dell Data Guardian.

Excluir algunos archivos del barrido en Windows o Mac (antes de habilitar el barrido)

Si su empresa decide cifrar un tipo de archivo adicional, como. txt, es posible que no desee ni necesite que todos los archivos con esa extensión se barran y cifren.

Antes de habilitar la protección básica de archivos para esa extensión, el administrador puede configurar otra política que le permite agregar una carpeta a la computadora local, y los archivos de esa carpeta no se barren. El administrador puede establecer una política, crear un

nombre de carpeta, proporcionar el nombre de la carpeta y sugerir dónde puede agregar esa carpeta. Estos pueden ser archivos necesarios para el sistema o archivos que no requieren protección.

IMPORTANTE:

Debe crear la carpeta antes de que el administrador habilite la política de protección básica de archivos.

1 Utilice el nombre de la carpeta y la ruta proporcionada por el administrador.
   - En el caso de Mac, vaya a **Panel de preferencias > Exclusiones de protección básica de archivos**. Aquí se muestra el nombre de la carpeta que se va a crear y la ruta.

2 Agregue archivos que no se deben cifrar con la extensión especificada, como .txt. De manera opcional, puede agregar subcarpetas con nombres creados por el usuario.

   NOTA:

   Si tiene archivos con esa extensión que se cifraron anteriormente, colocarlos en esa carpeta no los descifrará. Permanecen cifrados. Si tiene una carpeta de **Documentos no protegidos**, que el administrador puede crear a través de otra política, puede colocar tipos de protección básica de archivos en esta carpeta para descifrarlos.

3 Después de habilitar la protección básica de archivos, si tiene archivos no protegidos con esa extensión en una red o una unidad externa, puede copiarlos en la carpeta excluida. Permanecen sin cifrar. De lo contrario, se cifran.

Si la computadora tiene más de un usuario, solo el usuario que tenga la sesión iniciada actualmente puede colocar archivos en esa carpeta y excluirlos del barrido. Se barrerá o cifrará cualquier archivo que otro usuario coloque en la carpeta.

Eliminación de una extensión de archivo en Windows o Mac

El administrador puede optar por quitar una extensión de archivo. Si es así, se realiza un barrido en su computadora para descifrar esos tipos de archivo.

- La pestaña *Propiedades > Dell Data Guardian* del archivo cifrado deja de aparecer.
- Si tenía íconos superpuestos de archivo, estos dejarán de aparecer.
- El descifrado de archivos puede tardar varios minutos en completarse. Si un archivo con esa extensión sigue cifrado, es posible que se abriera durante el barrido o que esté almacenado en un servidor de archivos o en otra ubicación.

Comuníquese con el administrador para solicitar la recuperación de cualquier archivo con esa extensión que no esté descifrado.

Aplicaciones de Office

Puede utilizar una aplicación de Office para abrir un archivo cifrado con protección básica de archivos, pero el contenido es de solo lectura.

Portal web

En Configuración > Políticas, si la Protección básica de archivos está configurada en "True", el administrador agregó tipos de archivos que no son de Office, los cuales Data Guardian cifrará cuando se descarguen del portal web. El administrador debe indicarle los tipos de archivo.

NOTA:

Si carga un tipo de archivo que aún no es compatible, el contenido será ilegible en el portal web.

Puede cargar tipos de archivos que no sean de Office, sin importar si están cifrados o sin cifrar. Sin embargo, cuando descarga un archivo que no sea de Office, la extensión de archivo varía.

Archivos que no son de Office (como .txt o .png)	Descripción de la descarga
Cifrados antes de cargarlos	Cuando se descargan desde el portal web, mantienen la extensión de archivo, como .txt o .png.

Archivos que no son de Office (como .txt o .png)	Descripción de la descarga
Por ejemplo: archivos que no son de Office ya cifrados por Windows o Mac.	
Archivos no cifrados	Cuando se descargan desde el portal web, la extensión del archivo varía dependiendo de si el administrador agregó la extensión a una política. Sin embargo, están cifrados. Ejemplos de un archivo .txt descargado desde el portal web: • **nombredelarchivo.txt**: el administrador agregó el tipo de archivo .txt a una política. • **nombredelarchivo.txt.xen**: el tipo de archivo .txt no está incluido en la política. Se cifra el archivo, pero se agrega una extensión .xen.

Si está activada la política *Editar* en el portal web, los usuarios pueden editar los archivos que no son de Office.

Identifier	**GUID-932E973E-B2CD-4305-B50F-F85231243FA4**
Status	**In Translation**

Usar un proveedor de almacenamiento en la nube

Según la política, el portal web puede acceder a un proveedor de almacenamiento en la nube. Para obtener más información, consulte la ayuda en línea del portal web.

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center alojado y grupo de usuarios suspendido

Con Dell Security Center alojado, si un grupo de usuarios no realiza pagos durante un período específico, se puede suspender a ese grupo de usuarios. Esto aplica para Windows, Mac, dispositivos móviles y portales web.

Los usuarios internos y externos de Data Guardian pueden experimentar lo siguiente:

- Todas las plataformas: si intenta instalar Data Guardian, activarlo o iniciar sesión, aparece un cuadro de diálogo en el que se indica que un grupo de usuarios está suspendido.
- Mac: si el grupo de usuarios se suspende mientras Data Guardian está abierto, aparece el diálogo de grupo de usuarios suspendido después de que cierra Explorer y todos los archivos e intenta abrir un archivo protegido.
- Portal web:
  - Si ya inició sesión y carga un archivo cifrado, aparece un mensaje que se indica que la carga falló.
  - Si se carga un archivo cifrado o no cifrado y, luego, se suspende el grupo de usuarios, aparece un mensaje en el que se indica que la descarga falló.
  - Si se cierra la sesión e intenta iniciar sesión otra vez, aparece un cuadro de diálogo que indica que el grupo de usuarios se encuentra suspendido.

Póngase en contacto con el administrador.

Identifier	GUID-FF3D5442-1632-454D-8787-1
Status	Translation Validated

Utilizar 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.

Los usuarios externos deben cumplir con los requisitos del servidor. Además, el dominio o usuario no debe estar en la lista negra de la empresa.

Para un entorno alojado, solo los usuarios externos se pueden activar con un grupo de usuarios.

Las opciones para los usuarios externos incluyen:

- **Windows:** descargar e instalar un cliente de Data Guardian. Consulte las Tareas del usuario interno en Windows y las Tareas del usuario externo.
- **Mac:** consulte Usuario externo y Mac.
- **Móvil**
- **Portal web:** en lugar de descargar un cliente de Data Guardian, use el portal web de Data Guardian. Los usuarios externos pueden ver un archivo .pdf o .xen de documento de Office protegido Basado en la política, el usuario externo puede editar el archivo. Consulte Usuario externo y portal web.

Identifier	GUID-EBDBAE23-A90F-4603-934B-6B40EE93C248
Status	In Translation

Tareas del usuario interno en Windows

Para compartir archivos protegidos con un usuario externo, puede:

- Uso de la opción *Acceso a archivos protegidos* con documentos de Office protegidos
- Aprobar o denegar el acceso cuando un usuario externo lo solicita
- Enviar un documento de Office protegido a través de un correo electrónico de Outlook.

