Chameleon

Manual del usuario del dispositivo Basic.

powered by

LucidPORT

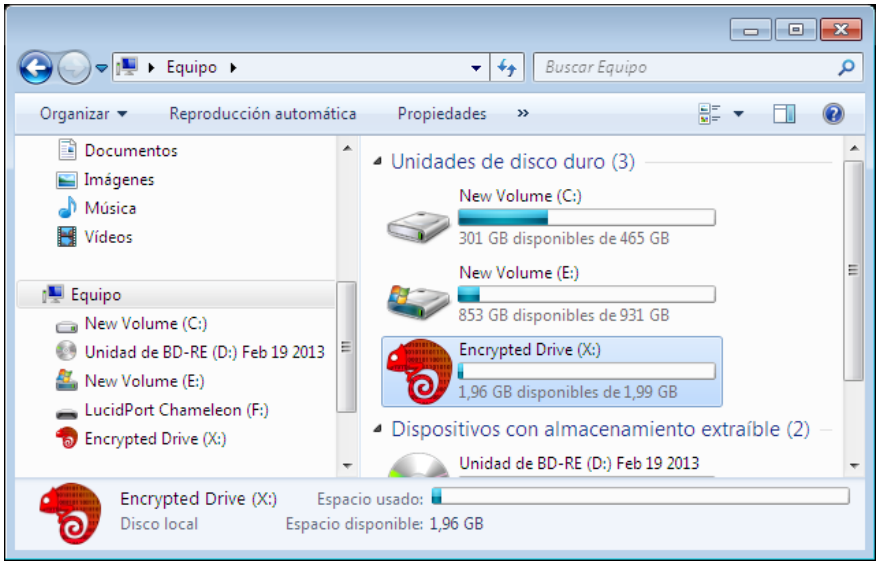
Tabla de contenidos

1 Introducción 2
2 Instalación y configuración 2
2.1 Desinstalación 5
3 Unidades Chameleon encriptadas: Protección de los datos 5
4 Cifrado de archivos y carpetas individuales 8
4.1 Encriptar archivos y carpetas individuales 8
4.2 Desencriptado de archivos 11
4.3 Ver los detalles de los archivos encriptados 14
5 Duplicación de un dispositivo Chameleon 15
6 Desactivación de dispositivos perdidos Chameleon 16
6.1 Migración de archivos encriptados (.cge) 18
7 Protección por contraseña 19
7.1 Cambio de contraseña 19
8 Cómo agregar, eliminar, cambiar el tamaño y las unidades encriptadas 21
9 Funciones y Limitaciones Adicionales 22
9.1 Utilización de un dispositivo Chameleon con varios equipos 22
9.2 Utilización de varios dispositivos con el mismo equipo 23
9.3 Archivo de paginación de Windows 23
9.4 Extracción segura 24
9.5 Copia de seguridad de datos 25
10 Limited Warranty and Legal Notices 25

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

1 Introducción

Chameleon protege los archivos en su PC con una encriptación AES-256. Chameleon se diferencia de los otros dispositivos de encriptación USB por la protección de los archivos en el disco duro en lugar de transferirlos a un dispositivo USB. Chameleon crea una unidad encriptada usando un espacio libre en su disco duro. Los archivos y las aplicaciones almacenados en esta unidad encriptada están protegidos y solo se puede acceder a ellos cuando el dispositivo Chameleon está enchufado. Al igual que la llave de su coche, el dispositivo Chameleon actúa como una llave física para el disco duro.



Chameleon funciona con PCs basados en Windows XP, Vista y Windows7.

2 Instalación y configuración

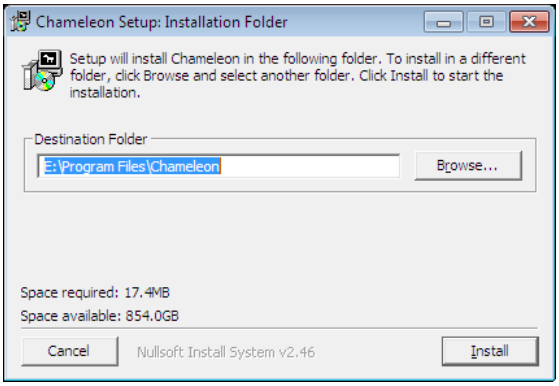
1. Antes de instalar el software Chameleon, asegúrese de que todas las versiones anteriores del software Chameleon han sido desinstaladas. La desinstalación no elimina las actuales unidades encriptadas.

2. **Inserte el CD de instalación y ejecute el programa de instalación**.[1] (También puede descargar el programa de instalación desde http://www.marathon6.com/chameleon.)

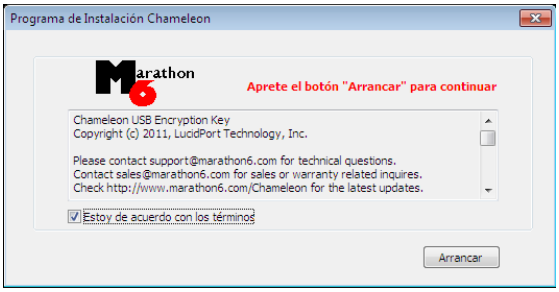
[1] En algunos equipos Windows7, se puede abrir una ventana de control con la advertencia de que un programa está tratando de hacer cambios en el equipo. Seleccione "Sí" o "Instalar" si esto ocurre.

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

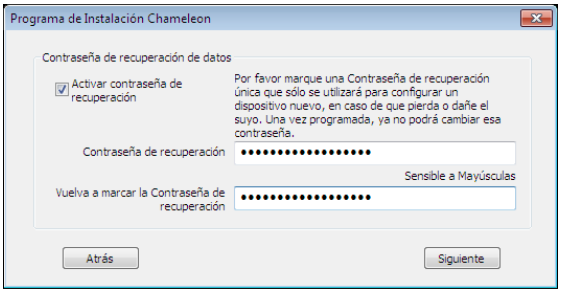
3. **Haga clic en el botón "Install"** para cargar el software.



4. **Inserte el dispositivo Chameleon** y **presionar "Arrancer"** para iniciar el asistente de instalación.



5. **Elija entre A), B), o C)**



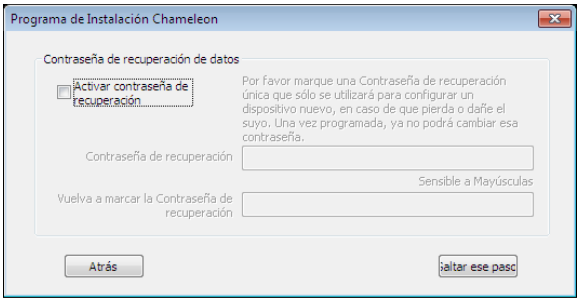
A) Elija una frase de contraseña de recuperación. Esta contraseña sólo se utiliza para realizar duplicados de su dispositivo Chameleon (en caso de que lo pierda) y no es necesaria durante el funcionamiento normal. Usted puede pensar en la contraseña de recuperación como a una contraseña almacenada en el propio dispositivo.

