Recuperación de Encryption

Encryption v10.0/Data Guardian v2.0

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.

Encryption v10.0/Data Guardian v2.0

2018 - 08

Rev. A01

Contenido

1

Introducción a la recuperación

En esta sección se describe lo necesario para crear un entorno de recuperación.

- Medios CD-R, DVD-R o medios USB formateados
  - Si va a grabar un CD o DVD, consulte Grabar la ISO del entorno de recuperación en CD/DVD para obtener más información.
  - Si va a utilizar un medio USB, consulte Grabar el entorno de recuperación en un medio extraíble para obtener más información.
- Paquete de recuperación para dispositivos en error
  - Para clientes administrados remotamente, las instrucciones siguientes explican cómo recuperar un paquete de recuperación desde su Dell Servidor de administración de seguridad.
  - Para clientes administrados localmente, el paquete de recuperación se creó durante la configuración en una unidad de red compartida o en un medio externo. Localice este paquete antes de continuar.

Cómo ponerse en contacto con Dell ProSupport

Llame al 877-459-7304, extensión 4310039 para obtener soporte telefónico sobre su producto Dell 24 horas al día, 7 días a la semana.

De manera adicional, puede obtener soporte en línea para los productos Dell en dell.com/support. El soporte en línea incluye controladores, manuales, recomendaciones técnicas, P+F y posibles problemas.

Tenga su Código de servicio rápido o Etiqueta de servicio a mano cuando realice la llamada para asegúrese de ayudarnos a conectarle rápidamente con el experto técnico adecuado.

Para obtener los números de teléfono fuera de los Estados Unidos, consulte Números de teléfono internacionales de Dell ProSupport.

2

Recuperación de cifrado basado en la política o de archivo/carpeta

Se requiere una recuperación cuando la computadora cifrada no inicia en el sistema operativo. Esto se produce cuando el registro se modifica de forma incorrecta o si han ocurrido cambios de hardware en una computadora cifrada.

Con la recuperación de cifrado basado en la política o cifrado de archivo/carpeta (FFE), puede recuperar el acceso a lo siguiente:

- A un equipo que no se inicia y que muestra una petición para realizar recuperación de SDE.
- A una computadora que muestra un pantallazo azul con un código STOP de 0x6f o 0x74.
- A un equipo en el que no se pueden editar políticas ni acceder a los datos cifrados.
- A un servidor que ejecuta Dell Encryption que cumple con las condiciones anteriores.
- A un equipo en el que se debe sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM.

NOTA: Hardware Crypto Accelerator no es compatible, a partir de v8.9.3.

Descripción general del proceso de recuperación

NOTA: La recuperación requiere un entorno de 32 bits.

Para recuperar un sistema defectuoso:

1. Grabe el entorno de recuperación en un CD/DVD o cree una unidad USB de arranque. Consulte Apéndice A - Grabar el entorno de recuperación.
2. Obtenga el archivo de recuperación.
3. Realice la recuperación.

Realizar el cifrado basado en la política o la recuperación de FFE

Siga estos pasos para realizar el cifrado basado en la política o la recuperación de FFE.

Obtención del archivo de recuperación: cliente de cifrado FFE o cifrado basado en políticas

Para descargar el archivo de recuperación:

1. Descargue el paquete de instalación de Dell Encryption desde http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers . Diríjase a la carpeta **AdminUtilities** del paquete de instalación y abra **CMGAd.exe**.
2. En el campo **Servidor de Dell**, ingrese el Security Management Server/Security Management Server Virtual en el que se activó la computadora.
3. En el campo **Administrador de Dell**, ingrese un nombre de cuenta de usuario que tenga privilegios de administrador forense.
4. En el campo **Contraseña**, ingrese la contraseña del administrador forense.

5 En el campo **MCID**, ingrese el FQDN del dispositivo que se desea recuperar.

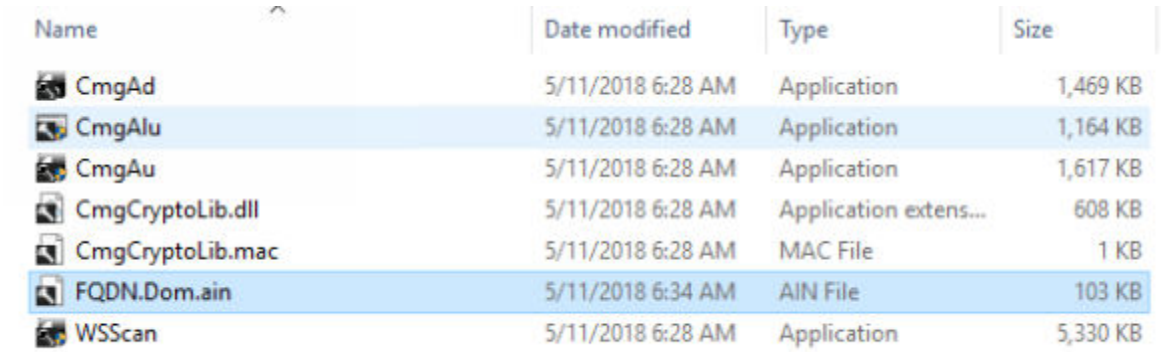
- En el campo **DCID** corresponde al identificador de recuperación del dispositivo que se desea recuperar.

6 Seleccione **Siguiente**.

7 Defina y confirme una **frase de contraseña** para el archivo de recuperación. Esta frase de contraseña es necesaria para realizar la recuperación.

8 En el campo **Descargar en:**, ingrese una ubicación de destino para el paquete de recuperación y seleccione **Siguiente**. De manera predeterminada, esta se encontrará en el directorio desde el cual se ejecutó CMGAd.exe.

9 El paquete de recuperación descarga en la carpeta especificada en **Descargar en:**.



10 Copie el archivo del paquete de recuperación en una ubicación a la que se pueda acceder al arrancar en WinPE.

Obtener el archivo de recuperación - Equipo administrado localmente

Para obtener el archivo de recuperación de Encryption Personal:

1 Localice el archivo de recuperación denominado **LSARecovery_<systemname> > .exe**. Este archivo fue almacenado en una unidad de red o unidad de almacenamiento extraíble al hacerse la instalación de Encryption Personal por medio del asistente de configuración.

2 Copie **LSARecovery_<systemname> > .exe** en el equipo de destino (el equipo que tiene los datos que desea recuperar).

Realizar una recuperación

1 Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar. Se abre un entorno WinPE.

> **NOTA: Desactive SecureBoot antes de comenzar el proceso de recuperación. Cuando haya terminado, vuelva a activar SecureBoot.**

2 Ingrese **x** y pulse **Intro** para acceder al símbolo del sistema.

3 Vaya al archivo de recuperación e inícielo.

4 Seleccione una opción:

- Mi sistema no se inicia y muestra un mensaje que me pide que ejecute la recuperación SDE.

  Esto le permitirá volver a crear las comprobaciones de hardware que realiza el cliente Encryption cuando lo inicia en el SO.

- Mi sistema no me permite el acceso a la información cifrada, ni modificar las políticas, o se está reinstalando.

  Utilícelo si se debe sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM.

5 En el cuadro de diálogo Información de recuperación y copia de seguridad, confirme que es correcta la información acerca del equipo cliente que se debe recuperar y haga clic en **Siguiente**.

Al recuperar equipos que no sean de Dell, los campos Número de serie y Etiqueta de activos se dejarán en blanco.

6 En el cuadro de diálogo que muestra los volúmenes del equipo, seleccione todas las unidades correspondientes y haga clic en **Siguiente**.

Haga clic en Mayús o Ctrl para resaltar varias unidades.

Si la unidad seleccionada no tiene cifrado basado en la política o FFE, no se realizará la recuperación.

7 Ingrese su contraseña de recuperación y haga clic en **Siguiente**.

Con un cliente administrado de forma remota, esta es la contraseña proporcionada en el paso 3 en Obtener el archivo de recuperación - Equipo administrado de forma remota.

En Encryption Personal, la contraseña es la Contraseña del administrador de cifrado que se estableció para el sistema al custodiar las claves.

8 En el cuadro de diálogo Recuperar, haga clic en **Recuperar**. Se inicia el proceso de recuperación.

9 Una vez completada la recuperación, haga clic en **Finalizar**.

> **NOTA:**
>
> Asegúrese de extraer cualquier medio USB o CD\DVD que utilizó para iniciar la máquina. Si no hace esto, es posible que se vuelva a iniciar al entorno de recuperación.

10 Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

Recuperación de datos con unidad de cifrado

Si el equipo de destino no puede iniciarse y no hay ningún error de hardware, la recuperación de datos se puede realizar en un equipo iniciado en un entorno de recuperación. Si el equipo de destino no puede iniciarse y ha fallado el hardware o es un dispositivo USB, la recuperación de datos se puede realizar iniciando en una unidad secundaria. Cuando utiliza una unidad, verá el sistema de archivos y podrá navegar por los directorios. Sin embargo, si intenta abrir o copiar un archivo, se producirá un error *Acceso denegado*.

Recuperar datos con unidad de cifrado

Para recuperar datos con unidad de cifrado:

1 Para obtener la Id. de recuperación/DCID del equipo, seleccione una opción:
   a Ejecute WSScan en cualquier carpeta donde se almacenan los datos cifrados comunes.
   Se muestra el ID de recuperación/DCID de ocho caracteres después de "Común".

   b Abra la Remote Management Console y selecciona la pestaña **Detalles y acciones** del extremo.
   c En la sección Detalle de Shield de la pantalla Detalles de extremo, localice la Id. de recuperación/DCID.

2 Para descargar la clave desde el servidor, vaya a la utilidad Dell Administrative Unlock (**CMGAu**).
   La utilidad Dell Administrative Unlock se puede obtener desde Dell ProSupport.

3 En el cuadro de diálogo Dell Administrative Utility (CMGAu), ingrese la siguiente información (algunos campos se rellenan previamente) y haga clic en **Siguiente**.
   Servidor: nombre del host completo del servidor, por ejemplo:

   Servidor de dispositivos (clientes anteriores a 8.x): **https://<server.organization.com>:8081/xapi**

   Servidor de seguridad: **https://<server.organization.com>:8443/xapi/**

   Admin Dell: el nombre de la cuenta para el administrador forense (habilitado en Security Management Server/Security Management Server Virtual)

   Contraseña de Admin Dell: la contraseña de la cuenta del administrador forense (habilitado en Security Management Server/Security Management Server Virtual)

   MCID: borre el campo MCID

   DCID: el ID de recuperación/DCID que ha obtenido antes.

4 En el cuadro de diálogo Dell Administrative Utility, seleccione **No, realizar una descarga desde un servidor ahora** y haga clic en **Siguiente**.

   NOTA:
   Si no tiene instalado el cliente Encryption, se muestra el mensaje *Error de desbloqueo*. Muévalo a un equipo que tenga instalado cliente Encryption.

5 Cuando la descarga y el desbloqueo se hayan completado, copie los archivos que necesite recuperar de esta unidad. Se pueden leer todos los archivos. ***No haga clic en Finalizar hasta que haya recuperado los archivos***.

6 Cuando haya recuperado los archivos y ya pueda volver a bloquearlos, haga clic en **Finalizar**.
   Después de hacer clic en Finalizar, los archivos cifrados ya no estarán disponibles.

Recuperación de Hardware Crypto Accelerator

NOTA: Hardware Crypto Accelerator no es compatible, a partir de v8.9.3.

Con la recuperación de Hardware Crypto Accelerator (HCA), puede recuperar el acceso a lo siguiente:

- Archivos en una unidad cifrada de HCA: este método descifra la unidad mediante las claves proporcionadas. Puede seleccionar la unidad específica que necesita descifrar durante el procesado de recuperación.
- Una unidad cifrada de HCA después de la sustitución del hardware: este método se utiliza después de sustituir la tarjeta de Hardware Crypto Accelerator o la placa base/TPM. Puede ejecutar una recuperación para volver a tener acceso a los datos cifrados sin tener que descifrar la unidad.

Requisitos de recuperación

Para la recuperación de HCA, necesita lo siguiente:

- Acceso a la ISO de entorno de recuperación (la recuperación requiere un entorno de 32 bits)
- CD\DVD o medios USB de arranque

Descripción general del proceso de recuperación

NOTA: La recuperación requiere un entorno de 32 bits.

Para recuperar un sistema defectuoso:

1. Grabe el entorno de recuperación en un CD/DVD o cree una unidad USB de arranque. Consulte Apéndice A - Grabar el entorno de recuperación.
2. Obtenga el archivo de recuperación.
3. Realice la recuperación.