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 secundario en un archivo protegido y seleccione **Acceso a archivos protegidos**. Puede seleccionar hasta 50 archivos a la vez. Se abre la ventana Compartir acceso a documentos protegidos. Los archivos se pueden encontrar en estas ubicaciones:

- Carpeta local o una unidad de red
- Correo electrónico
- Medios extraíbles
- Recurso compartido de red

2 En el campo *Correo electrónico para compartir* en la parte superior derecha, ingrese 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, para usuarios externos que aún no estén registrados, es informarles que recibirán un correo electrónico con las instrucciones que les permitirán registrarse en Dell Server, descargar y activar Data Guardian y, a continuación, 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.

Enviar un archivo protegido por correo electrónico a través de Outlook

Cuando adjunte un archivo protegido y haga clic en *Enviar*, una petición de confirmación le recuerda que se compartirá la clave de los archivos protegidos.

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

Identifier	**GUID-967BF32F-F6F1-4C5A-BA0B-34CA9F73A438**
Status	**In Translation**

Tareas del usuario externo en Windows

Un usuario interno podría decidir darle acceso a archivos protegidos. Es posible que reciba lo siguiente:

- Un correo electrónico con instrucciones para registrarse
- Archivos protegidos con una portada que contiene un enlace para registrar una dirección válida de correo electrónico

NOTA:
En la portada se indica el nombre para Dell Server local o una ID de instalación para ese grupo de usuarios específico si el Dell Security Center alojado es de varios grupos de usuarios. La portada también incluye vínculos para descargar el cliente Data Guardian.

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

- Registrarse en Data Guardian
- Descargar e instalar Data Guardian: el usuario externo debe tener derechos de administrador en su computadora.

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 Realice una de estas opciones:
   - Correo electrónico: haga clic en **Aceptar**.
   - Documento protegido en el que se muestra una advertencia en la portada: haga clic en el vínculo proporcionado para registrar una dirección de correo electrónico válida.

2 Siga una serie de pasos basados en el entorno de su empresa:

Dell Security Center alojado

Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security.

a Cuando se abra el portal del sitio web de Dell Data Guardian, ingrese su dirección de correo electrónico.

b Desplácese hacia abajo y haga clic en **Aceptar**.

c En la ventana Dell Security Center, desplácese hacia abajo hasta *¿Necesita una cuenta?* y, a continuación, haga clic en **Registrarse**.

d En la página de la cuenta nueva, ingrese un correo electrónico, un nombre determinado, apellido y contraseña. La contraseña debe tener al menos ocho caracteres e incluir una letra minúscula, una letra mayúscula, un carácter especial y un número.

e Haga clic en **Registrarse**.

f Vaya al correo electrónico que utilizó para registrarse, recupere el código de verificación e ingréselo.

NOTA:
Si no ve un mensaje de correo electrónico, revise el spam.

g Haga clic en **Confirmar cuenta**. Cuando se verifica su identidad, se abre el portal web.

h Arrastre el archivo protegido al portal web y haga clic en **Cargar ahora**.

i Recibirá un correo electrónico de bienvenida tras el registro. Este mensaje de correo electrónico contiene un vínculo para descargar un cliente Windows.

NOTA:
Si el Dell Security Center alojado es de varios grupos de usuarios, el correo electrónico también muestra una ID de instalación que necesitará.

Dell Management Server local

Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security.

NOTA:
Si es local, puede instalar Data Guardian antes de registrarse. Cuando lo active, haga clic en el vínculo **Registrar**.

a Cuando se abra la ventana de Dell Data Guardian, ingrese su dirección de correo electrónico.

b Haga clic en **Registrar**.

c En la página de registro, ingrese y confirme la contraseña y, a continuación, haga clic en **Iniciar sesión**.

Aparecerá un diálogo de confirmación de registro y se enviará un correo electrónico a la dirección que haya ingresado el usuario interno. Si no ve el mensaje de correo electrónico, revise los mensajes no deseados.

d En el correo electrónico de verificación de la cuenta de Dell Server, haga clic en el hipervínculo.

NOTA:
Si no ve un mensaje de correo electrónico, revise el spam.

e Avance por la página web.

f En la página de confirmación, haga clic en **Continuar para iniciar sesión**.

g En la página de inicio de sesión, haga clic en **¿Ha olvidado la contraseña?**

NOTA:
Dell Server tiene asignada una contraseña aleatoria que debe restablecer.

Dell Security Center alojado	Dell Management Server local
	h En la página Restablecer contraseña, ingrese 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 ingresado el usuario interno. i Abra el correo electrónico de activación de la cuenta y haga clic en el vínculo. El correo electrónico también muestra el nombre de Dell Server que debe utilizar cuando instale Data Guardian. j En la página Inicio de sesión, escriba la dirección de correo electrónico y la contraseña que ha utilizado para registrarse. k Haga clic en **Inicio de sesión**. Se abre una página de descarga de Data Guardian.

Descargar e instalar Data Guardian para Windows

Después de registrarse, puede hacer clic en un vínculo para descargar un cliente Windows. Según lo que el usuario interno haya proporcionado al principio, es posible que los vínculos estén disponibles aquí:

- Se abre una página de descarga para Servidor de administración de seguridad con opciones para el cliente Windows.
- En Servidor virtual de administración de seguridad, hacer clic en Windows le lleva al sitio dell.com/support.
- Si recibió un archivo protegido, la portada contiene vínculos para descargar un cliente.
- Es posible que reciba un correo electrónico de bienvenida con vínculos para descargar un cliente.

Estos pasos describen cómo instalar Data Guardian en Windows.

1 En Windows, haga clic en **Descargar (32 bits)** o **Descargar (64 bits)**, según el sistema operativo de su equipo.
2 Descargue el archivo de configuración en un directorio de su equipo.
3 Haga doble clic en el archivo de configuración para iniciar el instalador.
4 Seleccione un idioma y haga clic en **Aceptar**.
5 Si se le solicita que instale el paquete redistribuible Microsoft Visual C++ 2010, haga clic en **Aceptar**.
6 En la ventana de Bienvenida, haga clic en **Siguiente**.
7 Lea el contrato de licencia, acepte los términos y haga clic en **Siguiente**.
8 En la pantalla Carpeta de destino, haga clic en **Siguiente** para instalar en la ubicación predeterminada de **C:\Program Files\Dell\Dell Data Guardian\.**
9 En la pantalla Tipo de configuración, seleccione una de las siguientes opciones:

Dell Security Center alojado	Dell Management Server local
a Seleccione Dell Security Center alojado. b Si su empresa es de varios grupos de usuarios, ingrese la ID de instalación que se encuentra en la portada o en el correo electrónico de bienvenida. c Haga clic en **Siguiente**. d Siga con el paso 10.	a Seleccione Dell Management Server local. b En el campo *Nombre del servidor:*, ingrese el nombre del Dell Server 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. c Haga clic en **Siguiente**. d En la pantalla Confirmar servidor de activación, confirme que la dirección URL del Dell Server es correcta. El instalador agrega www o http(s) y el puerto. Haga clic en **Siguiente**. e Siga con el paso 10.