Seleccione una contraseña de recuperación única. Otro dispositivo Chameleon con la misma frase de contraseña de recuperación puede acceder a sus datos. Una vez programada, la frase de contraseña de recuperación no se puede cambiar.

Una buena contraseña contiene al menos 16 caracteres e incluye letras al azar (mayúsculas y minúsculas), números y símbolos especiales. Proteja su frase de contraseña de recuperación como protegería una contraseña. Un atacante que descubre su contraseña podría utilizarla para crear un duplicado de su dispositivo. No se puede duplicar un dispositivo Chameleon sin su frase de contraseña de recuperación.

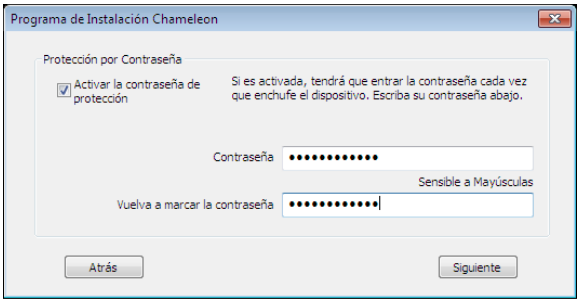
B) Para un mejor equilibrio entre seguridad y redundancia, utilice una secuencia aleatoria de al menos 64 números y letras como frase de contraseña de recuperación. Después de completar la instalación, crea varios dispositivos duplicados con esta secuencia como copias de seguridad (ver "*5 Duplicación de un dispositivo Chameleon*"). Para poder crear duplicados adicionales en el futuro, guardar la secuencia aleatoria en una ubicación segura. Si no, borra la secuencia.

C) Desactivar la recuperación de contraseña. Para una mayor seguridad, desactive la recuperación de contraseña. Esto indicará al dispositivo Chameleon de generar su propia clave de criptación aleatoria. Sin embargo, esto significa que usted no podrá duplicar el dispositivo si se pierde o se rompe.



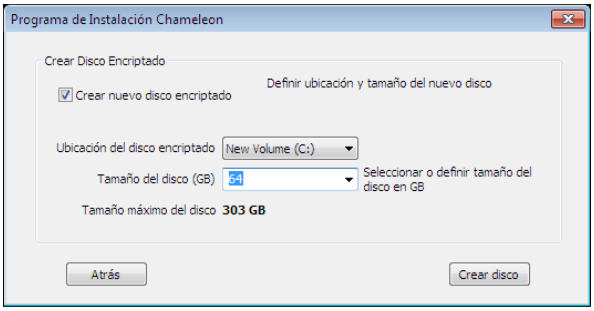
6. **Activar / Desactivar contraseña**. Cuando está activada, la contraseña debe introducirse cada vez que se conecta el dispositivo. Una contraseña no es obligatoria y puede ser agregada o cambiada en cualquier momento.

   Si está activada, la contraseña debe ser diferente de la contraseña de recuperación. Una contraseña protege el dispositivo Chameleon del uso no autorizado.



485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

7. **Crear una unidad encriptada**.
   Especificar el tamaño y la ubicación de la unidad. El instalador crea la unidad encriptada utilizando el espacio libre en esa ubicación. Puede residir en el disco duro local o en unidades USB externas. La unidad encriptada podrá cambiar de tamaño más adelante.



Todo el contenido copiado en la unidad encriptada está protegido automáticamente. Está accesible cuando el dispositivo se inserta, y desaparece cuando se retira el dispositivo.

2.1 Desinstalación

Puede desinstalar el software Chameleon, eligiendo "Chameleon" en el menú de inicio de Windows y seleccionando la opción "desinstalar" (Inicio> Todos los programas> Chameleon> Desinstalar). La desinstalación no borra sus unidades encriptadas. Para borrar las unidades encriptadas, elimine los directorios Chameleon del directorio de su disco duro al nivel superior (por ejemplo, C: \ Unidades Chameleon \). El directorio Chameleon sólo se puede eliminar cuando el dispositivo no está conectado.

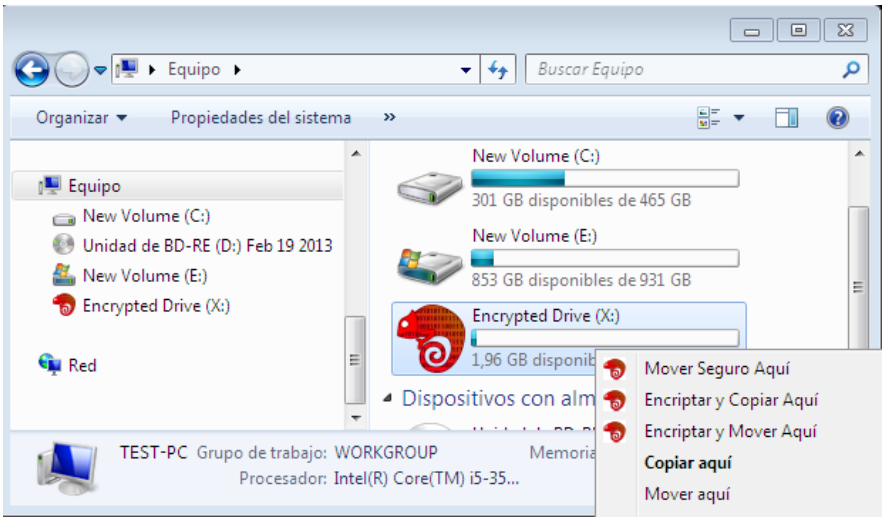
3 Unidades Chameleon encriptadas: Protección de los datos

Conecte su dispositivo para acceder a la unidad Chameleon encriptada. La unidad encriptada aparece como cualquier otra unidad en su sistema. Puede almacenar archivos en ella, abrir sus archivos, instalar y ejecutar programas, mover archivos de un directorio a otro, y administrar las aplicaciones desde la unidad encriptada. Una vez que el dispositivo Chameleon se retira, la unidad encriptada desaparece de Windows. Un examen forense de su disco duro revelará solamente datos encriptados, aparentemente al azar.

Sólo los archivos que se almacenan en esta unidad Chameleon están encriptados. Los archivos copiados o abiertos desde la unidad encriptada se descodifican automáticamente. Por ejemplo, si un usuario quiere adjuntar un archivo de una unidad encriptada a un correo electrónico, se adjunta un archivo desencriptado. Para la fijación de los archivos adjuntos de correo electrónico y almacenamiento en la nube (cloud), consulte la sección “4 `Cifrado de archivos y carpetas individuales`”.