Realizar la recuperación de HCA

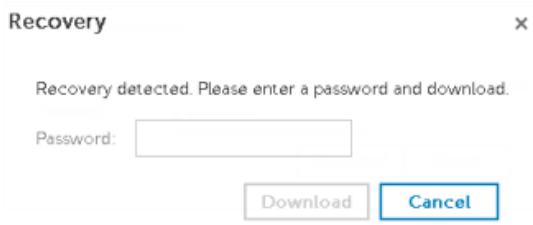
Siga estos pasos para realizar la recuperación de HCA.

Obtener el archivo de recuperación - Equipo administrado de forma remota

Para descargar el archivo **<machinename_domain.com>.exe** que se generó al instalar Dell Encryption:

1. Abra la consola de administración remota y, desde el panel izquierdo, seleccione **Administración** > **Recuperar extremo**.
2. En el campo Nombre de host, ingrese el nombre de dominio completo del extremo y haga clic en **Buscar**.
3. En la ventana Recuperación, ingrese una contraseña de recuperación y haga clic en **Descargar**.

   NOTA:
   Debe recordar esta contraseña para acceder a las claves de recuperación.



Obtener el archivo de recuperación - Equipo administrado localmente

Para obtener el archivo de recuperación de Encryption Personal:

1 Localice el archivo de recuperación denominado **LSARecovery_<systemname> > .exe**. Este archivo fue almacenado en una unidad de red o unidad de almacenamiento extraíble al hacerse la instalación de Encryption Personal por medio del asistente de configuración.

2 Copie **LSARecovery_<systemname> > .exe** en el equipo de destino (el equipo que tiene los datos que desea recuperar).

Realizar una recuperación

1 Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar.

Se abre un entorno WinPE.

NOTA: Desactive SecureBoot antes de comenzar el proceso de recuperación. Cuando haya terminado, active SecureBoot.

2 Escriba **x** y pulse **Intro** para acceder al símbolo del sistema.

3 Vaya al archivo de recuperación guardado e inícielo.

4 Seleccione una opción:

- Deseo descifrar mi unidad HCA cifrada.
- Deseo restaurar el acceso a mi unidad HCA cifrada.

5 En el cuadro de diálogo nformación de recuperación y copia de seguridad, confirme que el número de activo o la etiqueta de servicio son correctos y haga clic en **Siguiente**.

6 En el cuadro de diálogo que muestra los volúmenes del equipo, seleccione todas las unidades correspondientes y haga clic en **Siguiente**.

Haga clic en Mayús o Ctrl para resaltar varias unidades.

Si la unidad seleccionada no está cifrada con HCA, no se realizará la recuperación.

7 Ingrese su contraseña de recuperación y haga clic en **Siguiente**.

En un equipo administrado de forma remota, esta es la contraseña proporcionada en el paso 3 in Obtener el archivo de recuperación - Equipo administrado de forma remota.

En un equipo administrado localmente, la contraseña es la Contraseña del administrador de cifrado que estableció el sistema en Personal Edition al custodiar las claves.

8 En el cuadro de diálogo Recuperar, haga clic en **Recuperar**. Se inicia el proceso de recuperación.

9 Cuando se le solicite, vaya al archivo de recuperación guardado y haga clic en **Aceptar**.

Si está realizando un descifrado completo, el siguiente cuadro de diálogo mostrará el estado. Este proceso puede tardar un poco.

10 Cuando se muestre el mensaje para indicar que la recuperación ha finalizado correctamente, haga clic en **Finalizar**. Se reinicia el equipo.

Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

Recuperación de la unidad de cifrado automático (SED)

Con la recuperación de SED, puede recuperar el acceso a los archivos en una SED mediante los siguientes métodos:

- Realice un desbloqueo único de la unidad para omitir la autenticación previa al inicio (PBA).
- Desbloquéela y, a continuación, quite de forma permanente la PBA de la unidad. El inicio de sesión único no funcionará con la PBA quitada.
  - En un cliente SED administrado remotamente, para quitar la PBA, tendrá que desactivar el producto desde la Remote Management Console si es necesario para volver a habilitar la PBA en un futuro.
  - En un cliente SED administrado localmente, para quitar la PBA, tendrá que desactivar el producto del SO si es necesario para volver a habilitar la PBA en un futuro.

Requisitos de recuperación

Para la recuperación de SED, necesita lo siguiente:

- Acceso a la ISO de entorno de recuperación
- CD\DVD o medios USB de arranque

Descripción general del proceso de recuperación

NOTA: La recuperación requiere un entorno de 64 bits o 32 bits según el modo de arranque del BIOS.

Para recuperar un sistema defectuoso:

1 Grabe el entorno de recuperación en un CD/DVD o cree una unidad USB de arranque. Consulte Apéndice A - Grabar el entorno de recuperación.
2 Obtenga el archivo de recuperación.
3 Realice la recuperación.

Realizar la recuperación de SED

Siga estos pasos para realizar la recuperación de SED.

Obtener el archivo de recuperación - Cliente SED administrado remotamente

Obtenga el archivo de recuperación.

El archivo de recuperación se puede descargar desde la Remote Management Console. Para descargar el archivo *<hostname>-sed-recovery.dat* que se generó al instalar Dell Data Security:

a Abra la Remote Management Console y, en el panel izquierdo, seleccione **Administración > Recuperar datos**. A continuación, seleccione la pestaña **SED**.

b En la pantalla Recuperar datos, en el campo Nombre de host, ingrese el nombre de dominio completo del extremo y, a continuación, haga clic en **Buscar**.
c En el campo SED, seleccione una opción.
d Haga clic en **Crear archivo de recuperación**.
El archivo **<hostname>-sed-recovery.dat** se descarga.

Obtener el archivo de recuperación - Cliente SED administrado localmente

Obtenga el archivo de recuperación.

Se ha generado el archivo y se puede acceder a él desde la ubicación de la copia de seguridad que seleccionó al instalar Advanced Authentication en la computadora. El nombre de archivo es *OpalSPkey<systemname>.dat*.

Realizar una recuperación

1 Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar. Se abre un entorno de WinPE con la aplicación de recuperación.

NOTA: Desactive SecureBoot antes de comenzar el proceso de recuperación. Cuando haya terminado, active SecureBoot.

2 Elija una opción y pulse **Intro**.
3 Seleccione **Examinar**, localice el archivo de recuperación y, a continuación, haga clic en **Abrir**.
4 Seleccione una opción y haga clic en **Aceptar**.
- **Desbloqueo único de la unidad:** este método ignora la PBA.
- **Desbloquear unidad y eliminar la PBA**: este método desbloquea y luego elimina permanentemente la PBA de la unidad. Si quiere quitar la PBA tendrá que desactivar el producto desde la Remote Management Console (para un cliente SED administrado remotamente) o en el SO (para un cliente SED administrado localmente) si es necesario para volver a habilitar la PBA en el futuro. El inicio de sesión único no funcionará con la PBA quitada.

5 La recuperación está ahora completada. Presione cualquier tecla para volver al menú.
6 Pulse **r** para reiniciar el equipo.

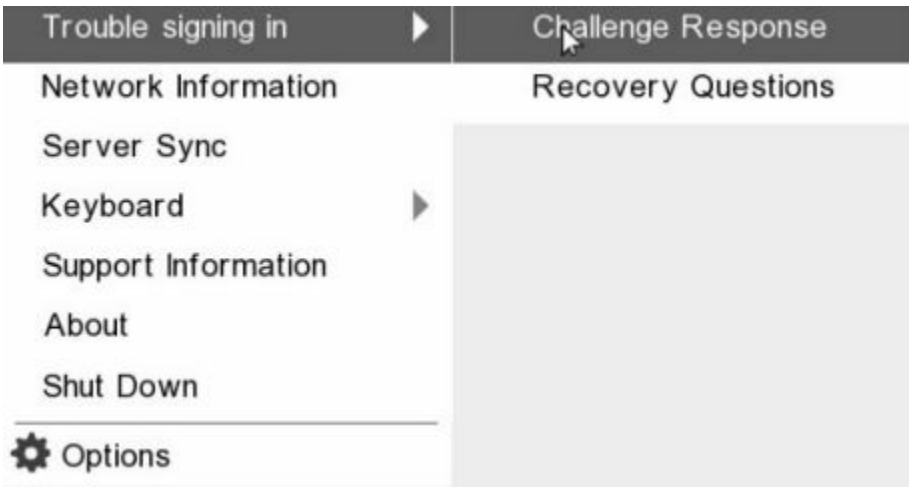
NOTA:
Asegúrese de extraer cualquier medio USB o CD\DVD que utilizó para iniciar el equipo. Si no hace esto, es posible que se vuelva a iniciar al entorno de recuperación.

7 Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

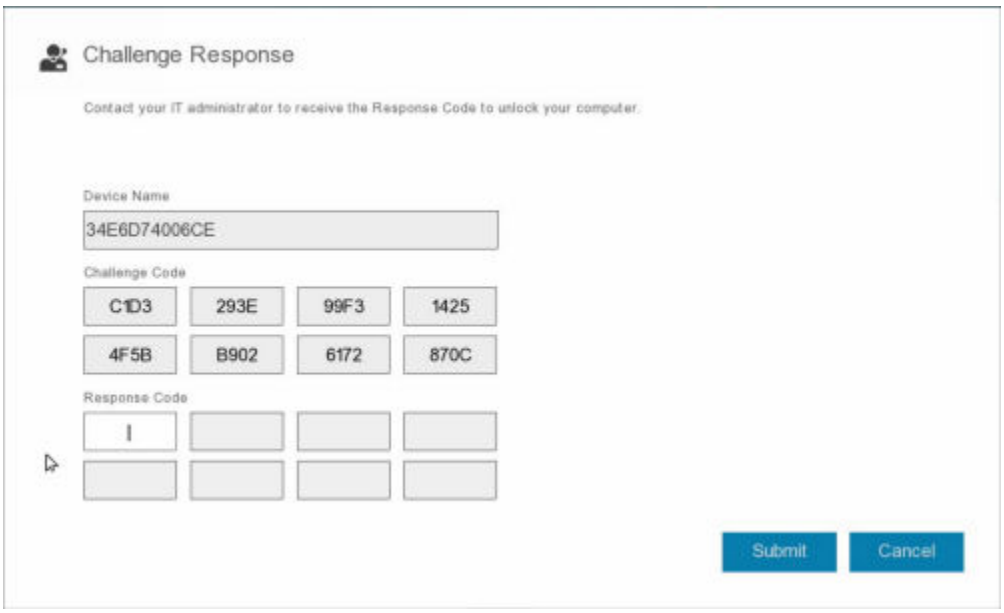
Recuperación de desafío con SED

Omitir el entorno de autenticación previa al inicio

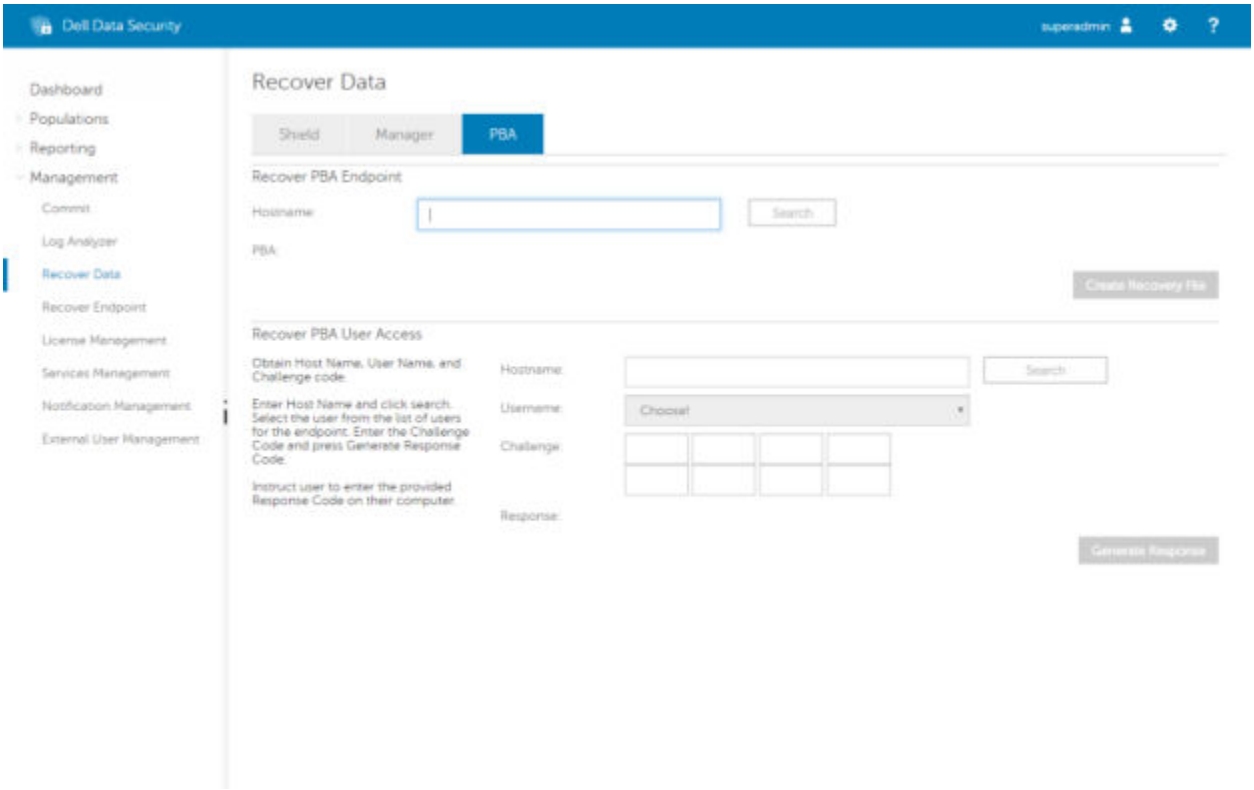
Los usuarios olvidan sus contraseñas y llaman a la mesa de ayuda solicitando acceder al entorno PBA. Utilice el mecanismo Desafío/Respuesta que está integrado en el dispositivo. Este es un mecanismo que funciona por usuario y se basa en un conjunto rotativo de caracteres alfanuméricos. El usuario debe ingresar su nombre en el campo **Nombre de usuario** y, luego, seleccionar **Opciones > Respuesta de desafío**.