10 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.

11 Haga clic en **Instalar** para comenzar la instalación.
Se mostrará una ventana de estado que muestra el progreso de la instalación.

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

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

La instalación de Data Guardian se ha completado.

14 Consulte Activar Data Guardian.

NOTA:

Asegúrese de ver notas y excepciones en Utilizar Data Guardian con Windows, por ejemplo, no puede abrir un archivo .pdf protegido desde la red. Puede utilizar Word para abrir un archivo .pdf protegido desde la red.

Identifier	**GUID-92B941BF-52D2-4302-AFA1-3D348E260E03**
Status	**In Translation**

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 el área de notificaciones, se muestra el icono de una nube con un signo de exclamación naranja.

2 Cuando se muestra un cuadro de diálogo en el área de notificaciones, 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 el área de notificaciones y seleccione **Activación de usuario**.

NOTA:

Para un entorno alojado, solo los usuarios externos se pueden activar con un grupo de usuarios a la vez. Si ya activó un grupo de usuarios, debe desinstalar Data Guardian y reinstalarlo con otra ID de instalación. Como alternativa, puede utilizar el portal web para cargar y ver los documentos protegidos.

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

NOTA:

Para local, si instaló Data Guardian antes de registrarse, cuando lo active, haga clic en el vínculo **Registrar**.

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

4 Confirme el estado de su modo de usuario. Haga clic en el ícono icono del área de notificaciones 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.

Identifier	**GUID-55AD51F6-9437-4B64-9A9F-E598A3BBDC74**
Status	**Translation Validated**

Solicitar el acceso de un usuario interno

Con Windows, Mac y dispositivos móviles, si un usuario externo instaló y activó Data Guardian, el usuario puede solicitar acceso a un documento de Office protegido o a un .pdf de un usuario interno. El usuario externo debe realizar una solicitud por separado para cada archivo.

1 Si abre un documento 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 el área de notificaciones, el usuario externo puede hacer clic con el botón secundario 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.

Identifier	**GUID-1DB6F793-018B-4F14-AA95-63980FCDD713**
Status	**Translation Validated**

Tareas de usuario externo y Mac

Tareas de usuario interno para Mac

Realice una de estas opciones:

- Documentos protegidos: enviar un archivo protegido al usuario externo mediante correo electrónico, recurso compartido de red o almacenamiento extraíble.
- Si está activado el cifrado de la nube de Data Guardian, en la interfaz de Dell Data Guardian, arrastre archivos protegidos hasta la columna situada junto a la columna del proveedor de almacenamiento en la nube.

Tareas de usuario externo para Mac

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 Cuando abra un documento protegido que muestra una advertencia en la portada, haga clic en el vínculo proporcionado para registrar una dirección válida de correo electrónico.

> **NOTA:**
> En la portada se indica el nombre para Dell Server local o una ID de instalación para ese grupo de usuarios específico si el Dell Security Center alojado es de varios grupos de usuarios. La portada incluye vínculos para descargar el cliente Data Guardian.

2 Realice alguna de estas opciones, según su entorno:

Dell Security Center alojado	Dell Management Server local
Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security.	Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security.
a Cuando se abra el portal del sitio web de Dell Data Guardian, ingrese su dirección de correo electrónico. b Desplácese hacia abajo y haga clic en **Aceptar**. c En la ventana Dell Security Center, desplácese hacia abajo hasta *¿Necesita una cuenta?* y, a continuación, haga clic en **Registrarse**. d En la página de la cuenta nueva, ingrese un correo electrónico, un nombre determinado, apellido y contraseña. La contraseña debe tener al menos ocho caracteres e incluir una letra minúscula, una letra mayúscula, un carácter especial y un número.	a Cuando se abra la ventana de Dell Data Guardian, ingrese su dirección de correo electrónico. b Haga clic en **Registrar**. c En la página de registro, ingrese y confirme la contraseña y, a continuación, haga clic en **Iniciar sesión**. Aparecerá un diálogo de confirmación de registro y se enviará un correo electrónico a la dirección que haya ingresado el usuario interno. Si no ve el mensaje de correo electrónico, revise los mensajes no deseados. d Abra el correo electrónico de verificación de la cuenta y haga clic en el vínculo.

Dell Security Center alojado

e Haga clic en **Registrarse**.

f Vaya al correo electrónico que utilizó para registrarse, recupere el código de verificación e ingréselo.

> **NOTA:** Si no ve un mensaje de correo electrónico, revise el spam.

g Haga clic en **Confirmar cuenta**. Cuando se verifica su identidad, se abre el portal web.

h Cargue el archivo protegido para verlo.

Recibirá un correo electrónico con vínculos para la descarga del cliente Mac. O puede hacer clic en el vínculo en la portada. Consulte lo siguiente.

Dell Management Server local

El correo electrónico también muestra el nombre de Dell Server que debe utilizar cuando instale Data Guardian.

e En la página de Confirmación de registro, haga clic en **Volver a la página de inicio**.

Puede hacer clic en un vínculo en la portada para descargar e instalar un cliente. Consulte lo siguiente.

Descargue e instale un cliente de Data Guardian (opcional)

1 En la página Dell Data Guardian, escriba la dirección de correo electrónico y la contraseña que ha utilizado para registrarse.

2 Haga clic en **Inicio de sesión**.

Se abre una página de descarga de Data Guardian con diferentes opciones para Windows, iOS, Android y Mac OS X.

3 En Mac OS X, haga clic en **Descargar**.

4 En la página *Controladores y descargas*, seleccione **Apple Mac OS** y haga clic en **Descargar**.

5 Descargue el archivo .dmg en un directorio de su computadora y ejecute el archivo .pkg.

6 Para iniciar sesión/activar, realice una de estas opciones:

Dell Security Center alojado

a Utilice la dirección de correo electrónico que utilizó cuando se registró.

b La información de inicio de sesión es lo que se utiliza para iniciar sesión en .dmg.

c Haga clic en **Inicio de sesión**.

Dell Management Server local

a Consulte la Ayuda en línea integrada de Data Guardian e ingrese el nombre de Dell Server que aparece en el correo electrónico de verificación de la cuenta.

b También ingrese su dirección de correo electrónico y la contraseña. La información de inicio de sesión es la que utilizó para registrarse.

c Haga clic en **Inicio de sesión**.

Identifier	**GUID-B2D2A78A-86B7-4D46-A530-C531CE3B706A**
Status	**Translation Validated**

Usuario externo y dispositivo móvil

Si un usuario interno comparte un vínculo a través de la nube a un archivo protegido, en el archivo se muestra una portada que contiene un vínculo para registrar una dirección de correo electrónico válida.