Puede copiar los archivos a la unidad encriptada simplemente arrastrandos y soltándolos allí. Sin embargo, se conserva el archivo original sin encriptarlo en su ubicación original. Un método más seguro es hacer un clic derecho, arrastrar y soltar. Mantenga pulsado el botón derecho del ratón y

arrastre el archivo seleccionado a la unidad encriptada. Aparece un diálogo que muestra "Copiar", "Mover", y "Mover Seguro Aqui". La opción de mover seguro mueve el archivo a la unidad encriptada, y borra cualquier resto de ese archivo de su ubicación original.[2] Si se trata de una cantidad significativa de datos, esto puede tomar algún tiempo.

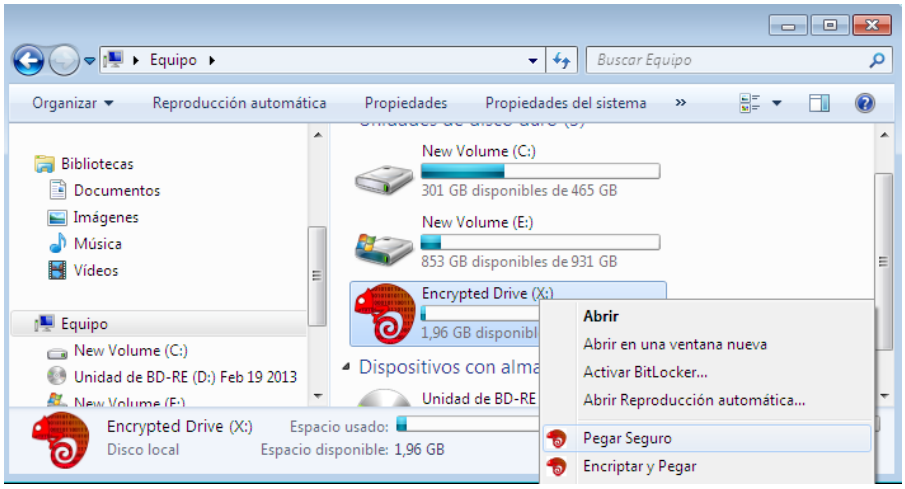


También puede mover con seguridad un archivo a la unidad encriptada mediante el uso de la opción de pegado seguro. Haga clic derecho sobre el archivo o carpeta que desea mover y, a continuación, seleccione "Cortar". Después, haga clic en la unidad encriptada o uno de sus sub-directorios, y seleccione "Pegar Seguro". Al igual que la opción de mover seguro, la opción pegar seguro borra todo rastro de los archivos encriptados del disco duro.

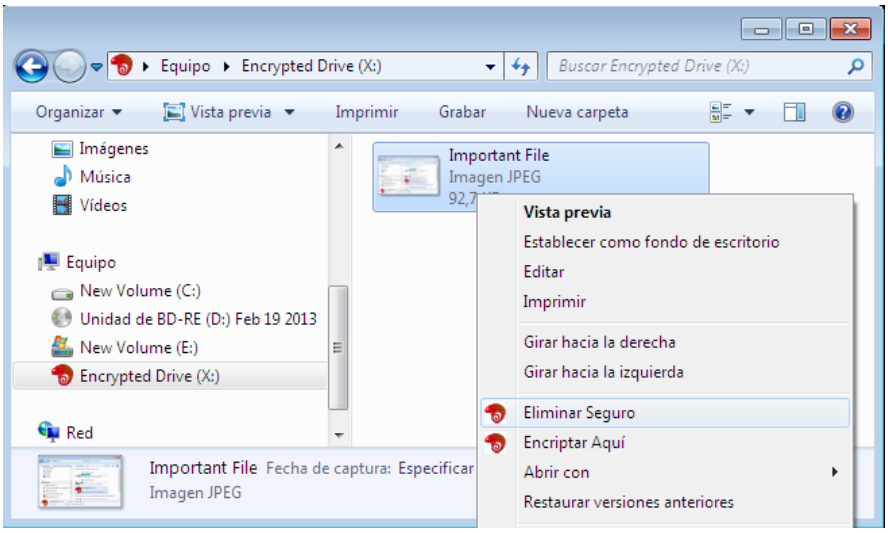
Los comandos seguros sólo están disponibles cuando el dispositivo Chameleon está enchufado.

[2] La función estándar de Windows “mover” copia el archivo, y marca a continuación el archivo original como borrado. El archivo borrado se puede recuperar con herramientas especiales. La opción de mover seguro impide una recuperación al sobrescribir el archivo borrado.

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com



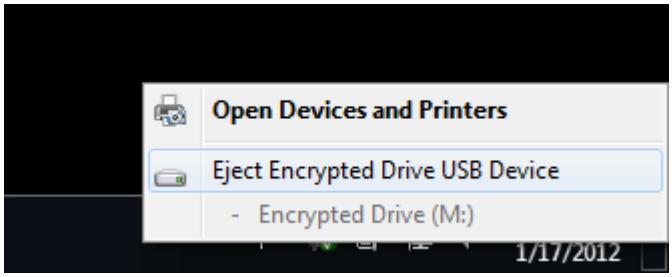
El software Chameleon también añade una función de borrado seguro. Haga clic derecho sobre cualquier archivo o carpeta y seleccione "Eliminar Seguro". Es más seguro que borrar el archivo y luego borrarlo de nuevo desde la papelera de reciclaje de Windows. Borrar seguro sobrescribe todos los bits del archivo del disco duro, esto puede tomar algún tiempo si se trata de una cantidad significativa de datos. Las funciones normales de cortar, pegar y borrar de Windows aún están disponibles.



Borrar un archivo almacenado en una unidad encriptada, lo coloca en la Papelera de reciclaje de Windows. Usted puede recuperar el archivo desde esta papelera de reciclaje, siempre y cuando el dispositivo Chameleon está conectado. Los archivos borrados desaparecerán de la papelera de reciclaje cuando se retira el dispositivo. Reaparecen en la papelera de reciclaje cuando el dispositivo se vuelve a insertar. No es necesario borrar los archivos ubicados en la unidad encriptada.

Los archivos creados directamente en la unidad encriptada se protegen automáticamente. Sin embargo, algunas aplicaciones almacenan la información temporal en el disco sin encriptar. Esta información puede ser recuperable con herramientas especializadas. Usted debe configurar sus aplicaciones para que almacenen sus archivos temporales en la unidad encriptada. Esto se puede lograr mediante la instalación de aplicaciones directamente en la unidad encriptada.