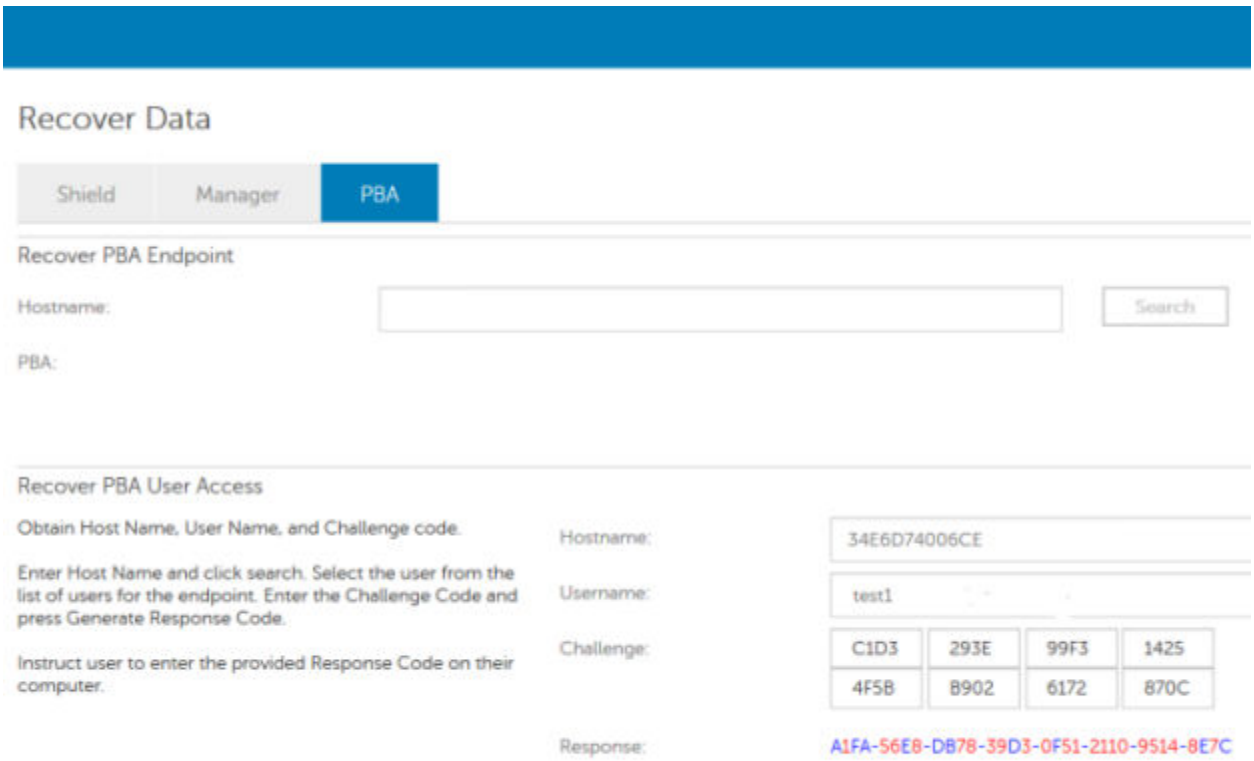
Aparece la siguiente información después de seleccionar **Respuesta de desafío**.



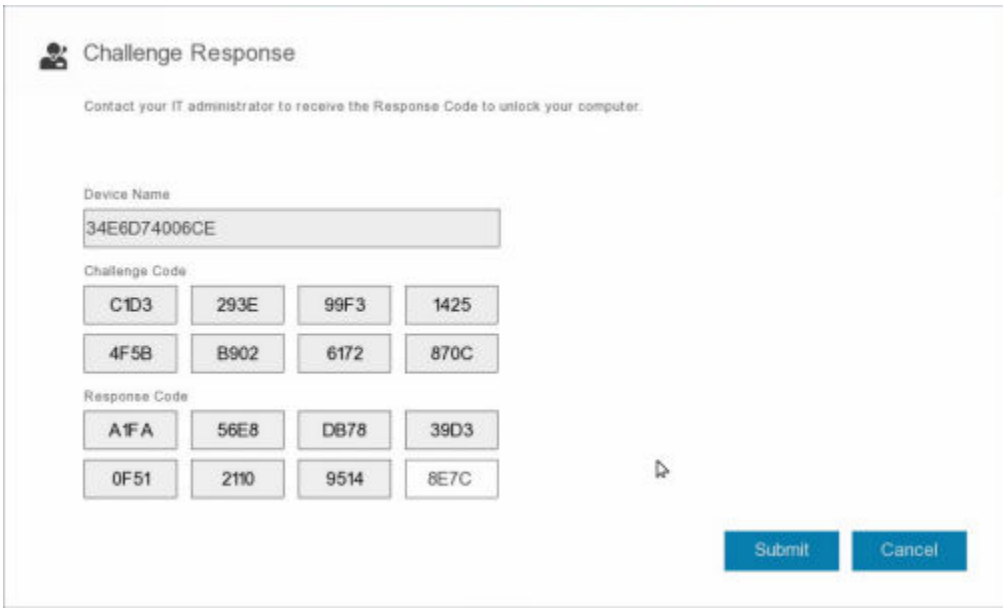
El campo **Nombre de dispositivo** se utiliza por los técnicos de la mesa de ayuda dentro de la consola de administración remota para encontrar el dispositivo correcto y, luego, seleccionar un nombre de usuario. Se encuentra dentro **Administración > Recuperar datos** en la pestaña **PBA**.



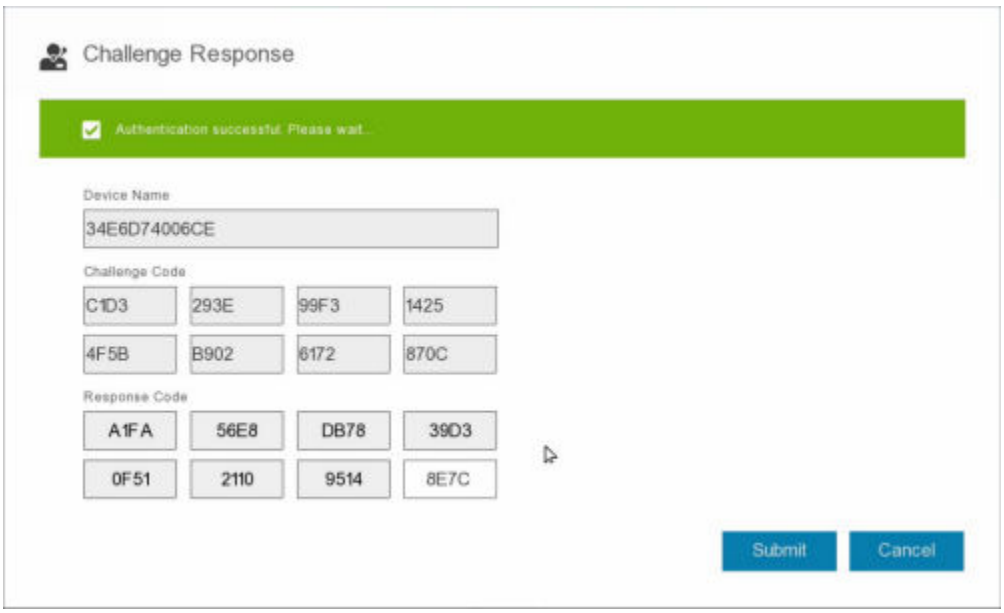
Se proporciona el Código de desafío al técnico de la mesa de ayuda, quién ingresa los datos y, luego, hace clic en el botón **Generar respuesta**.



Estos datos resultantes poseen colores a juego para ayudar a distinguir entre números (rojo) y caracteres alfabéticos (azul). Estos datos se leen al usuario final, quien los ingresa en el entorno PBA y, luego, hace clic en el botón **Enviar**, moviendo al usuario a Windows.



Después de realizar una autenticación exitosa, aparecerá el siguiente mensaje:



Recuperación de desafío finalizada.

5

Recuperación de cifrado de disco completo

La recuperación le permite recuperar el acceso a archivos en una unidad cifrada con cifrado de disco completo.

NOTA: No se debe interrumpir el descifrado. Si el descifrado se interrumpe, se puede producir la pérdida de datos.

Requisitos de recuperación

Para una recuperación de cifrado de disco completo, necesita lo siguiente:

- Acceso a la ISO de entorno de recuperación
- CD\DVD o medios USB de arranque

Descripción general del proceso de recuperación

NOTA: La recuperación requiere un entorno de 64 bits.

Para recuperar un sistema defectuoso:

1 Grabe el entorno de recuperación en un CD/DVD o cree una unidad USB de arranque. Consulte Apéndice A - Grabar el entorno de recuperación.
2 Obtenga el archivo de recuperación.
3 Realice la recuperación.

Realizar recuperación de cifrado de disco completo

Siga estos pasos para realizar una recuperación de cifrado de disco completo.

Obtener el archivo de recuperación: cliente de cifrado de disco completo

Obtenga el archivo de recuperación.

Descargue el archivo de recuperación desde la consola de administración remota. Para descargar el archivo *<hostname>-sed-recovery.dat* que se generó al instalar Dell Data Security:

a Abra la consola de administración remota y, desde el panel izquierdo, seleccione **Administración > Recuperar datos**. A continuación, seleccione la pestaña **PBA**.
b En la pantalla Recuperar datos, en el campo Nombre de host, ingrese el nombre de dominio completo del extremo y, a continuación, haga clic en **Buscar**.
c En el campo SED, seleccione una opción.
d Haga clic en **Crear archivo de recuperación**.

El archivo **<hostname>-sed-recovery.dat** se descarga.

Realizar una recuperación

1 Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar. Se abre un entorno de WinPE con la aplicación de recuperación.

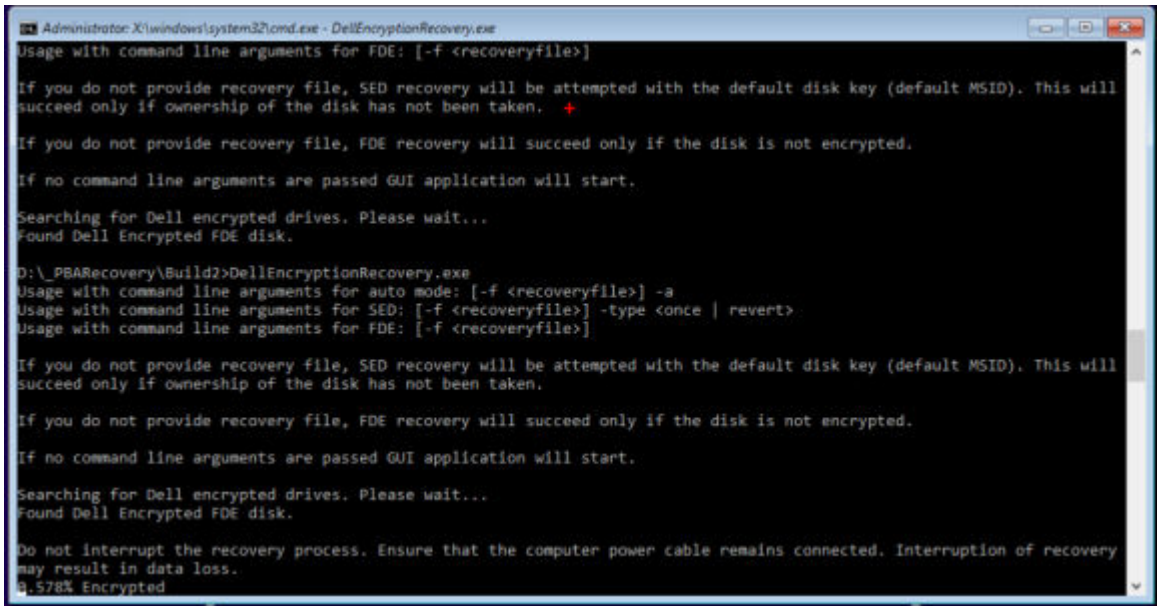
> **NOTA: Desactive SecureBoot antes de comenzar el proceso de recuperación. Cuando haya terminado, vuelva a activar SecureBoot.**

2 Elija una opción y pulse **Intro**.

3 Seleccione **Examinar**, localice el archivo de recuperación y, a continuación, haga clic en **Abrir**.

4 Haga clic en **Aceptar**.

.