> **NOTA:** En la portada se indica el nombre para Dell Server local o una ID de instalación para ese grupo de usuarios específico si el Dell Security Center alojado es de varios grupos de usuarios. La portada también incluye vínculos para descargar el cliente Data Guardian.

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

- Registrarse en Data Guardian
- Descargar e instalar Data Guardian: el usuario externo debe tener derechos de administrador en su computadora.

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 la advertencia de la portada, haga clic en el vínculo proporcionado para registrar una dirección de correo electrónico válida.

2 Siga una serie de pasos basados en el entorno de su empresa:

Dell Security Center alojado

Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security.

a Cuando se abra el portal del sitio web de Dell Data Guardian, ingrese su dirección de correo electrónico.

b Desplácese hacia abajo y haga clic en **Aceptar**.

c En la ventana Dell Security Center, desplácese hacia abajo hasta *¿Necesita una cuenta?* y, a continuación, haga clic en **Registrarse**.

d En la página de la cuenta nueva, ingrese un correo electrónico, un nombre determinado, apellido y contraseña. La contraseña debe tener al menos ocho caracteres e incluir una letra minúscula, una letra mayúscula, un carácter especial y un número.

e Haga clic en **Registrarse**.

f Vaya al correo electrónico que utilizó para registrarse, recupere el código de verificación e ingréselo.

> **NOTA:**
> Si no ve un mensaje de correo electrónico, revise el spam.

g Haga clic en **Confirmar cuenta**. Cuando se verifica su identidad, se abre el portal web.

h Arrastre el archivo protegido al portal web y haga clic en **Cargar ahora**.

i Recibirá un correo electrónico de bienvenida tras el registro. Este mensaje de correo electrónico contiene un vínculo para descargar un cliente Windows.

> **NOTA:**
> Si el Dell Security Center alojado es de varios grupos de usuarios, el correo electrónico también muestra una ID de instalación que necesitará.

Dell Management Server local

Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security.

> **NOTA:**
> Si es local, puede instalar Data Guardian antes de registrarse. Cuando lo active, haga clic en el vínculo **Registrar**.

a Cuando se abra la ventana de Dell Data Guardian, ingrese su dirección de correo electrónico.

b Haga clic en **Registrar**.

c En la página de registro, ingrese y confirme la contraseña y, a continuación, haga clic en **Iniciar sesión**.

Aparecerá un diálogo de confirmación de registro y se enviará un correo electrónico a la dirección que haya ingresado el usuario interno. Si no ve el mensaje de correo electrónico, revise los mensajes no deseados.

d En el correo electrónico de verificación de la cuenta de Dell Server, haga clic en el hipervínculo.

> **NOTA:**
> Si no ve un mensaje de correo electrónico, revise el spam.

e Avance por la página web.

f En la página de confirmación, haga clic en **Continuar para iniciar sesión**.

g En la página de inicio de sesión, haga clic en **¿Ha olvidado la contraseña?**

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

h En la página Restablecer contraseña, ingrese 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 ingresado el usuario interno.

i Abra el correo electrónico de activación de la cuenta y haga clic en el vínculo.

El correo electrónico también muestra el nombre de Dell Server que debe utilizar cuando instale Data Guardian.

j En la página Inicio de sesión, escriba la dirección de correo electrónico y la contraseña que ha utilizado para registrarse.

k Haga clic en **Inicio de sesión**.

Se abre una página de descarga de Data Guardian.

Descargar e instalar Data Guardian para dispositivos móviles

Realice una de estas opciones:

- Instalar o desinstalar Data Guardian en un dispositivo Android
- Instalar o desinstalar Data Guardian en un dispositivo iOS

Identifier	**GUID-FE0A7159-E0F3-4E21-9FE6-008C831F7D44**
Status	**Translation Validated**

Usuario externo y portal web

Tareas del usuario interno

Un usuario interno puede realizar una de las siguientes tareas:

- Enviar al usuario externo la URL de la empresa para acceder al portal web de Data Guardian.
- Enviar un archivo protegido al usuario externo. Cuando el usuario abre el archivo, se muestra una portada.

El usuario externo solo puede ver archivos .pdf o .xen de un documento de Office protegido o editar archivos en función de la política. Sin embargo, el usuario externo no debe descargar un cliente de Data Guardian.

Tareas del usuario externo para el portal web

Para registrarse en el portal web de Data Guardian:

1 Haga clic en la URL del portal web, ya sea que se haya recibido de un usuario interno o en la portada de un archivo protegido.

2 En la pantalla de acuerdo de licencia, desplácese hacia abajo y haga clic en **Aceptar**.

3 Realice una de las siguientes acciones, estas varían si su empresa está alojada o está un entorno Local.

Dell Security Center alojado	**Dell Management Server local**
Una solución de software como servicio (SaaS) alojada para administrar el software de Dell Data Security.	Un servidor local ubicado en la red empresarial para administrar el software de Dell Data Security.
a Ingrese una dirección de correo electrónico y una contraseña. b Haga clic en **Iniciar sesión**. c Ingrese un correo electrónico, el nombre, el apellido y la contraseña. La contraseña debe tener al menos ocho caracteres e incluir una letra minúscula, una letra mayúscula, un carácter especial y un número. d Haga clic en **Registrarse**. e Vaya al correo electrónico que utilizó para registrarse, recupere el código de verificación e ingréselo. f Ingrese el código de verificación y haga clic en **Confirmar cuenta**. Se abre el portal web.	a b Haga clic en **¿Aún no tiene una cuenta?** c Ingrese una dirección de correo electrónico y haga clic en **Registrarse**. **NOTA:** En el caso de usuarios internos que deseen registrarse como externos, es una dirección de correo electrónico sin dominio. d En la página de registro, ingrese y confirme la contraseña, y luego haga clic en **Registrarse**. La página de confirmación indicará que se envió un correo electrónico de confirmación a la dirección de correo electrónico entregada. e Para completar la activación de la cuenta, abra el correo titulado *Verificación de la cuenta* y haga clic en el enlace. f En la pantalla de Confirmación del registro, haga clic en **Volver a la página de inicio**. g Escriba la dirección de correo electrónico y la contraseña que haya utilizado para registrarse.
Si un usuario interno no comparte la clave, puede acceder al portal web, pero no abrir el archivo.	

4 Se abrirá la página de carga de archivos de Dell Data Guardian.

5 Haga clic en **Examinar** para navegar hasta el archivo y cargarlo, o bien arrastre y suelte el archivo en el portal web.

6 Haga clic en **?** para ver la Ayuda en línea para cada página.

Para editar archivos, el administrador debe modificar una política para ese usuario. Si logra acceder luego de registrarse, debe cerrar sesión en el portal web y volver a iniciar sesión.

De manera opcional, puede descargar un cliente Data Guardian. La portada incluye vínculos para descargar el cliente Data Guardian. En la portada también se indica el nombre para Dell Server local o una ID de instalación para ese grupo de usuarios específico si el Dell Security Center alojado es de varios grupos de usuarios.