Puede conectar o desconectar el dispositivo Chameleon en cualquier momento. Su equipo sigue siendo plenamente funcional sin el dispositivo Chameleon. Sólo la unidad encriptada (y todos los programas y datos en la misma) no estarán disponibles. Tenga en cuenta que desconectar el dispositivo mientras escribe datos en la unidad encriptada puede dañar esos datos. Es similar a sacar un disco duro externo mientras se utiliza. Para estar absolutamente seguro de que no se está produciendo, utilice la función Quitar seguro de Windows antes de desenchufar el dispositivo.



Si se abre una aplicación con un archivo encriptado, la aplicación y el archivo puede aún ser accesible incluso después de desconectar el dispositivo Chameleon. Por ejemplo, digamos que usted está editando un archivo protegido en Microsoft Word. Si desconecta el dispositivo, una copia de este archivo está abierta en Word. No se puede guardar el archivo en la unidad encriptada hasta que vuelva a insertar el dispositivo. Sin embargo, usted todavía puede ver y editar las partes del archivo en caché en la memoria de trabajo.

4 Cifrado de archivos y carpetas individuales

El dispositivo Chameleon encripta automáticamente todos los datos que se colocan en la unidad encriptada y desencripta automáticamente todos los datos tomados de la unidad encriptada. Aunque práctico y seguro, esto no protege la información que usted manda por correo electrónico o almacena en la red. Para estas situaciones, el dispositivo Chameleon puede encriptar y descriptar archivos y carpetas individuales.

4.1 Encriptar archivos y carpetas individuales

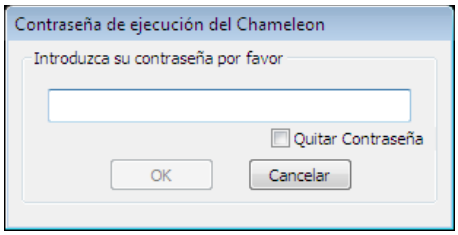
Puede encriptar un archivo, un grupo de archivos o directorios enteros (pero no los accesos directos o iconos especiales como la Papelera de reciclaje de Windows). Los archivos

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

encriptados por un dispositivo Chameleon sólo puede ser desencriptados utilizando el mismo dispositivo (o por TIC Master).

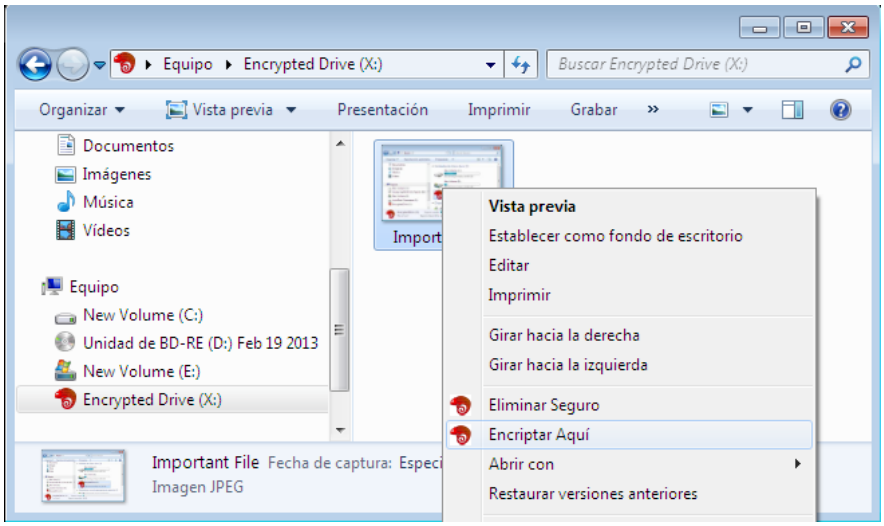
1. **Conecte el dispositivo**

2. **Introduzca su contraseña (si está activada)**



3. **Haga clic derecho sobre el archivo** o la carpeta que desea proteger.

4. **Seleccione "Encriptar Aquí"** para crear la versión encriptada del archivo seleccionado

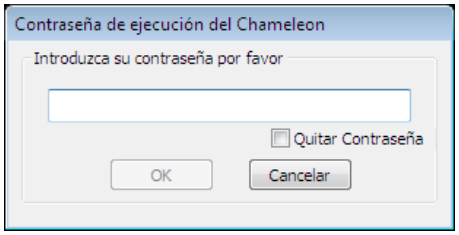


El archivo encriptado aparece como un archivo en la misma carpeta con el mismo nombre de archivo pero con la extensión ".cge". Si lo desea, puede cambiar el nombre del archivo, pero no la extensión. Este archivo se encripta mediante el hardware AES-256 del dispositivo. A la diferencia de la unidad encriptada, el archivo encriptado es todavía visible cuando se retira el dispositivo. Se puede adjuntar a un correo electrónico, copiar a una unidad de disco USB, almacenar en la red, o sincronizar con un servicio en la nube (cloud).

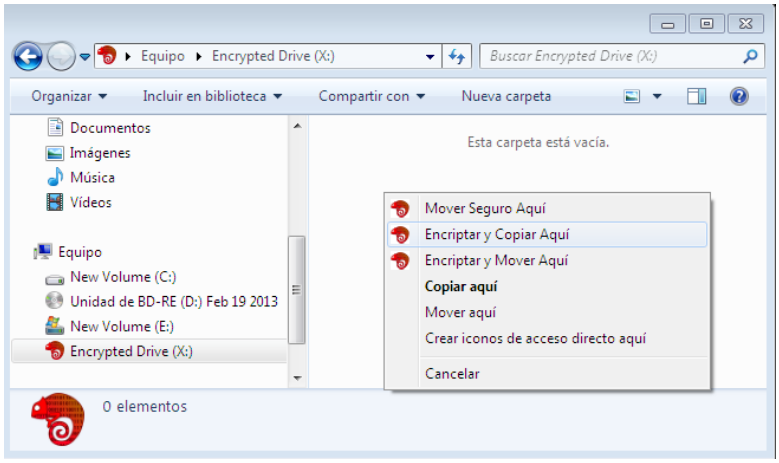
Puede encriptar archivos y carpetas individuales también con un simple arrastrar y soltar el botón derecho.

1. **Conecte el dispositivo**

2. **Introduzca su contraseña (si está activada)**



3. **Haz clic y mantén pulsado el botón derecho del ratón sobre el archivo** o la carpeta que desea proteger.
4. **Arrastre el puntero del ratón** la carpeta de destino y suelte el botón derecho del ratón. El archivo encriptado se creará en esta carpeta.



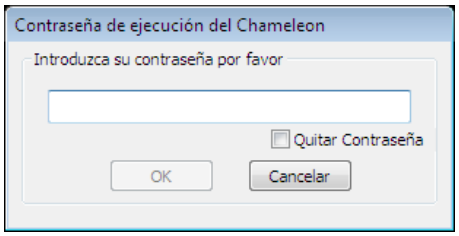
5. **Seleccione "Encriptar y Mover Aquí" o "Encriptar y Copia Aquí"**.
" Encriptar mover aquí " coloca el archivo encriptado a su destino mientras borra seguro el archivo de origen.