5 La recuperación está ahora completada. Presione cualquier tecla para volver al menú.

6 Pulse **r** para reiniciar el equipo.

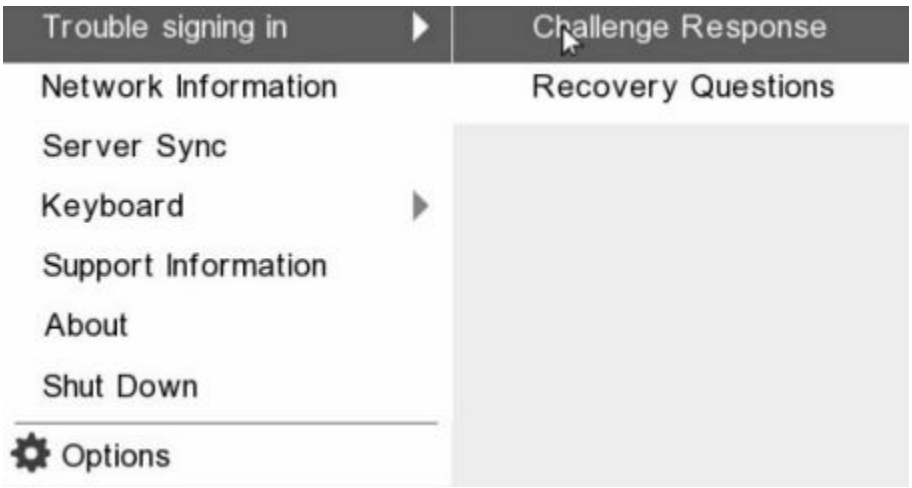
> **NOTA:**
> Asegúrese de extraer cualquier medio USB o CD\DVD que utilizó para iniciar el equipo. Si no hace esto, es posible que se vuelva a iniciar al entorno de recuperación.

7 Después de reiniciar el equipo, debe tener un equipo en pleno funcionamiento. Si los problemas continúan, póngase en contacto con Dell ProSupport.

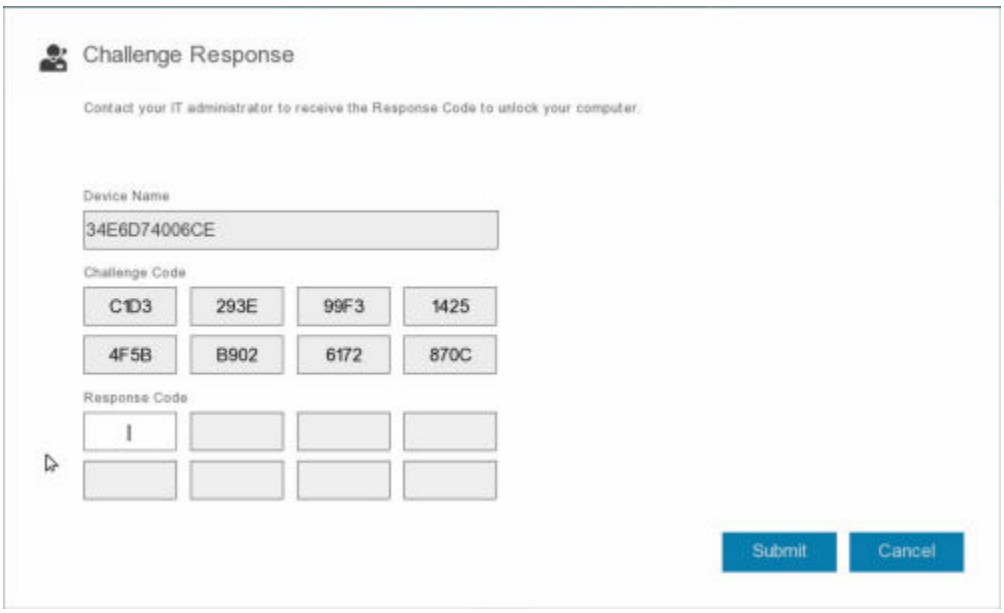
Recuperación de desafío con cifrado de disco completo

Omitir el entorno de autenticación previa al inicio

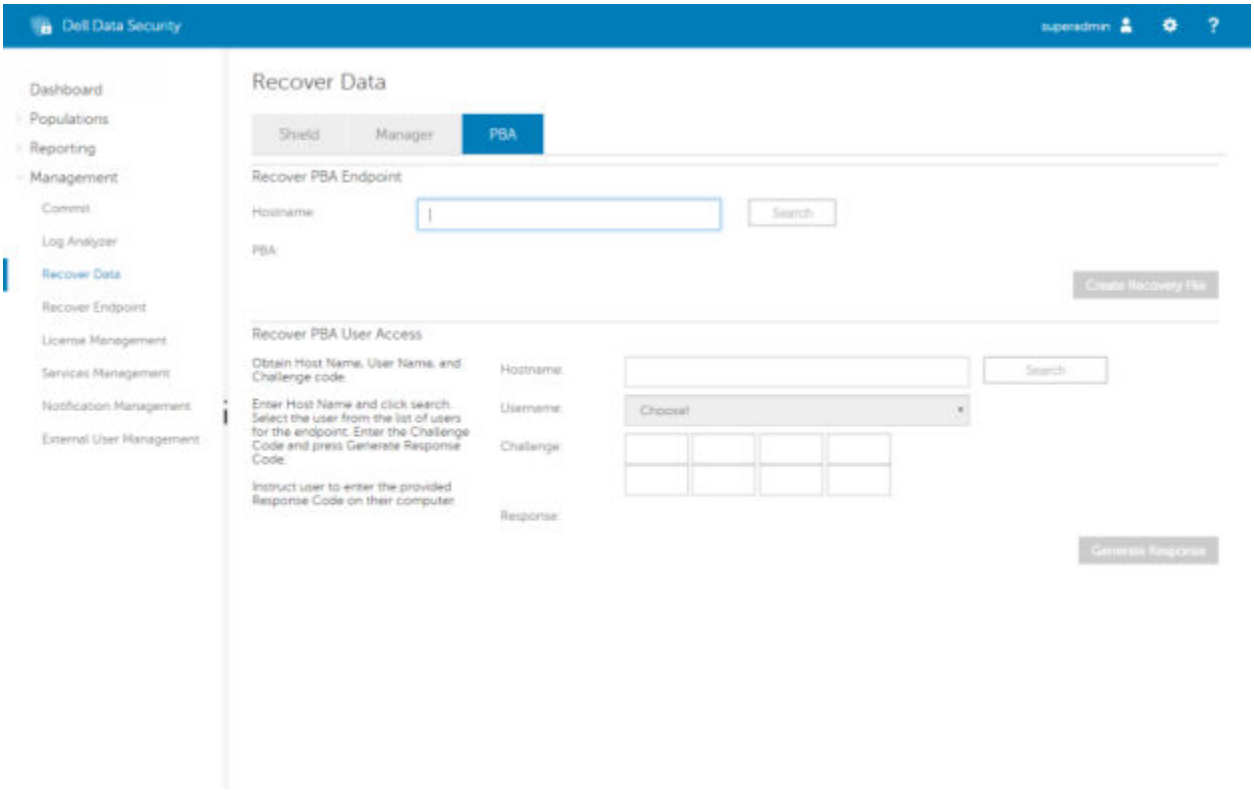
Los usuarios olvidan sus contraseñas y llaman a la mesa de ayuda solicitando acceder al entorno PBA. Utilice el mecanismo Desafío/Respuesta que está integrado en el dispositivo. Este es un mecanismo que funciona por usuario y se basa en un conjunto rotativo de caracteres alfanuméricos. El usuario debe ingresar su nombre en el campo **Nombre de usuario** y, luego, seleccionar **Opciones > Respuesta de desafío**.



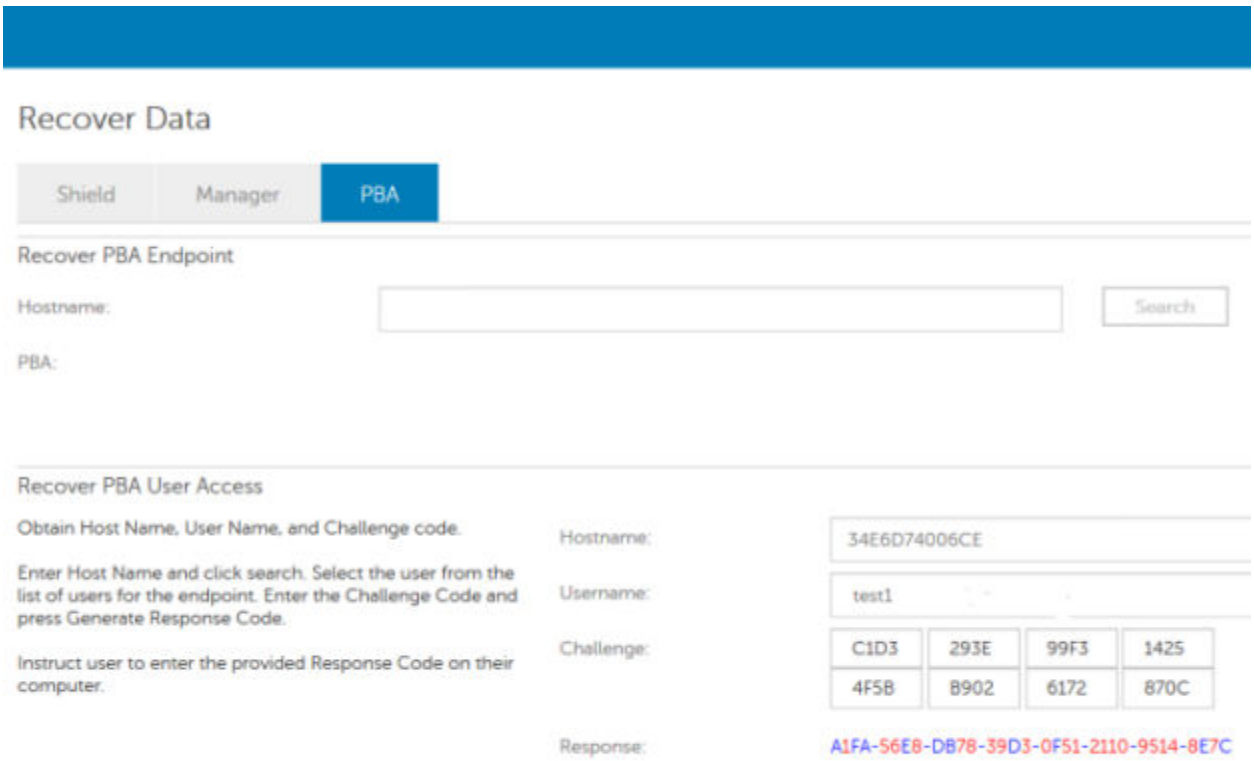
Aparece la siguiente información después de seleccionar **Respuesta de desafío**.