Solicitar el acceso de un usuario interno

Si carga un documento de Office protegido o un .pdf y aparece un cuadro de diálogo *Error en carga* que indica que no tiene acceso, puede solicitar el acceso al autor del archivo:

1 En el cuadro de diálogo *Error en carga*, haga clic en **Sí**.
2 Espere el correo electrónico del usuario interno en el que se indica si se le otorgó o denegó el acceso.

NOTA:
Si no recibe un correo electrónico del usuario interno, debe esperar 48 horas antes de solicitar el acceso otra vez. Si abre el archivo protegido antes de que el usuario interno apruebe el acceso, aparece un mensaje que indica que la solicitud está pendiente.

Identifier	**GUID-01B874EC-88D4-4264-803C-472B65D1180F**
Status	**Translation Validated**

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 a Dell Server 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 a Dell Server 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

Identifier	**GUID-8882A835-A7A8-4C7B-8330-3080F871A121**
Status	**Translation Validated**

Dell Security Center alojado y grupo de usuarios suspendido

Con Dell Security Center alojado, si un grupo de usuarios no realiza pagos durante un período específico, se puede suspender a ese grupo de usuarios. Esto aplica para Windows, Mac, dispositivos móviles y portales web.

Los usuarios internos y externos de Data Guardian pueden experimentar lo siguiente:

- Todas las plataformas: si intenta instalar Data Guardian, activarlo o iniciar sesión, aparece un cuadro de diálogo en el que se indica que un grupo de usuarios está suspendido.

- Mac: si el grupo de usuarios se suspende mientras Data Guardian está abierto, aparece el diálogo de grupo de usuarios suspendido después de que cierra Explorer y todos los archivos e intenta abrir un archivo protegido.
- Portal web:
  - Si ya inició sesión y carga un archivo cifrado, aparece un mensaje que se indica que la carga falló.
  - Si se carga un archivo cifrado o no cifrado y, luego, se suspende el grupo de usuarios, aparece un mensaje en el que se indica que la descarga falló.
  - Si se cierra la sesión e intenta iniciar sesión otra vez, aparece un cuadro de diálogo que indica que el grupo de usuarios se encuentra suspendido.

Póngase en contacto con el administrador.

Identifier	GUID-EF1D5890-EB47-482E-AF29-
Status	In Translation

Mejorar la seguridad con los Grupos de acceso de Data Guardian (entorno local)

Los Grupos de acceso de Data Guardian mejoran la seguridad mediante la creación de grupos de usuarios que pueden colaborar con datos cifrados. Los usuarios fuera de un grupo no pueden acceder ni revisar los datos, a menos que el propietario del archivo les otorgue acceso. Los Grupos de acceso pueden incluir usuarios internos y externos. Puede utilizar Grupos de acceso con Windows, Mac, dispositivos móviles y el portal web.

Seleccione una de estas opciones según su empresa:

- La empresa tiene Data Guardian instalado con el modo de participación
- La empresa tiene Data Guardian instalado con el Modo de protección forzada
- La empresa aún no tiene Data Guardian ni el modo de participación
- La empresa aún no tiene Data Guardian ni el Modo de protección forzada

También puede realizar lo siguiente:

- Cambiar el propietario de un archivo cifrado
- Revocar el acceso a una clave

Identifier	GUID-F71ADE66-5107-4796-B57E-FC00340C788C
Status	In Translation

La empresa tiene Data Guardian instalado con el Modo de participación

Si su empresa utiliza grupos de acceso para mejorar la seguridad de los datos confidenciales, debe conocer quién está en su grupo de acceso. Al principio, para asegurar una transición fluida, su empresa puede proporcionar un breve período para procesar los archivos compartidos y cifrados existentes. Después de que finalice el período de transición, los miembros de su grupo de acceso pueden ver cualquier archivo cifrado y compartido que cree. Puede otorgar acceso a las personas fuera de su grupo de acceso.

Identifique a los miembros de su grupo de acceso

El administrador le informará quién se encuentra en uno o más de sus grupos de acceso, según la persona que necesite acceder a archivos específicos. Esto puede incluir usuarios internos y externos. Si trabaja en datos confidenciales con usuarios específicos, puede solicitar que el administrador cree un grupo de acceso para ese contenido.

Utilice un período de transición para procesar archivos cifrados y compartidos

Si ya tiene Data Guardian instalado y se cifran los archivos existentes, la práctica recomendada para su empresa es contar con un breve período de transición para los archivos cifrados que se comparten. Para facilitar una transición sin problemas, tenga en cuenta lo siguiente en el caso de los archivos cifrados y compartidos:

- El propietario o el autor del archivo, ya sea interno o externo, continúan teniendo acceso al archivo.
- Los usuarios internos o externos dentro de su grupo de acceso tienen acceso a la mayoría de los archivos compartidos. Según el tipo de clave asociada con algunos archivos, puede perder el acceso a algunos.
- Usuarios internos fuera de su grupo de acceso: los usuarios deben abrir los archivos compartidos durante el período de transición para obtener acceso a la clave. Si no abren un archivo cifrado compartido durante este breve período, perderán su acceso al archivo.
- Usuarios externos que no están en su grupo de acceso: si ya otorgó acceso a un archivo cifrado, el usuario externo seguirá teniendo acceso después del período de transición.

Si pierde el acceso a un archivo después del período de transición, puede solicitar el acceso al propietario.

Recuperar el acceso a los archivos cifrados compartidos después del período de transición

Para Windows y Mac en el modo de suscripción, puede realizar lo siguiente para recuperar el acceso:

- Documentos de Office protegidos: un cuadro de diálogo les informa a los usuarios internos y externos que deben solicitar el acceso; el propietario del archivo puede decidir si desea concederlo.
- Tipos de archivo adicionales cifrados mediante protección básica de archivos: no existe ningún indicador después de compartirlos. El usuario debe saber quién es el propietario del archivo y hacer clic con el botón secundario en el archivo cifrado para encontrar el ID de la clave en la pestaña Data Guardian. El usuario puede enviar esa información al propietario y solicitar el acceso.

Colaborar en nuevos archivos cifrados después del período de transición

Para los nuevos archivos que cree y cifre después del período de transición:

- Usuarios internos o externos dentro de su grupo de acceso: cuentan con acceso a todos los archivos cifrados compartidos.
  - Cualquier persona eliminada del grupo de acceso pierde su derecho de acceso.
  - Si se elimina del grupo al propietario de un archivo, los otros usuarios todavía tienen acceso.
- Usuarios internos o externos fuera de su grupo de acceso: no pueden ver un archivo cifrado.
  - Un usuario interno dentro del grupo de acceso puede otorgar acceso.
  - Si un usuario externo es el propietario de un archivo cifrado, este usuario puede otorgar acceso a otra persona.
  - Si un usuario interno o externo fuera del grupo recibe un documento de Office protegido e intenta abrirlo, aparece un cuadro de diálogo en el cual se les informa que deben solicitar acceso.
  - Si un usuario interno o externo fuera del grupo recibe e intenta abrir un tipo de archivo de protección básica de archivos, el usuario puede hacer clic con el botón secundario en el archivo cifrado para encontrar el ID de clave en la pestaña Data Guardian y enviar esa información al propietario.