"Encriptar y Copia Aquí" hace lo mismo sin borrar el archivo de origen.

Puede encriptar un archivo o una carpeta también mediante la opción de pegado:

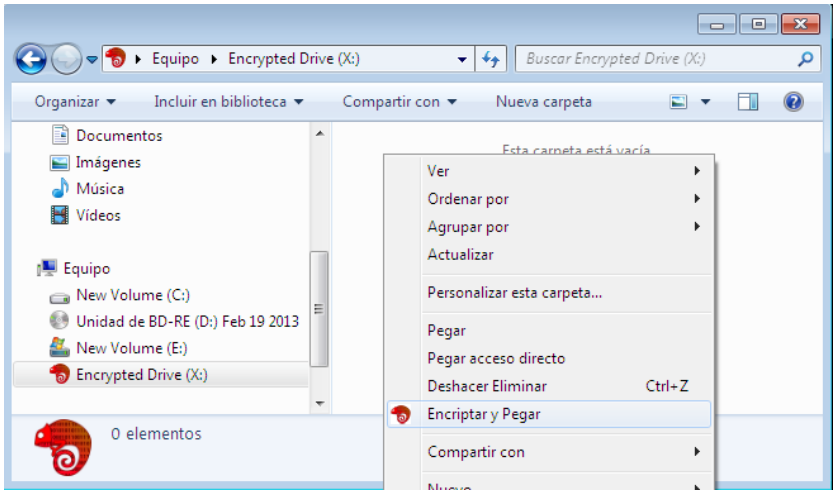
1. **Conecte el dispositivo**

2. **Introduzca su contraseña (si está activada)**



3. **Haga clic derecho sobre el archivo** o la carpeta que desee encriptar, a continuación, seleccione "Cortar" o "Copiar". Usted puede utilizar también los shorcuts (atajos de teclado) Cortar (Ctrl + X) o Copiar (CTRL + C).

4. **Haga clic en la unidad o directorio de destino.**



5. **Seleccione "Encriptado y Pegar "**

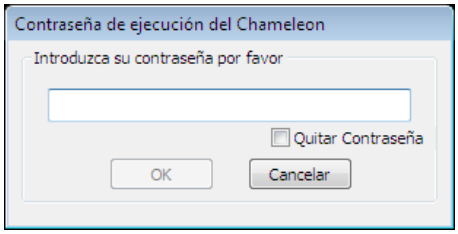
Esto coloca el archivo encriptado en el destino. Si selecciona "Cortar", el archivo de origen será borrado con seguridad después de la encriptación.

4.2 Desencriptado de archivos

Para descriptar un archivo cge:

1. **Conecte el dispositivo**

2. **Introduzca su contraseña (si está activada)**



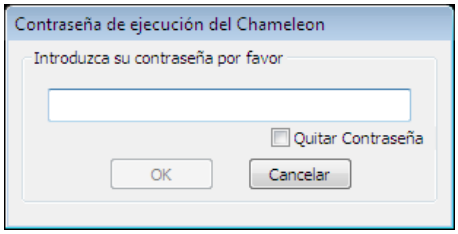
3. **Haga doble clic en el archivo .cge**.
   El proceso de desencriptación se iniciará inmediatamente.

Nota: Si abre el archivo.cge de una aplicación (por ejemplo, un navegador web) utilizando (por ejemplo) "Abrir con", el archivo se descargará y se descriptará en una carpeta temporal elegida por la aplicación. Esto posicionará el contenido descriptado del archivo .cge en una carpeta de archivos no deseada. En lugar de abrir el archivo .cge directamente desde la aplicación, guarde el archivo .cge en una carpeta de su elección (la opción "Guardar Como"), y luego descripta el archivo.

Los otros métodos para descriptar los archivos .cge son idénticos a los para encriptar:

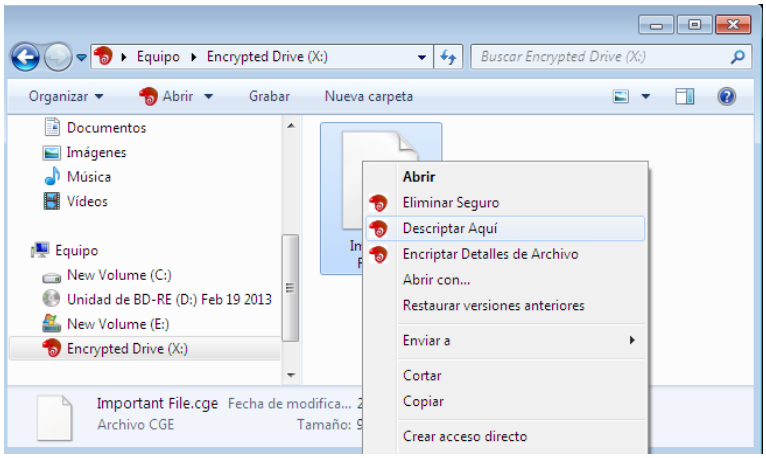
1. **Conecte el dispositivo**

2. **Introduzca su contraseña (si está activada)**



3. **Haga clic derecho sobre el archivo .cge** a descriptar.

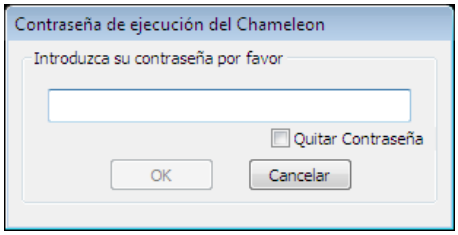
4. **Seleccione "Descriptar Aquí"** para crear una copia del archivo o de la carpeta descriptado contenido dentro del archivo .cge



Del mismo modo, puede descriptar los archivos .cge utilizando el método del clic derecho arrastrar / soltar. Utilice este método cuando el archivo .cge se encuentra en un almacenamiento no encriptado. Es más seguro porque evita que sus datos no encriptados residan (temporalmente) en el almacenamiento sin protección. Por ejemplo, usted puede tener un archivo .cge guardado en una unidad de red. En vez de hacer doble clic en el archivo para descriptarlo en la carpeta de red, puede utilizar el siguiente método para descriptar el archivo en su disco duro local.