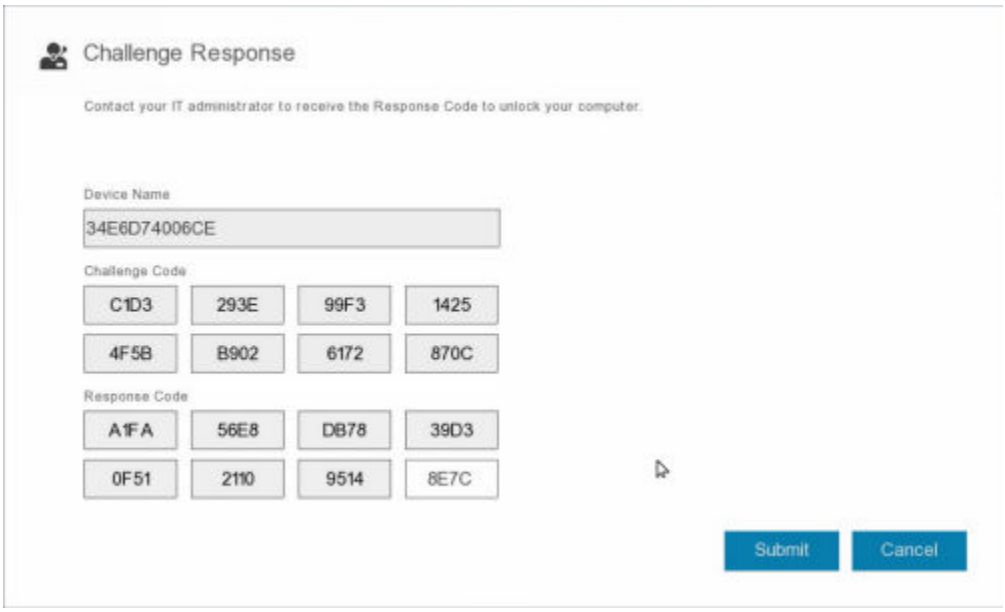
El campo **Nombre de dispositivo** se utiliza por los técnicos de la mesa de ayuda dentro de la consola de administración remota para encontrar el dispositivo correcto y, luego, seleccionar un nombre de usuario. Se encuentra dentro **Administración > Recuperar datos** en la pestaña **PBA**.



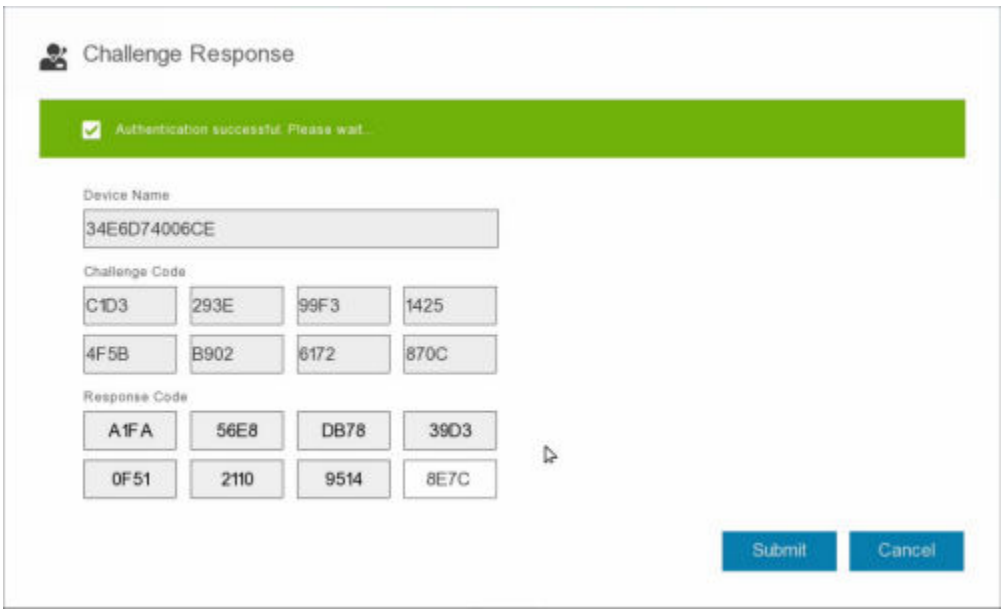
Se proporciona el Código de desafío al técnico de la mesa de ayuda, quién ingresa los datos y, luego, hace clic en el botón **Generar respuesta**.



Estos datos resultantes poseen colores a juego para ayudar a distinguir entre números (rojo) y caracteres alfabéticos (azul). Estos datos se leen al usuario final, quien los ingresa en el entorno PBA y, luego, hace clic en el botón **Enviar**, moviendo al usuario a Windows.



Después de realizar una autenticación exitosa, aparecerá el siguiente mensaje:



Recuperación de desafío finalizada.

6

Cifrado de disco completo y recuperación de Dell Encryption

En este capítulo se detallan los pasos de recuperación necesarios para restaurar el acceso a los archivos protegidos de Dell Encryption en un disco protegido con cifrado de disco completo.

NOTA: No se debe interrumpir el descifrado. Si el descifrado se interrumpe, se puede producir la pérdida de datos.

Requisitos de recuperación

Para realizar la recuperación de Dell Encryption y cifrado de disco completo, necesita lo siguiente:

- Acceso a la ISO de entorno de recuperación
- CD\DVD o medios USB de arranque

Descripción general del proceso de recuperación

NOTA: La recuperación requiere un entorno de 64 bits.

Para recuperar un sistema defectuoso:

1 Grabe el entorno de recuperación en un CD/DVD o cree una unidad USB de arranque. Consulte Apéndice A - Grabar el entorno de recuperación.
2 Obtenga los archivos de recuperación para Dell Encryption y el cifrado de disco completo.
3 Realice la recuperación.

Realización de la recuperación de un disco completo cifrado y de un disco cifrado de Dell

Siga estos pasos para realizar la recuperación de un disco completo cifrado y de un disco cifrado de Dell.

Obtener el archivo de recuperación: cliente de cifrado de disco completo

Obtenga el archivo de recuperación.

Descargue el archivo de recuperación desde la consola de administración remota. Para descargar el archivo *<hostname>-sed-recovery.dat* que se generó al instalar Dell Data Security:

a Abra la consola de administración remota y, desde el panel izquierdo, seleccione **Administración > Recuperar datos**. A continuación, seleccione la pestaña **PBA**.
b En la pantalla Recuperar datos, en el campo Nombre de host, ingrese el nombre de dominio completo del extremo y, a continuación, haga clic en **Buscar**.
c En el campo SED, seleccione una opción.

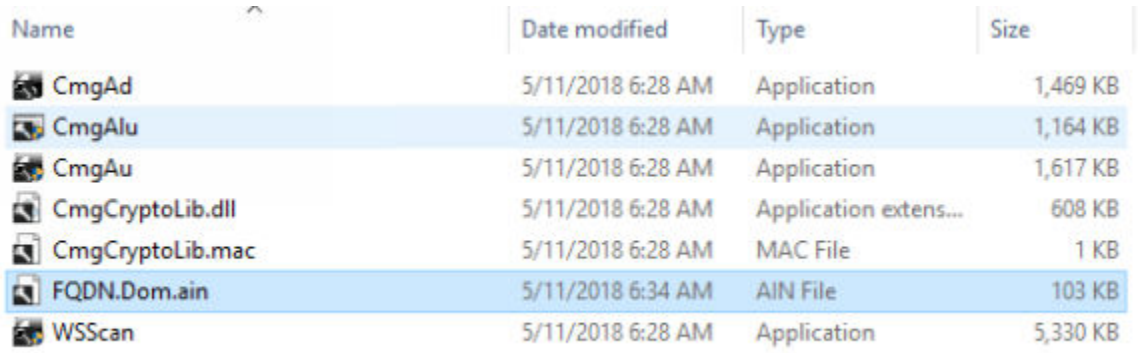
d Haga clic en **Crear archivo de recuperación**.
El archivo **<hostname>-sed-recovery.dat** se descarga.

Obtención del archivo de recuperación: cliente de cifrado FFE o cifrado basado en políticas

Para descargar el archivo de recuperación:

1 Descargue el paquete de instalación de Dell Encryption desde http://www.dell.com/support/home/us/en/19/product-support/product/dell-data-protection-encryption/drivers . Diríjase a la carpeta **AdminUtilities** del paquete de instalación y abra **CMGAd.exe**.
2 En el campo **Servidor de Dell**, ingrese el Security Management Server/Security Management Server Virtual en el que se activó la computadora.
3 En el campo **Administrador de Dell**, ingrese un nombre de cuenta de usuario que tenga privilegios de administrador forense.
4 En el campo **Contraseña**, ingrese la contraseña del administrador forense.
5 En el campo **MCID**, ingrese el FQDN del dispositivo que se desea recuperar.
   - En el campo **DCID** corresponde al identificador de recuperación del dispositivo que se desea recuperar.
6 Seleccione **Siguiente**.
7 Defina y confirme una **frase de contraseña** para el archivo de recuperación. Esta frase de contraseña es necesaria para realizar la recuperación.
8 En el campo **Descargar en:**, ingrese una ubicación de destino para el paquete de recuperación y seleccione **Siguiente**. De manera predeterminada, esta se encontrará en el directorio desde el cual se ejecutó CMGAd.exe.

9 El paquete de recuperación descarga en la carpeta especificada en **Descargar en:**.

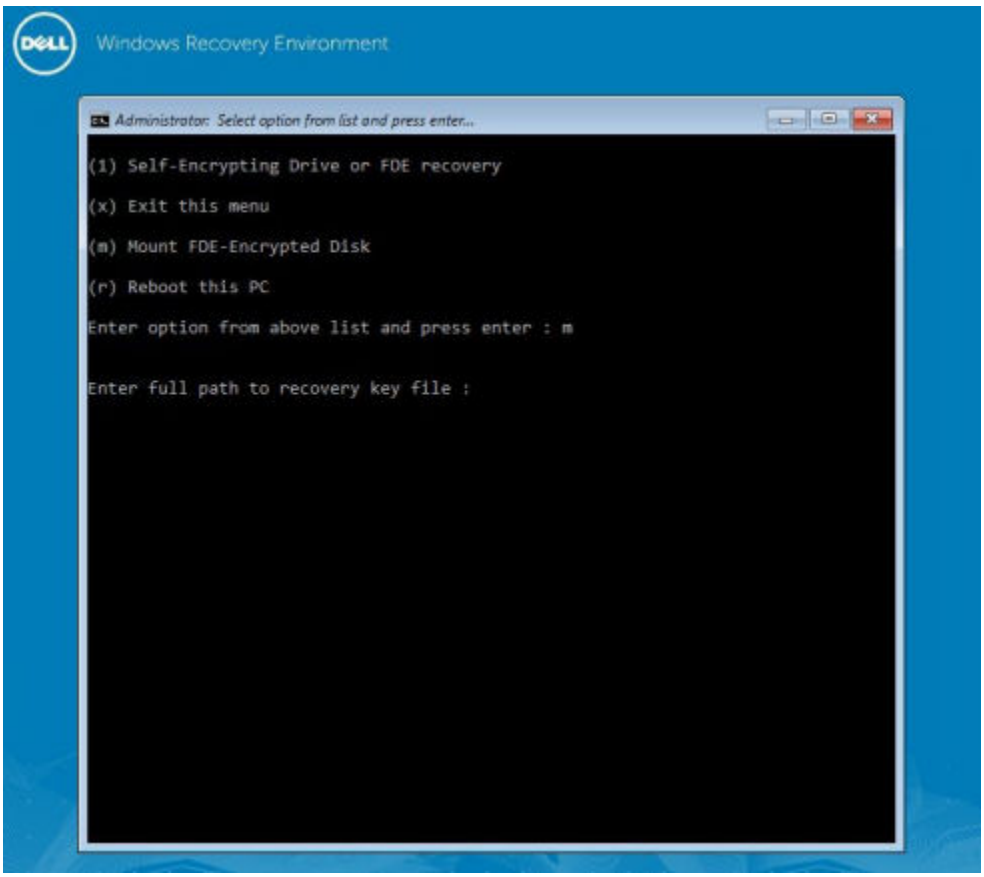


10 Copie el archivo del paquete de recuperación en una ubicación a la que se pueda acceder al arrancar en WinPE.

Realizar una recuperación

1 Con los medios de arranque creados anteriormente, realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar. Se abre un entorno de WinPE con la aplicación de recuperación.

NOTA: Desactive SecureBoot antes de comenzar el proceso de recuperación. Cuando haya terminado, vuelva a activar SecureBoot.