Identifier	GUID-18DE070B-862D-4CAF-8CDE-DA86552E6C57
Status	In Translation

La empresa tiene Data Guardian instalado con el modo de protección forzada

Si su empresa utiliza grupos de acceso para mejorar la seguridad de los datos confidenciales, debe conocer quién está en su grupo de acceso. Al principio, para asegurar una transición fluida, su empresa puede proporcionar un breve período para procesar los archivos compartidos y cifrados existentes. Después de que finalice el período de transición, los miembros de su grupo de acceso pueden ver cualquier archivo cifrado y compartido que cree. Puede otorgar acceso a las personas fuera de su grupo de acceso.

Identifique a los miembros de su grupo de acceso

El administrador le informará quién se encuentra en uno o más de sus grupos de acceso, según la persona que necesite acceder a archivos específicos. Esto puede incluir usuarios internos y externos. Si trabaja en datos confidenciales con usuarios específicos, puede solicitar que el administrador cree un grupo de acceso para ese contenido.

Utilice un período de transición para procesar archivos cifrados y compartidos

Si ya tiene Data Guardian instalado y se cifran los archivos existentes, la práctica recomendada para su empresa es contar con un breve período de transición para los archivos cifrados que se comparten. Para facilitar una transición sin problemas, tenga en cuenta lo siguiente en el caso de los archivos cifrados y compartidos:

- El propietario o el autor del archivo, ya sea interno o externo, continúan teniendo acceso al archivo.
- Los usuarios internos o externos dentro de su grupo de acceso tienen acceso a la mayoría de los archivos compartidos. Según el tipo de clave asociada con algunos archivos, puede perder el acceso a algunos.
- Usuarios internos fuera de su grupo de acceso: los usuarios deben abrir los archivos compartidos durante el período de transición para obtener acceso a la clave. Si no abren un archivo cifrado compartido durante este breve período, perderán su acceso al archivo.
- Usuarios externos que no están en su grupo de acceso: si ya otorgó acceso a un archivo cifrado, el usuario externo seguirá teniendo acceso después del período de transición.

Si pierde el acceso a un archivo después del período de transición, puede solicitar el acceso al propietario.

Recuperar el acceso a los archivos cifrados compartidos después del período de transición

En el caso de Windows y Mac en el modo de protección forzada, puede realizar lo siguiente para recuperar el acceso:

- Documentos de Office protegidos: un cuadro de diálogo les informa a los usuarios internos y externos que deben solicitar el acceso; el propietario del archivo puede decidir si desea concederlo.
- Tipos de archivo adicionales cifrados mediante protección básica de archivos: no existe ningún indicador después de compartirlos. El usuario debe saber quién es el propietario del archivo y hacer clic con el botón secundario en el archivo cifrado para encontrar el ID de la clave en la pestaña Data Guardian. El usuario puede enviar esa información al propietario y solicitar el acceso.

Colabore en archivos recién creados después del período de transición

Para los nuevos archivos que cree y cifre después del período de transición:

- Usuarios internos o externos dentro de su grupo de acceso: cuentan con acceso a todos los archivos cifrados compartidos.
  - Cualquier persona eliminada del grupo de acceso pierde su derecho de acceso.
  - Si se elimina del grupo al propietario de un archivo, los otros usuarios todavía tienen acceso.
- Usuarios internos o externos fuera de su grupo de acceso: no pueden ver un archivo cifrado.
  - Un usuario interno dentro del grupo de acceso puede otorgar acceso.
  - Si un usuario externo es el propietario de un archivo cifrado, este usuario puede otorgar acceso a otra persona.
  - Si un usuario interno o externo fuera del grupo recibe un archivo cifrado e intenta abrirlo, aparece un cuadro de diálogo en el cual se les informa que deben solicitar acceso.

Identifier	**GUID-BDD3EF46-A9A1-48C2-BB76-B9D874BC37E4**
Status	**In Translation**

La empresa aún no tiene Data Guardian ni el Modo de participación

Si su empresa tiene previsto utilizar Data Guardian con grupos de acceso para mejorar la seguridad de los datos confidenciales, la práctica recomendada es identificar los archivos que usted comparte con usuarios internos o externos y averiguar si esos usuarios estarán en algún grupo de acceso que el administrador crea para usted. Al principio, para asegurar una transición fluida, su empresa puede proporcionar un breve período para procesar los archivos compartidos existentes. Después de que finalice el período de transición, los miembros de su grupo de acceso pueden ver cualquier archivo cifrado compartido que cree. Puede otorgar acceso a las personas fuera de su grupo de acceso, a fin de que pueda colaborar con ellos sin que disminuya la seguridad.

Identifique a los miembros de su grupo de acceso

El administrador le informará quién se encuentra en uno o más de sus grupos de acceso, según la persona que necesite acceder a archivos específicos. Esto puede incluir usuarios internos y externos. Si trabaja en datos confidenciales con usuarios específicos, puede solicitar que el administrador cree un grupo de acceso para ese contenido.

Utilice un período de transición para procesar archivos compartidos

Cuando Data Guardian está instalado, se produce un barrido en Windows o Mac y se cifran los siguientes archivos si el administrador habilitó una política para estos.

- Tipos de archivo adicionales como .txt o .png, configurados para la protección básica de archivos
- Archivos de clasificación de datos (Windows)
- Archivos de clasificación TITUS (Windows)

Si ya colabora en archivos o los comparte con usuarios internos o externos, es posible que estos usuarios estén o no en su grupo de acceso. La práctica recomendada para una transición fluida es contar con un breve período de transición para procesar cualquiera de esos archivos cifrados que se comparten con otros usuarios. Debe iniciar sesión en su computadora durante este período de transición.

Tenga en cuenta lo siguiente si desea seguir compartiendo o colaborando en esos archivos:

- Para los archivos compartidos mencionados anteriormente, la primera persona que inicia sesión y que pasa por un proceso de barrido en su computadora se convierte en el propietario de cualquier archivo compartido.
- Si otra persona se convierte en el propietario del archivo y el autor original no está en su grupo de acceso, el propietario original debe solicitar acceso al nuevo propietario. El propietario original también puede solicitar que el administrador cambie la propiedad.
- A las computadoras de usuarios externos no se les realiza barrido; por lo tanto, las copias de archivos compartidos sin protección no pasan por un barrido ni se cifran.
- Si el cifrado de nube de Data Guardian está habilitado y si los usuarios comparten carpetas o archivos en un proveedor de almacenamiento en la nube, estos archivos también pasarán por un barrido.