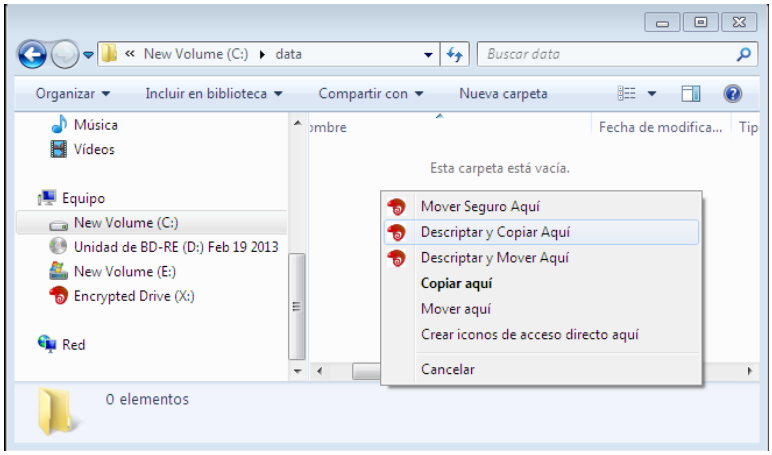
1. **Conecte el dispositivo**

2. **Introduzca su contraseña (si está activada)**



3. **Haz clic y mantén pulsado el botón derecho del ratón sobre el archivo .cge**.

4. **Arrastre el puntero del ratón** a la carpeta de destino y suelte el botón derecho del ratón. El contenido descriptado será creado en esta carpeta.



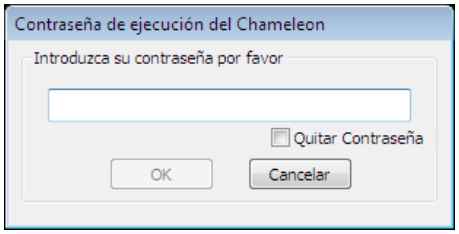
5. **Seleccione "Descriptar y Mover Aquí" o " Descriptar y Copiar Aquí"**.
" Descriptar y Mover Aquí " coloca el contenido descriptado a su destino con seguridad mientras borra el archivo .cge. Utilizará este método para evitar que sus datos no encriptados se queden (temporalmente) en un almacenamiento remoto o sin garantía.

   "Descriptar y Copiar Aquí" hace lo mismo sin borrar el archivo de origen.

La opción Pegar Descriptar está también disponible:

1. **Conecte el dispositivo**

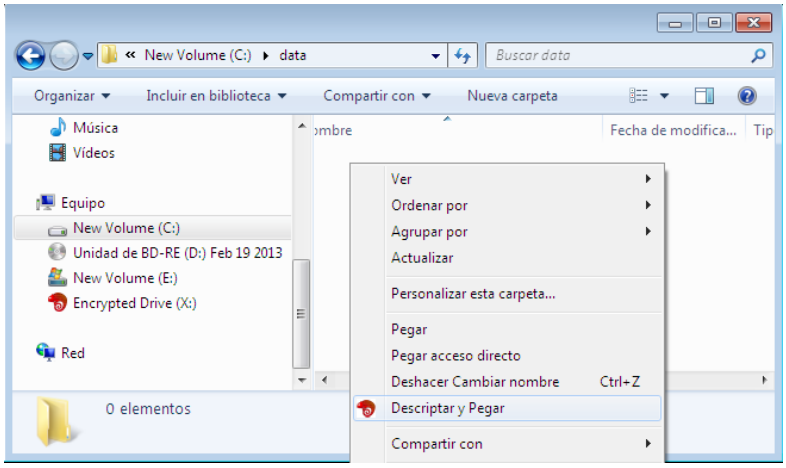
2. **Introduzca su contraseña (si está activada)**



3. **Haga clic derecho sobre el archivo .cge** a descriptar, a continuación, ccione "Cortar" o "Copiar". También puede utilizar los shortcuts (atajos de teclado) Cortar (Ctrl + X) o Copiar (Ctrl + C).

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Haga clic en la unidad o directorio destino.**



5. **Seleccione "Descriptar y Pegar”**

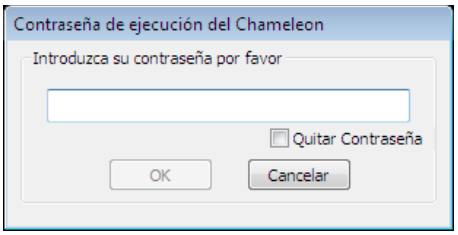
Esto coloca el contenido descriptado en el destino. Si selecciona "Cortar", el archivo de origen se borra de forma segura después de la descriptación completa.

4.3 Ver los detalles de los archivos encriptados

Para ver los detalles de un archivo encriptado:

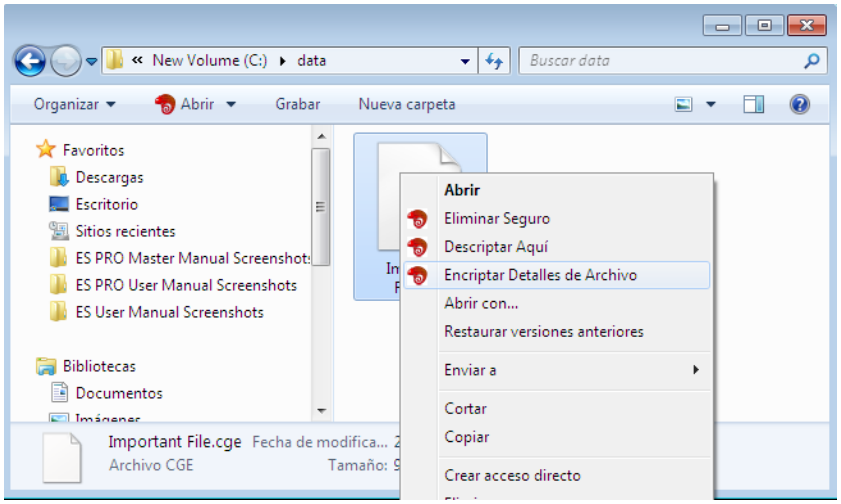
1. **Conecte el dispositivo**

2. **Introduzca su contraseña (si está activada)**

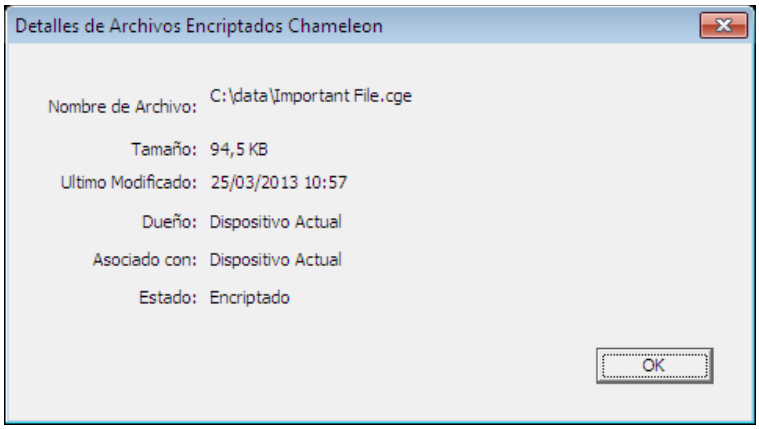


3. **Haga clic derecho sobre el archivo .cge**

4. **Seleccione "Encriptar Eetalles de Archivo"**



5. Los detalles de los archivos se muestran en una ventana nueva



5 Duplicación de un dispositivo Chameleon

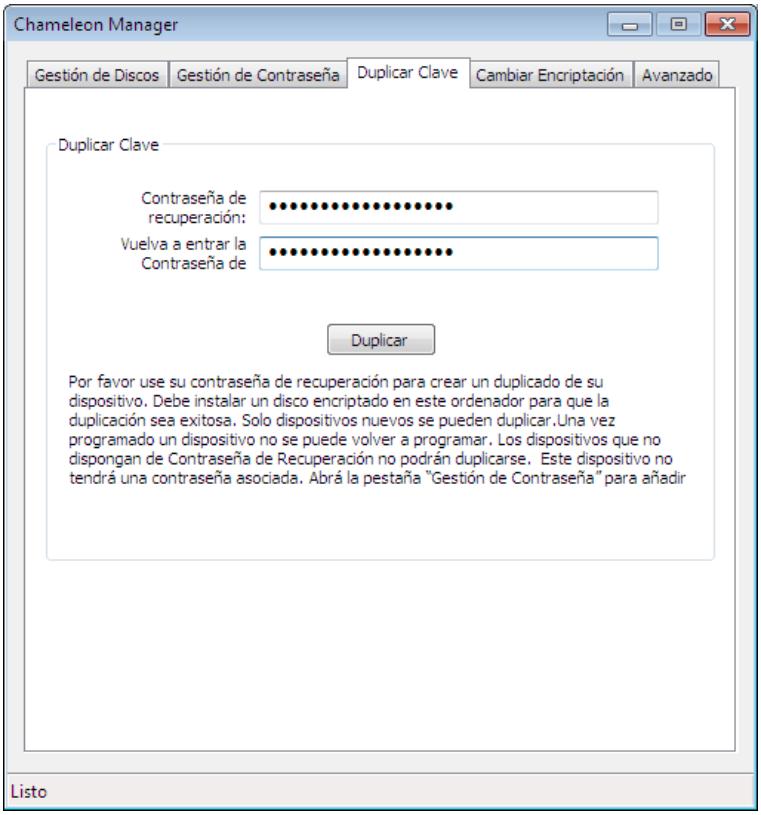
Si se pierde o se rompe el dispositivo Chameleon, los datos en la unidad encriptada se pueden recuperar usando un nuevo dispositivo Chameleon y la frase de contraseña de recuperación que había especificado durante la instalación. Este proceso también se puede utilizar para crear dispositivos Chameleon duplicados. Los dispositivos sin contraseña de recuperación no pueden ser duplicados.

1. **Conecte un nuevo dispositivo Chameleon.**

2. **Inicie el Manager de Chameleon** Haga clic en Windows "Inicio"> >
   Todos los programas >
   Chameleon >
   Chameleon Manager

3. **En la "Duplicar Clave", ingrese su frase de contraseña de recuperación original.**

4. **Haga clic en el botón "Duplicar".**



Este nuevo dispositivo duplicado no tendrá una contraseña asociada con él. Haga clic en " Gestión de Contraseña " para agregar una.

Usted no necesita el dispositivo Chameleon original para hacer un duplicado. Sin embargo, como medida de precaución, una unidad encriptada debe estar presente para lograr la duplicación.

6 Desactivación de dispositivos perdidos Chameleon

Puede bloquear un dispositivo perdido cambiando la contraseña de recuperación de un dispositivo y migrando todas las unidades[3] encriptadas a un dispositivo nuevo. Cada dispositivo sólo se puede cambiar una vez. Para repetir este procedimiento, se necesita un nuevo dispositivo Chameleon. Como medida de precaución, una unidad encriptada debe estar presente para lograr la migración.

Usted necesitará un dispositivo Chameleon programado con la frase de contraseña de recuperación original que especificó durante la instalación. Si el dispositivo original se ha perdido, usted tendrá que preparar un reemplazo (see "5 `Duplicación de un dispositivo Chameleon`"). Su disco duro (C: \) debe tener suficiente espacio libre para guardar todos los datos de las unidades encriptadas. Según el volumen de datos encriptados, este proceso puede

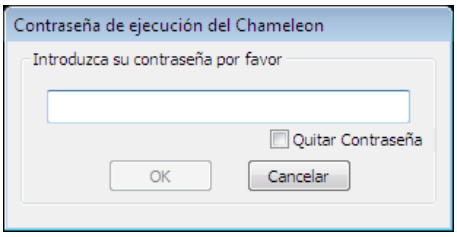
[3] Incluyendo las copias de seguridad

tardar algún tiempo. Las unidades (y copias de seguridad) encriptadas seguirán disponibles con el dispositivo original / perdido. Se le pedirá que las migren cuando se conectaran de nuevo.

Para cambiar el dispositivo y migrar las unidades encriptadas:

1. **Conecte un duplicado del dispositivo Chameleon original**.

2. **Introduzca su contraseña** (si está activada).



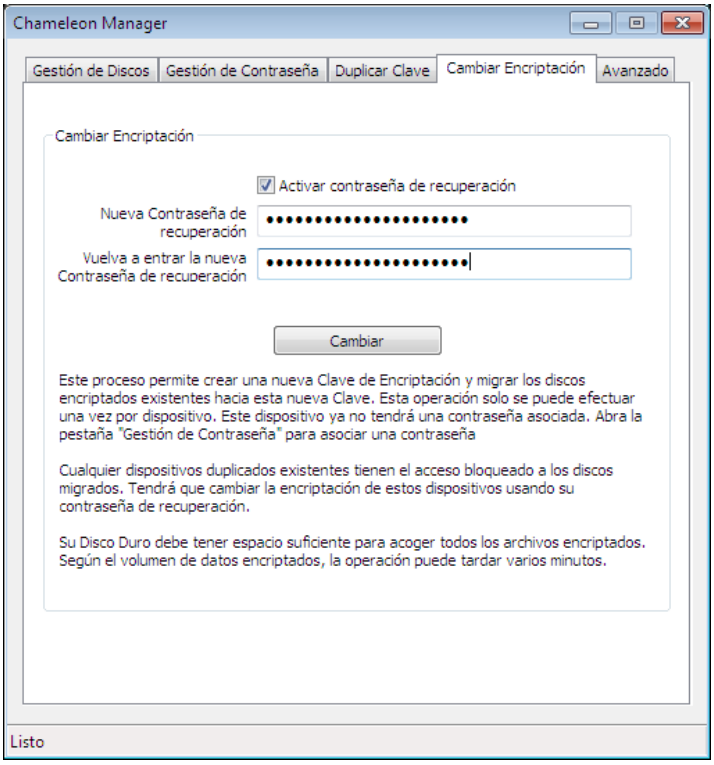
3. **Inicie el Manager de Chameleon**

Haga clic en Windows "Inicio" >
Todos los programas >
Chameleon >
Chameleon Manager

4. **Seleccione la opción "Cambiar de Encriptación"**.