2 Seleccione la opción tres y presione **Intro**.

3 Cuando se le solicite, ingrese la ubicación y el nombre del archivo de recuperación.

4 Mediante el uso de la clave de recuperación, se monta el disco completo cifrado.

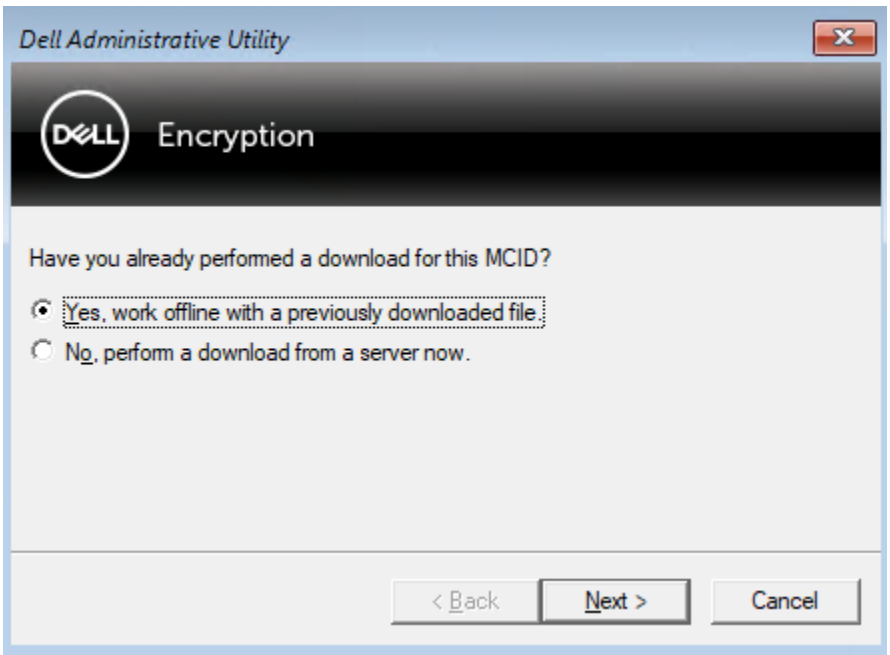
```
Enter option from above list and press enter : m

Enter the full path to the recovery key file: c:\recovery\opalSPKey.DESKTOP-XXYYZZ.recovery.dat

Recoveryfile loaded
====================   Disk 0   ====================
     Cylinders       = 15566
     Tracks/cylinder = 255
     Sectors/track   = 63
     Bytes/sector    = 512
     Disk size       = 128035676160 (Bytes)
                     = 119.24 GB
---> Disk 0, returned status...........: EDriverStatus_Success
====================   Disk 1   ====================
     Cylinders       = 973
     Tracks/cylinder = 255
     Sectors/track   = 63
     Bytes/sector    = 512
     Disk size       = 8004304896 (Bytes)
                     = 7.45 GB
---> Disk 0, returned status...........: EDriverStatus_DriveNotEncrypted
```

.

5 Diríjase a la utilidad CMGAu.exe con el siguiente comando: `cd DDPEAdminUtilities\`

6 Inicie CMGAu.exe con el siguiente comando: `\DDPEAdminUtilities>CmgAu.exe`

Seleccione **Sí, deseo trabajar sin conexión con un archivo descargado anteriormente**.



7 En el campo **Archivo descargado:**, ingrese la ubicación del **Paquete de recuperación**; a continuación, ingrese la **frase de contraseña** del administrador forense y seleccione **Siguiente**.

Una vez completada la recuperación, haga clic en **Finalizar**.

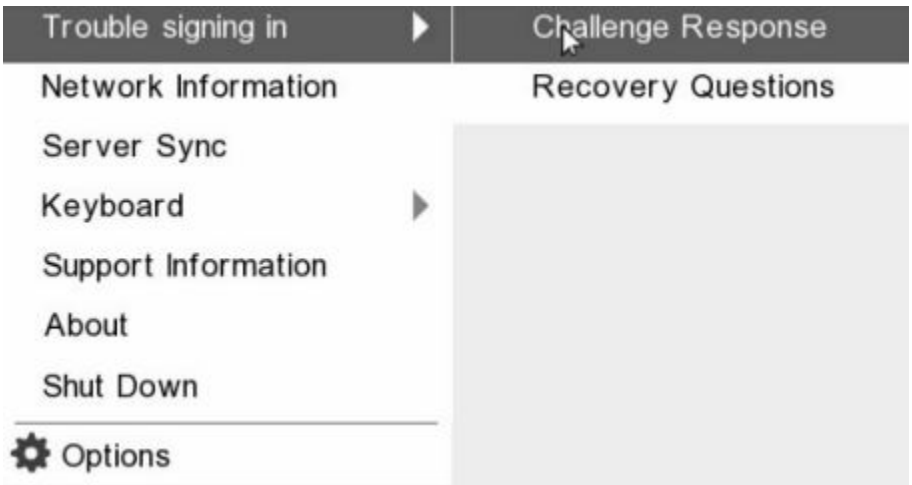
NOTA:
Asegúrese de extraer cualquier medio USB o CD\DVD que utilizó para iniciar el equipo. Si no hace esto, es posible que se vuelva a iniciar al entorno de recuperación.

8 Después de reiniciar la computadora, debería poder acceder a los archivos cifrados. Si los problemas continúan, póngase en contacto con Dell ProSupport.

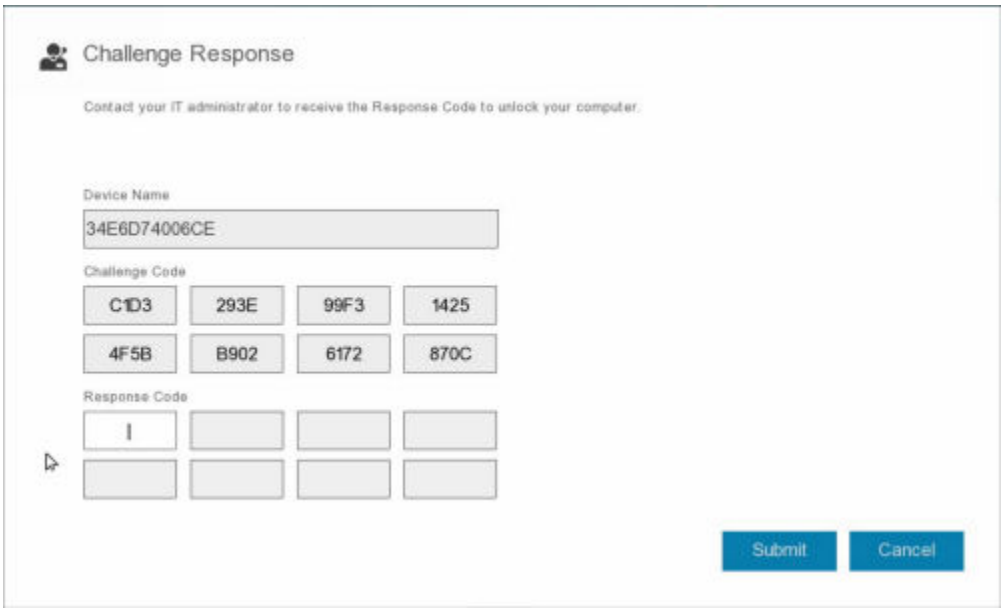
Recuperación de desafío con cifrado de disco completo

Omitir el entorno de autenticación previa al inicio

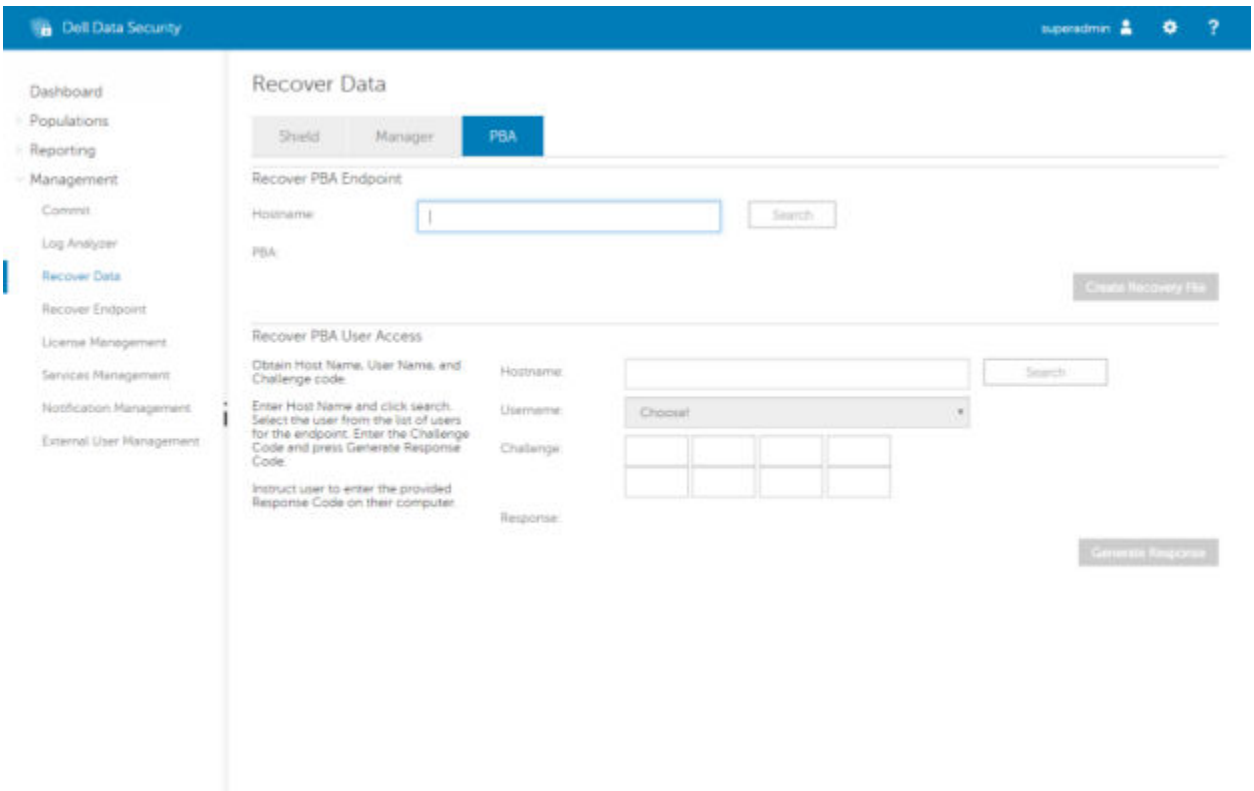
Los usuarios olvidan sus contraseñas y llaman a la mesa de ayuda solicitando acceder al entorno PBA. Utilice el mecanismo Desafío/Respuesta que está integrado en el dispositivo. Este es un mecanismo que funciona por usuario y se basa en un conjunto rotativo de caracteres alfanuméricos. El usuario debe ingresar su nombre en el campo **Nombre de usuario** y, luego, seleccionar **Opciones > Respuesta de desafío**.



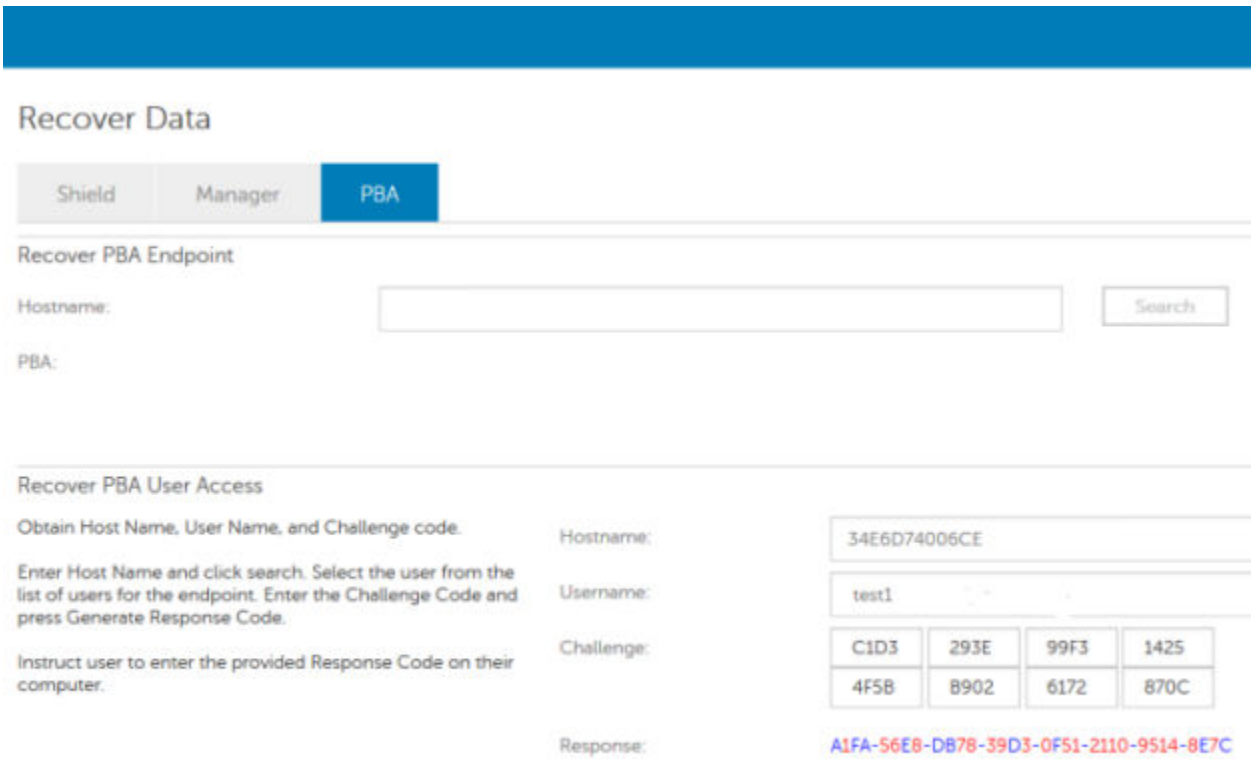
Aparece la siguiente información después de seleccionar **Respuesta de desafío**.