Colabore en archivos recién creados después del período de transición

Para los nuevos archivos que cree y cifre después del período de transición:

- Usuarios internos o externos dentro de su grupo de acceso: cuentan con acceso a todos los archivos cifrados compartidos.
  - Cualquier persona eliminada del grupo de acceso pierde su derecho de acceso.
  - Si se elimina del grupo al propietario de un archivo, los otros usuarios todavía tienen acceso.
- Usuarios internos o externos fuera de su grupo de acceso: no pueden ver un archivo cifrado.
  - Un usuario interno dentro del grupo de acceso puede otorgar acceso.
  - Si un usuario externo es el propietario de un archivo cifrado, este usuario puede otorgar acceso a otra persona.
  - Si un usuario interno o externo fuera del grupo recibe un archivo cifrado e intenta abrirlo, aparece un cuadro de diálogo en el cual se les informa que deben solicitar acceso.

Identifier	**GUID-16B7D77E-57D2-47D9-B2CC-39DB65B223E2**
Status	**In Translation**

La empresa aún no tiene Data Guardian ni el Modo de protección forzada

Si su empresa tiene previsto utilizar Data Guardian con grupos de acceso para mejorar la seguridad de los datos confidenciales, la práctica recomendada es identificar los archivos que usted comparte con usuarios internos o externos y averiguar si esos usuarios estarán en algún grupo de acceso que el administrador crea para usted. Al principio, para asegurar una transición fluida, su empresa puede proporcionar un breve período para procesar los archivos compartidos existentes. Después de que finalice el período de transición, los miembros de su grupo de acceso pueden ver cualquier archivo cifrado compartido que cree. Puede otorgar acceso a las personas fuera de su grupo de acceso, a fin de que pueda colaborar con ellos sin que disminuya la seguridad.

Identifique a los miembros de su grupo de acceso

El administrador le informará quién se encuentra en uno o más de sus grupos de acceso, según la persona que necesite acceder a archivos específicos. Esto puede incluir usuarios internos y externos. Si trabaja en datos confidenciales con usuarios específicos, puede solicitar que el administrador cree un grupo de acceso para ese contenido.

Utilice un período de transición para procesar archivos compartidos

Cuando Data Guardian está instalado, se produce un barrido en Windows o Mac y se cifran los siguientes archivos si el administrador habilitó una política para estos.

- Documentos de Office

- Archivos PDF
- Tipos de archivo adicionales como .txt o .png, configurados para la protección básica de archivos

La práctica recomendada para una transición fluida es contar con un breve período de transición para procesar cualquiera de esos archivos cifrados que se comparten con otros usuarios. Debe iniciar sesión en su computadora durante este período de transición.

Tenga en cuenta lo siguiente si desea seguir compartiendo o colaborando en esos archivos:

- Para los archivos compartidos mencionados anteriormente, la primera persona que inicia sesión y que pasa por un proceso de barrido en su computadora se convierte en el propietario de cualquier archivo compartido.
- Si otra persona se convierte en el propietario del archivo y el autor original no está en su grupo de acceso, el propietario original debe solicitar acceso al nuevo propietario. El propietario original también puede solicitar que el administrador cambie la propiedad.
- A las computadoras de usuarios externos no se les realiza barrido; por lo tanto, las copias de archivos compartidos sin protección no pasan por un barrido ni se cifran.
- Si el cifrado de nube de Data Guardian está habilitado y si los usuarios comparten carpetas o archivos en un proveedor de almacenamiento en la nube, estos archivos también pasarán por un barrido.

Colabore en archivos recién creados después del período de transición

Para los nuevos archivos que cree y cifre después del período de transición:

- Usuarios internos o externos dentro de su grupo de acceso: cuentan con acceso a todos los archivos cifrados compartidos.
  - Cualquier persona eliminada del grupo de acceso pierde su derecho de acceso.
  - Si se elimina del grupo al propietario de un archivo, los otros usuarios todavía tienen acceso.
- Usuarios internos o externos fuera de su grupo de acceso: no pueden ver un archivo cifrado.
  - Un usuario interno dentro del grupo de acceso puede otorgar acceso.
  - Si un usuario externo es el propietario de un archivo cifrado, este usuario puede otorgar acceso a otra persona.
  - Si un usuario interno o externo fuera del grupo recibe un archivo cifrado e intenta abrirlo, aparece un cuadro de diálogo en el cual se les informa que deben solicitar acceso.

Identifier	**GUID-2627974A-3D0D-4075-81BC-86DFD31CF90B**
Status	**Translated**

Cambiar el propietario de un archivo cifrado

Durante el período de transición para grupos de acceso, si se designó a otro usuario como el propietario de un documento cifrado compartido cuyo autor original sea usted, puede solicitar que el administrador lo designe a usted como el propietario.

Identifier	**GUID-0ED28BBC-3A7C-48F3-A1AE-A5039C39C392**
Status	**In Translation**

Revocar el acceso a una clave

Si otorga acceso a un archivo cifrado a un usuario externo, el usuario tiene la clave para abrir ese archivo.

De manera opcional, si ya no desea que el usuario externo tenga acceso al archivo, puede solicitar al administrador que revoque la clave. Esto se aplica solo a usuarios externos.

Identifier	GUID-8B76A529-19A6-4107-983B-707F5AB1D09C
Status	In Translation

Compartir archivos protegidos previamente en Windows

Debe tener Data Guardian instalado y asignado a uno o más grupos de acceso.
Si un usuario interno o externo no está en su grupo de acceso, puede compartir previamente un archivo protegido.

1 Haga clic con el botón secundario en un archivo protegido y seleccione **Acceso a archivos protegidos**.

En la interfaz de usuario de *uso compartido de acceso a archivo protegido*, el nombre del documento se muestra en Archivo seleccionado.

2 En *correo electrónico para compartir*, haga clic en **Agregar** e ingrese una dirección de correo electrónico válida de un usuario externo o interno que no esté en el grupo de acceso.

Puede agregar hasta diez direcciones individuales a la vez.

3 Para modificar una dirección de correo electrónico, haga clic en **Modificar**.

4 Para eliminar una dirección de correo electrónico, seleccione una entrada y haga clic en **Eliminar**.

NOTA:
Se indica el nombre del propietario del archivo y no se puede seleccionar ni eliminar.

5 En Grupos disponibles, se muestran sus grupos de acceso. Seleccione uno o más grupos y utilice las flechas para agregar a los *Grupos compartidos*.

6 Haga clic en **Aceptar**. Se mostrará un mensaje de finalización satisfactoria.

NOTA:
Los usuarios externos no pueden compartir el documento protegido con otro usuario externo.

Si esta es la primera vez que un usuario externo recibe un archivo protegido de Data Guardian, el usuario debe instalar Data Guardian o utilizar el portal web para ver el archivo protegido.

Identifier	GUID-C67795A0-FA20-4E32-9A2B-89654D67DFB2
Status	In Translation

Compartir archivos protegidos previamente en Mac

Debe tener Data Guardian instalado y asignado a uno o más grupos de acceso.
Si un usuario interno o externo no está en su grupo de acceso, puede compartir previamente un archivo protegido.

1 Haga clic con el botón secundario en un archivo protegido y seleccione **Acceso a archivos protegidos**.

En la interfaz de usuario de *uso compartido de acceso a archivo protegido*, el nombre del documento se muestra en Archivo seleccionado.