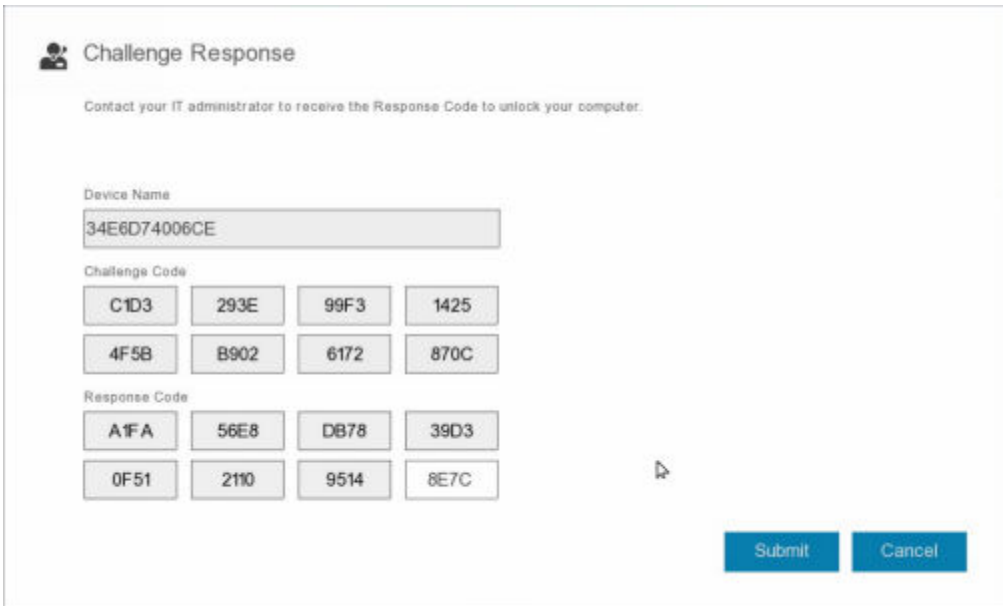
El campo **Nombre de dispositivo** se utiliza por los técnicos de la mesa de ayuda dentro de la consola de administración remota para encontrar el dispositivo correcto y, luego, seleccionar un nombre de usuario. Se encuentra dentro **Administración > Recuperar datos** en la pestaña **PBA**.



Se proporciona el Código de desafío al técnico de la mesa de ayuda, quién ingresa los datos y, luego, hace clic en el botón **Generar respuesta**.



Estos datos resultantes poseen colores a juego para ayudar a distinguir entre números (rojo) y caracteres alfabéticos (azul). Estos datos se leen al usuario final, quien los ingresa en el entorno PBA y, luego, hace clic en el botón **Enviar**, moviendo al usuario a Windows.



Después de realizar una autenticación exitosa, aparecerá el siguiente mensaje:

Recuperación de desafío finalizada.

7

Control de dispositivo PBA

El control de dispositivo PBA se aplica a los extremos cifrados con SED o cifrado de disco completo.

Usar Control de dispositivo PBA

Los comandos PBA de un extremo concreto se ejecutan en el área Control de dispositivo PBA. Cada comando tiene una clasificación de prioridad. Un comando con una prioridad mayor cancela los comandos de prioridades inferiores en la cola de aplicación. Para obtener una lista de clasificaciones de prioridad de comandos, consulte *AdminHelp* disponible haciendo clic en el signo de interrogación (?) en la consola de administración remota. Los controles de dispositivo PBA están disponibles en la página Detalles de extremo de la consola de administración remota.

Los siguientes comandos están disponibles en el control de dispositivo de PBA:

- **Bloquear**: bloquea la pantalla PBA y evita que cualquier usuario inicie sesión en el equipo.
- **Desbloquear**: desbloquea la pantalla PBA después de que haya sido bloqueada en este extremo, ya sea enviando un comando Bloqueo o sobrepasando la cantidad máxima de intentos de autenticación que la política permite.
- **Quitar usuarios**: esta opción elimina todos los usuarios de la PBA.
- **Omitir inicio de sesión**Omite la pantalla una vez para permitir un usuario en el equipo sin autentificar. El usuario todavía tendrá que iniciar sesión en Windows después de haber omitido PBA.
- **Borrar**: el comando Borrar funciona como una "restauración a estado de fábrica" para la unidad cifrada. El comando Borrar puede utilizarse para redirigir un equipo o, en una situación de emergencia, borrar el equipo, lo que provocará que los datos no puedan volver a recuperarse. Asegúrese de que este sea el comportamiento deseado antes de invocar este comando. Para un cifrado de disco completo, el comando Borrar elimina criptográficamente la unidad y remueve el PBA. Para SED, el comando Borrar elimina criptográficamente la unidad y el PBA muestra el mensaje "Dispositivo bloqueado". Para readaptar el SED, elimine el PBA con la aplicación Recuperación de SED.

8

Recuperación de la clave de propósito general

Se utiliza la Clave de propósito general (GPK) para cifrar una parte del registro para los usuarios de dominio. Sin embargo, raras veces, durante el proceso de inicio se vuelve inutilizable y no se puede abrir. Si ocurre esto, se muestran los siguientes errores en el archivo CMGShield.log en el equipo cliente:

```
[12.06.13 07:56:09:622 GeneralPurposeK: 268] GPK - Failure while unsealing data [error = 0xd]

[12.06.13 07:56:09:622 GeneralPurposeK: 631] GPK - Unseal failure

[12.06.13 07:56:09:622 GeneralPurposeK: 970] GPK - Failure to get keys for the registry driver
```

Si no se puede abrir la GPK, esta se debe recuperar. Para ello, extráigala del paquete de recuperación que se ha descargado de Dell Server.

Recuperar la GPK

Obtener el archivo de recuperación

Para descargar el archivo **<machinename_domain.com>.exe** que se generó al instalar Dell Data Security:

1 Abra la consola de administración remota y, desde el panel izquierdo, seleccione **Administración** > **Recuperar extremo**.

2 En el campo Nombre de host, ingrese el nombre de dominio completo del extremo y haga clic en **Buscar**.

3 En la ventana Recuperación, ingrese una Contraseña de recuperación y haga clic en **Descargar**.

> **NOTA:**
> Debe recordar esta contraseña para acceder a las claves de recuperación.

El archivo **<machinename_domain.com>.exe** se descarga.

Realizar una recuperación

1 Cree un medio de inicio del entorno de recuperación. Para obtener instrucciones, consulte Apéndice A - Grabar el entorno de recuperación.

> **NOTA: Desactive SecureBoot antes de comenzar el proceso de recuperación. Cuando haya terminado, active SecureBoot.**

2 Realice el inicio con dichos medios en un sistema de recuperación o en el dispositivo con la unidad que está intentando recuperar.
Se abre un entorno WinPE.

3 Ingrese **x** y pulse **Intro** para acceder al símbolo del sistema.

4 Vaya al archivo de recuperación e inícielo.
Se abre el cuadro de diálogo de diagnóstico del cliente Encryption y se genera el archivo de recuperación en segundo plano.

5 En el símbolo del sistema de administrador, ejecute **<machinename_domain.com** > **.exe** > **-p <password** > **-gpk**
Devuelve el archivo GPKRCVR.txt para su equipo.

6 Copie el archivo **GPKRCVR.txt** en la raíz de la unidad del sistema operativo del equipo.

7 Reinicie el equipo.
El sistema operativo consumirá el archivo GPKRCVR.txt y volverá a generar la GPK en ese equipo.
8 Si se le solicita, reinicie de nuevo.

9

Recuperación de BitLocker Manager

Para recuperar datos, obtenga una contraseña de recuperación o paquete de claves de la Remote Management Console, que le permitan desbloquear los datos en el equipo.

Recuperar datos

1 Inicie sesión como administrador de Dell en la Remote Management Console.

2 En el panel izquierdo, haga clic en **Management** > **Recover Data** (Administración > Recuperar datos).

3 Haga clic en la pestaña **Manager** (Administrador).

4 Para *BitLocker*:

Ingrese el **Recovery ID** (ID de recuperación) recibido de BitLocker. De manera opcional, si ingresa el Nombre de host y el Volumen, se completará la Id. de recuperación.

Haga clic en **Get Recovery Password** (Obtener contraseña de recuperación) o **Create Key Package** (Crear paquete de claves).

En función de la manera en que desee realizar la recuperación, utilizará la contraseña de recuperación o el paquete de claves para recuperar datos.

Para el *TPM*:

Ingrese el **Hostname** (Nombre de host).

Haga clic en **Get Recovery Password** (Obtener contraseña de recuperación) o **Create Key Package** (Crear paquete de claves).

En función de la manera en que desee realizar la recuperación, utilizará la contraseña de recuperación o el paquete de claves para recuperar datos.

5 Para completar la recuperación, consulte las Instrucciones de recuperación de Microsoft.

NOTA:

Si BitLocker Manager no es "propietario" de TPM, la contraseña y el paquete de claves de TPM no estarán disponibles en la base de datos de Dell. Recibirá un mensaje de error indicando que Dell no puede encontrar la clave, que es el comportamiento esperado.

Para recuperar un TPM "con propietario" de una entidad distinta de BitLocker Manager, deberá seguir el proceso de recuperación del TPM de ese propietario específico o seguir su propio proceso existente para la recuperación del TPM.

10

Recuperación de contraseña

Normalmente, los usuarios olvidan su contraseña. Afortunadamente, existen varios métodos para que los usuarios puedan volver a acceder a un equipo con autenticación previa al inicio cuando lo hagan.

- La función Recovery Questions (Preguntas de recuperación) ofrece autenticación basada en preguntas y respuestas.
- Los códigos de desafío/respuesta permiten a los usuarios trabajar con su administrador para volver a tener acceso a sus equipos. Esta función solo está disponible para usuarios con equipos administrados por su organización.

Preguntas de recuperación

La primera vez que un usuario inicia sesión en un equipo, se le solicita que responda a un conjunto estándar de preguntas que el administrador ha configurado. Después de inscribir sus respuestas a estas preguntas, la próxima vez que olvide su contraseña, se le solicitarán las respuestas. Suponiendo que responda correctamente a las preguntas, podrá iniciar sesión y volver a acceder a Windows.

Requisitos previos

- Las preguntas de recuperación debe configurarlas el administrador.
- El usuario debe haber inscrito sus respuestas a las preguntas.
- Antes de hacer clic en la opción de menú **Trouble Signing In** (Problema de inicio de sesión), el usuario debe ingresar un nombre de usuario y un dominio válidos.

Para acceder a las preguntas de recuperación desde la pantalla de inicio de sesión de PBA:

1 Ingrese un nombre de dominio y un nombre de usuario válidos.
2 En el lado inferior izquierdo de la pantalla, haga clic en **Options** > **Trouble Signing In** (Opciones > Problema de inicio de sesión).
3 Cuando aparezca el cuadro de diálogo Q&A (Preguntas y respuestas), ingrese las respuestas que proporcionó al inscribirse en las preguntas de recuperación por primera vez.

11

Recuperación de la contraseña de Medios externos de cifrado

Medios externos de cifrado le ofrece la capacidad de proteger los medios de almacenamiento extraíbles dentro y fuera de la organización, lo que permite a los usuarios cifrar flash drives USB y otros medios de almacenamiento extraíbles. El usuario asigna una contraseña a cada medio extraíble que desea proteger. Esta sección describe el proceso de recuperación del acceso a un dispositivo de almacenamiento USB cifrado cuando un usuario olvida la contraseña de un dispositivo.

Recuperar el acceso a los datos

Cuando un usuario escribe de forma incorrecta su contraseña tantas veces que se supera el número permitido de intentos de contraseña, el dispositivo USB entra en modo de autenticación manual.

Autenticación manual es un proceso que consiste en proporcionar códigos del cliente a un administrador que ha iniciado sesión en Dell Server.

En modo de autenticación manual, el usuario tiene dos opciones para restablecer su contraseña y recuperar el acceso a sus datos.

El administrador proporciona un código de acceso al cliente, que permite al usuario restablecer su contraseña y recuperar el acceso a sus datos cifrados.

1 Cuando se le solicite su contraseña, haga clic en el botón **I Forgot** (La he olvidado).

Se abrirá el cuadro de diálogo de confirmación.

2 Haga clic en **Sí** para confirmar. Después de la confirmación, el dispositivo entra en modo de autenticación manual.

3 Póngase en contacto con el administrador del departamento de soporte técnico y proporciónele los códigos que aparecen en el cuadro de diálogo.