2 En *correo electrónico para compartir*, haga clic en **Agregar** e ingrese una dirección de correo electrónico válida de un usuario externo o interno que no esté en el grupo de acceso.

Puede agregar hasta diez direcciones individuales a la vez.

3 Para eliminar una dirección de correo electrónico, seleccione una entrada y haga clic en **Eliminar**.

NOTA:
Se indica el nombre del propietario del archivo y no se puede seleccionar ni eliminar.

4 En Grupos disponibles, se muestran sus grupos de acceso. Seleccione uno o más grupos y utilice las flechas para agregar a los *Grupos compartidos*.

5 Haga clic en **Aceptar**. Se mostrará un mensaje de finalización satisfactoria.

> **NOTA:**
> Los usuarios externos no pueden compartir el documento protegido con otro usuario externo.

Si esta es la primera vez que un usuario externo recibe un archivo protegido de Data Guardian, el usuario debe instalar Data Guardian o utilizar el portal web para ver el archivo protegido.

Identifier	GUID-FAF997A4-8E8E-4DCB-BA76-575F951F0799
Status	In Translation

Compartir archivos protegidos previamente en iOS o Android

Si un usuario interno o externo no está en su grupo de acceso, puede compartir previamente un archivo protegido.

1 Toque un archivo protegido.

2

> **NOTA:**
> En la pestaña *Usuarios*, se muestra el nombre del propietario del archivo, pero no se puede seleccionar ni eliminar. Si ya compartió el archivo con usuarios internos o externos, se muestran esos nombres.

3 En la pestaña *Usuarios*, para agregar la dirección de correo electrónico de un usuario externo o un usuario interno que no está en su grupo de acceso, haga clic en el icono del signo más (+) en la parte inferior derecha.

4 Para eliminar una dirección de correo electrónico, deslice y toque **Eliminar**.

5 Toque la pestaña **Grupos** para ver los grupos de acceso.

6 Toque un grupo para compartir un archivo protegido.

> **NOTA:**
> Una marca de verificación indica un grupo con el cual elige compartir el archivo protegido.

7 En la parte superior derecha, toque **Compartir**.

Se mostrará un mensaje de finalización satisfactoria. Los usuarios externos no pueden compartir el documento protegido con otro usuario externo.

Si esta es la primera vez que un usuario externo recibe un archivo protegido de Data Guardian, el usuario debe instalar Data Guardian o utilizar el portal web para ver el archivo protegido.

Identifier	GUID-455BE40E-83D4-4C42-890C-18067EE3CFD5
Status	In Translation

Compartir archivos protegidos previamente en el portal web

Si un usuario interno o externo no está en su grupo de acceso, puede compartir previamente un archivo protegido.

1 En el portal web, cargue un documento protegido.

Si el administrador lo incluyó en uno o más grupos de acceso, se muestra un icono de *acceso a archivo protegido* al lado del icono de descarga.

2 Haga clic en el icono de **acceso a archivo protegido**.

En la interfaz de usuario de *uso compartido de acceso a archivo protegido*, el nombre del documento se muestra en Archivo seleccionado.

3 En *Correo electrónico para compartir*, haga clic en **Agregar nuevo**.

4 Ingrese una dirección de correo electrónico válida de un usuario externo o interno que no esté en su grupo de acceso y haga clic en la marca de verificación para guardarla. Puede agregar hasta diez direcciones individuales a la vez.

> **NOTA:**
> Para eliminar una dirección de correo electrónico, haga clic en **X**. El nombre de la persona que comparte el documento se destaca y no se puede seleccionar ni eliminar.

5 En Grupos disponibles, se muestran sus grupos de acceso. Haga clic en **Seleccionar todo** o haga clic en el icono de flecha junto a una opción para agregar a *Grupos compartidos* o para eliminar.

6 Haga clic en **Aceptar**.

> **NOTA:**
> Los usuarios externos no pueden compartir el documento protegido con otro usuario externo.

Si esta es la primera vez que un usuario externo recibe un archivo protegido de Data Guardian, el usuario debe instalar el portal web.

Identifier	**GUID-5BE95524-98D7-476C-9790-CA2298568418**
Status	**In Translation**

Compartir archivos protegidos previamente como un usuario externo

Debe tener Data Guardian instalado y asignado a uno o más grupos de acceso.
Si usted creó el archivo o es el propietario de un archivo protegido, puede compartir previamente el archivo con un usuario interno. No puede compartir el documento protegido con otro usuario externo. Si no es el propietario del archivo, no puede compartirlo.

- El *correo electrónico para compartir* no enumera los nombres de otros usuarios con los que se ha compartido el documento protegido.
- No se muestran grupos en Grupos disponibles. Solo puede compartir archivos con personas.

1 Haga clic con el botón secundario en un archivo protegido y seleccione **Acceso a archivos protegidos**.

En la interfaz de usuario de *uso compartido de acceso a archivo protegido*, el nombre del documento se muestra en Archivo seleccionado.

2 En *correo electrónico para compartir*, haga clic en **Agregar** e ingrese una dirección de correo electrónico válida de un usuario externo o interno que no esté en el grupo de acceso.

Puede agregar hasta diez direcciones individuales a la vez.

3 Para modificar una dirección de correo electrónico, haga clic en **Modificar**.

4 Para eliminar una dirección de correo electrónico, seleccione una entrada y haga clic en **Eliminar**.

> **NOTA:**
> Como propietario del archivo, no puede seleccionar ni eliminar su nombre.

5 Haga clic en **Aceptar**. Se mostrará un mensaje de finalización satisfactoria.

Si esta es la primera vez que un usuario recibe un archivo protegido de Data Guardian, este debe instalar Data Guardian o utilizar el portal web para ver el archivo protegido.

Identifier	GUID-F97CE528-0A49-4763-80D0-0F5937EAE934
Status	In Translation

Modificar quién tiene acceso a correos electrónicos protegidos

Según la política establecida por el administrador, puede hacer clic con el botón secundario en un correo electrónico que haya protegido y enviado a los usuarios de su Grupo de acceso. Puede modificar quién tiene acceso a ese correo electrónico.

1 En Outlook, haga clic con el botón secundario en un correo electrónico etiquetado como [PROTEGIDO].

2 En la parte inferior, seleccione **Acceso de correo electrónico protegido**.

Se muestra una lista de los usuarios con los cuales se ha compartido el acceso.

3 Elimine usuarios individuales si ya no desea que tengan acceso al correo electrónico protegido.

Identifier	GUID-F553E0C3-FCF3-4782-8FD4-
Status	Translation Validated

Preguntas más frecuentes

Identifier	GUID-D70F8E30-C205-474A-BC17-DB3867AE07AE
Status	In Translation

Preguntas más frecuentes sobre diversos temas

Pregunta

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

Solución

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

Identifier	GUID-36E78894-7902-4034-8BFA-6D63A1743855
Status	Translation Validated

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 del área de notificaciones tiene una marca de verificación 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 de verificación *Abrir* no está seleccionada.
6 Haga clic en **Aceptar**.