4 Como administrador del departamento de soporte técnico, inicie sesión en la Remote Management Console. La cuenta del administrador del departamento de soporte técnico debe tener los privilegios correspondientes.

5 Vaya a la opción de menú **Recover Data** (Recuperar datos) en el panel izquierdo.

6 Ingrese los códigos proporcionados por el usuario final.

7 Haga clic en el botón **Generate Response** (Generar respuesta) en la esquina inferior izquierda de la pantalla.

8 Proporcione al usuario el código de acceso.

NOTA:

Asegúrese de autenticar manualmente al usuario antes de proporcionarle el código de acceso. Por ejemplo, plantee al usuario una serie de preguntas por teléfono que solo sabría él, como: "¿cuál es su número de ID de empleado?". Otro ejemplo: solicite al usuario que vaya al departamento de soporte técnico para que proporcione una identificación que garantice que es el propietario del medio. Si no se autentica a un usuario antes de proporcionarle un código de acceso por teléfono, un atacante podría obtener acceso al medio extraíble cifrado.

9 Restablezca su contraseña para el medio cifrado.

Se solicitará al usuario que restablezca su contraseña para el medio cifrado.

Recuperación automática

La unidad debe insertarse nuevamente en la máquina que originalmente realizó su cifrado para que la autorecuperación funcione. Siempre que el propietario del medio se autentique en el Mac o PC protegido, el cliente detecta la pérdida del material de claves y solicita al usuario que vuelva a iniciar el dispositivo. En ese momento, el usuario puede restablecer su contraseña y volver a acceder a sus datos cifrados. Este proceso puede resolver problemas con medios parcialmente dañados.

1 Inicie sesión en una estación de trabajo cifrada con Dell Data Security como propietario del medio.
2 Ingrese el dispositivo de almacenamiento extraíble cifrado.
3 Cuando se le solicite, ingrese una nueva contraseña para volver a iniciar el dispositivo de almacenamiento extraíble.

   Si se realiza correctamente, aparece una pequeña notificación para indicar que se ha aceptado.

4 Navegue al dispositivo de almacenamiento y confirme el acceso a los datos.

Recuperación de Dell Data Guardian

La herramienta de recuperación permite:

- El descifrado de lo siguiente:
  - Archivos documentos de Office protegidos con cualquier formato compatible: se pueden recuperar archivos que estén protegidos por el cifrado de documentos de Office protegidos de Data Guardian y su protección de proveedor de servicios en la nube.
  - Formatos de archivos indicados en la política de protección básica de archivos, si se permite.
- Custodia manual de material de claves
- Capacidad para comprobar archivos manipulados
- Capacidad para forzar el descifrado de documentos de Office protegidos en los que alguien ha manipulado el contenedor del archivo, por ejemplo, la portada del archivo de Office protegido en la nube o en un dispositivo que no cuenta con Data Guardian

NOTA:
Puede utilizar Windows Recovery Tool con archivos creados en Mac, dispositivos móviles o plataformas de portal web.

Requisitos previos

Los requisitos previos incluyen:

- Microsoft .NET Framework 4.5.2 en ejecución en el extremo que se va a recuperar.
- El rol de administrador forense se debe asignar en la consola de administración al administrador que lleve a cabo la recuperación.

Realizar recuperación de Data Guardian

Siga estos pasos para realizar la recuperación de documentos de Office protegidos con Data Guardian. Puede recuperar solo una computadora a la vez.

IMPORTANTE:
Para evitar pérdidas de contenido en caso de daños, descifre las copias de los archivos y no las versiones originales.

Realizar una recuperación desde Windows, una unidad flash USB o una unidad de red

Para realizar una recuperación:

1 Desde el medio de instalación de Dell, copie **RecoveryTools.exe** en una de estas ubicaciones:

- Equipo: copie el archivo .exe en el equipo en el que se van a recuperar los documentos de Office.
- USB: copie el archivo .exe en la unidad flash USB y ejecútelo desde esta.
- Unidad de red

IMPORTANTE:
Como administrador, asegúrese de copiar solo el archivo ejecutable **RecoveryTools.exe** y no el instalador. **RecoveryTools.exe** tiene un mejor rendimiento si no se está ejecutando un barrido o descifrado.

2 Haga doble clic en **RecoveryTools.exe** para iniciar la herramienta de recuperación.

3 En la ventana Herramienta de recuperación de Data Guardian, seleccione **Inicio de sesión en el dominio**.

> **NOTA:**
> La opción de inicio de sesión de SaaS para brindar una solución alojada estará disponible en una versión futura.

4 Ingrese el FQDN del Dell Server en el siguiente formato:
servidor.dominio.com

> **NOTA:**
> Se agrega automáticamente un prefijo y un sufijo a la FQDN.

5 Ingrese su nombre de usuario y su contraseña y haga clic en **Iniciar sesión**.

> **NOTA:**
> No desmarque la casilla *Activar confianza en SSL* a menos que lo indique el administrador.

> **NOTA:**
> Si no es administrador forense e ingresa las credenciales, se mostrará un mensaje que indica que no tiene derechos de inicio de sesión.

6 Si es administrador forense, se abrirá la herramienta de recuperación.

7 Seleccione **Origen**.

> **NOTA:**
> Debe navegar a un origen y un destino, aunque puede seleccionarlos en cualquier orden.

8 Haga clic en **Examinar** para seleccionar la carpeta o unidad que se va a recuperar.

9 Haga clic en **Aceptar**.

10 Haga clic en **Destino**, una carpeta vacía para los archivos descifrados o recuperados.

11 Haga clic en **Examinar** para seleccionar un destino; por ejemplo, un dispositivo externo, la ubicación de un directorio o el escritorio.

12 Haga clic en **Aceptar**.

13 Seleccione una o más casillas en función de lo que desee recuperar.

Opciones	Descripción
Custodia	• Recupere las claves generadas sin conexión que no se pudieron custodiar en el servidor de Dell. • Si una unidad de disco duro falla mientras el usuario está desconectado de la red, utilice la unidad secundaria para recuperar los datos y las claves no custodiadas del equipo.
Descifrar	Navegue con la herramienta de recuperación a un directorio que contenga los documentos de Office protegidos para descifrarlos. **NOTA:** Como práctica recomendada, descifre copias de los archivos, no los originales, en caso de daños. De manera opcional, si se ha producido manipulación, seleccione una de estas opciones o las dos (consulte más abajo para obtener información): • **Comprobación de manipulación**: comprueba los archivos manipulados, pero no los descifra.

Opciones	Descripción
	• **Comprobación de manipulación** y **Forzar descifrado incluso si está manipulado**: comprueba si hay archivos manipulados y, si el contenedor de un documento de Office protegido se ha manipulado, Data Guardian repara el contenedor y descifra el documento de Office.
Comprobación de manipulación	Detecta los archivos que se han manipulado, los registra y se lo notifica. Registra el autor de la manipulación del archivo. No descifra los archivos.
Forzar descifrado incluso si está manipulado	Para seleccionar esta opción, debe también seleccionar **Comprobación de manipulación**. Si una persona autorizada ha manipulado el contenedor de un documento de Office protegido, como la portada, ya sea en la nube o en un dispositivo que no cuenta con Data Guardian, seleccione esta opción para reparar el contenedor y forzar el descifrado del archivo de Office protegido. **NOTA:** Si alguien ha manipulado el archivo .xen de Office cifrado dentro del contenedor, el archivo no se podrá recuperar.

Cada archivo de Office protegido tiene una marca de agua oculta que contiene el historial del usuario original y el nombre de equipo, y cualquier otro nombre de equipo que haya modificado el archivo. De manera predeterminada, la herramienta de recuperación comprueba las marcas de agua ocultas y agrega un archivo de texto con una lista de todos los autores a una carpeta *HiddenWatermark* en los registros.

14 Una vez que se hayan completado las selecciones, haga clic en **Explorar**.

El área de registro muestra:

- Las carpetas encontradas y exploradas dentro del origen seleccionado
- Si el descifrado, por archivo, se ha realizado correctamente o no
- El nombre del último autor de un archivo

La herramienta de recuperación añade los archivos recuperados al destino seleccionado. Puede abrir y ver los archivos.

Ver datos desde rastro oculto de auditoría

En el caso de Windows, si la política de Rastro oculto de auditoría para documentos protegidos de Office está activada, la información del usuario se captura en los metadatos de archivos. Para ver estos datos, utilice la herramienta de recuperación:

1 Inicie la herramienta de recuperación.
   - Para ver el **origen**, vaya a una carpeta que contenga documentos protegidos de Office con datos ocultos de auditoría. La herramienta de recuperación copia la estructura de carpetas y subcarpetas para descifrar cualquier documento protegido de Office que tenga datos ocultos de auditoría.
   - Antes de ir a un **destino**, puede crear una carpeta llamada Archivos descifrados y, luego, ir hasta ella.
2 Seleccione **Descifrar**.
3 Una vez que se hayan completado las selecciones, haga clic en **Explorar**.

   La carpeta seleccionada como destino contiene una carpeta *Archivos recuperados* con fecha, la cual contiene lo siguiente:
   - Archivos Office protegidos y descifrados
   - Carpeta *Rastro de auditoría*, creada por la herramienta de recuperación, con un archivo .txt para cada archivo descifrado. Cada archivo .txt tiene un registro que muestra información del archivo descifrado, como los autores, el último autor o marcas de tiempo.

Apéndice A - Grabar el entorno de recuperación

Puede descargar Master Installer.

Grabar la ISO del entorno de recuperación en CD/DVD

El siguiente enlace contiene el proceso necesario para utilizar Microsoft Windows 7, Windows 8 o Windows 10 para crear un CD o DVD de arranque para el entorno de recuperación.

http://windows.microsoft.com/en-us/windows7/burn-a-cd-or-dvd-from-an-iso-file

Grabar el entorno de recuperación en un medio extraíble

Para crear una unidad USB de arranque, siga las instrucciones a continuación:

Inicio heredado:

1 Conecte una unidad USB al sistema.
2 Abra un símbolo del sistema como administrador.
3 Para ingresar la utilidad Diskpart, escriba **diskpart**.
4 Encuentre el disco de destino que desea modificar; para ello, escriba **enumerar discos**. Los discos se designarán por número.
5 Seleccione el disco apropiado mediante el comando **seleccionar disco #** donde # es el número de disco que corresponde a la unidad indicada por el paso anterior.
6 Para limpiar el disco, emita un comando **limpiar**. Esto purgará los datos de la unidad limpiando la tabla de archivos.
7 Cree una partición para almacenar la imagen de inicio.
   a El comando **crear partición principal** genera una partición principal en la unidad.
   b El comando **seleccionar partición 1** selecciona la partición nueva.
   c Utilice el siguiente comando para realizar un formateo rápido de la unidad con el sistema de archivos NTFS: **formatear FS=NTFS rápido**.
8 La unidad debe estar marcada como unidad de arranque. Utilice el comando **activo** para marcar la unidad como unidad de arranque.
9 Para mover los archivos directamente a la unidad, asigne una letra disponible a la unidad con el comando **asignar**.
10 La unidad se montará automáticamente y los contenidos del archivo ISO se pueden copiar en la raíz de la unidad.

Después de que los contenidos del ISO se hayan copiado completamente, la unidad se volverá una unidad de arranque y se puede utilizar para la recuperación.

Arranque EUFI:

1 Conecte una unidad USB al sistema.
2 Abra un símbolo del sistema como administrador.
3 Para ingresar la utilidad Diskpart, escriba **diskpart**.
4 Encuentre el disco de destino que desea modificar; para ello, escriba **enumerar discos**. Los discos se designarán por número.
5 Seleccione el disco apropiado mediante el comando **seleccionar disco #** donde # es el número de disco que corresponde a la unidad indicada por el paso anterior.

6 Para limpiar el disco, emita un comando **limpiar**. Esto purgará los datos de la unidad limpiando la tabla de archivos.

7 Cree una partición para almacenar la imagen de inicio.

   a El comando **crear partición principal** genera una partición principal en la unidad.

   b El comando **seleccionar partición 1** selecciona la partición nueva.

   c Utilice el siguiente comando para realizar un formateo rápido de la unidad con el sistema de archivos FAT32: **formatear FS=FAT32 rápido**.

8 La unidad debe estar marcada como unidad de arranque. Utilice el comando **activo** para marcar la unidad como unidad de arranque.

9 Para mover los archivos directamente a la unidad, asigne una letra disponible a la unidad con el comando **asignar**.

10 La unidad se montará automáticamente y los contenidos del archivo ISO se pueden copiar en la raíz de la unidad.

Después de que los contenidos del ISO se hayan copiado completamente, la unidad se volverá una unidad de arranque y se puede utilizar para la recuperación.