5. **. Introduzca la nueva frase de recuperación de contraseña**. (Refer to "2 Instalación y configuración **Error! Reference source not found.**" por la elección de una frase de contraseña de recuperación).

6. **Pulse el botón "Cambiar"**.



Este procedimiento de sustitución crea con la recuperación de contraseña nuevas unidades encriptadas con todos sus archivos encriptados dentro. El dispositivo Chameleon de

actualización no tendrá una contraseña asociada con él. Haga clic en " Gestión de Contraseña " para agregar una.

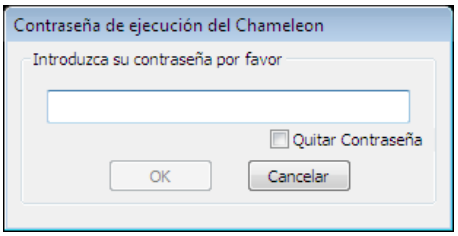
Las unidades encriptadas sin migrar están aún disponibles con el nuevo dispositivo Chameleon.

6.1 Migración de archivos encriptados (.cge)

Además de las unidades encriptadas, debe volver a encriptar también los archivos .cge codificados por la clave de criptación original.

1. **Conecte el dispositivo**

2. **Introduzca su contraseña** (si está activada)



3. **Inicie el "Migrador de archivos encriptados"**

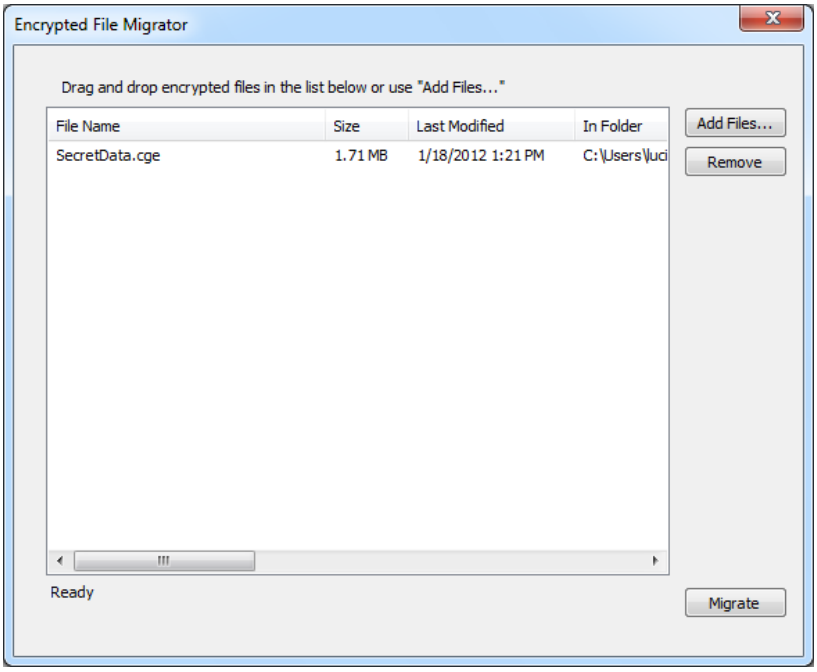
   Haga clic en Windows "Inicio" >
   Todos los programas >
   Chameleon >
   Migrador de archivos encriptados

4. **Seleccione los archivos .cge que desea migrar.**

   Arrastre directamente en la ventana de lista de archivos.

   o

   Haga clic en "Agregar archivos", busque y seleccione los archivos.



5. **Cierre todos los archivos abiertos que residen en las unidades encriptadas.**

   Antes de que el proceso de migración comience las unidades encriptadas se va a separar. Si un archivo está abierto, el Migrador pedirá al usuario de cerrarla.

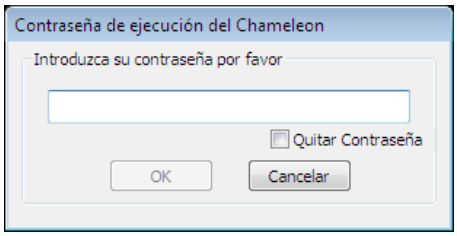
6. **Haga clic en el botón "migrar"**

Una vez el proceso de migración terminado, el dispositivo perdido no podrá acceder al archivo encriptado. El disco duro que contiene los archivos .cge debe tener suficiente espacio libre para guardar una copia del archivo más grande de la lista. Según el volumen de datos encriptados, este proceso puede tardar algún tiempo.

Sus unidades encriptadas se vuelve a unir cuando el proceso de migración se acaba.

7 Protección por contraseña

De forma predeterminada, no se requieren contraseñas para los dispositivos Chameleon. Sin embargo, la utilización de una protección con una contraseña asegura sus datos en caso de pérdida de su dispositivo junto con su PC. Cuando está activada, el software solicita al Chameleon la contraseña cada vez que se conecte o se reinicia el equipo o cuando deshiberna.



La contraseña es diferente de la frase de recuperación de contraseña. La recuperación de contraseña sólo se necesita en la inicialización o duplicación. Cuando está activada, la contraseña debe introducirse cada vez que se conecta el dispositivo. Se utiliza para prevenir el acceso no autorizado a su equipo, no para proteger sus datos. Dispositivos Chameleon con la misma frase de recuperación de contraseña, pero con diferentes contraseñas pueden acceder a las mismas unidades encriptadas.

Si olvida su contraseña, elimine la protección de contraseña entrando su frase de contraseña de recuperación cuanto se le pide su contraseña.

7.1 Cambio de contraseña

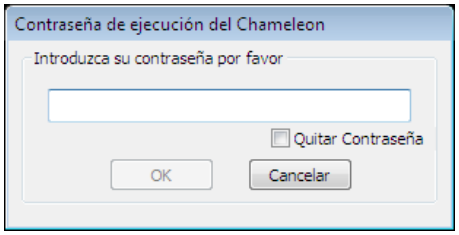
Usted puede agregar, cambiar o eliminar la protección con contraseña tantas veces como desee. Es posible tener dispositivos duplicados con diferentes contraseñas (o ninguna en absoluto).

Tenga en cuenta que un dispositivo Chameleon sin protección por contraseña puede acceder a los datos protegidos por un dispositivo diferente con protección por contraseña, siempre y cuando tengan la misma frase de contraseña de recuperación.

Para modificar las opciones de contraseña:

1. **Conecte el dispositivo**

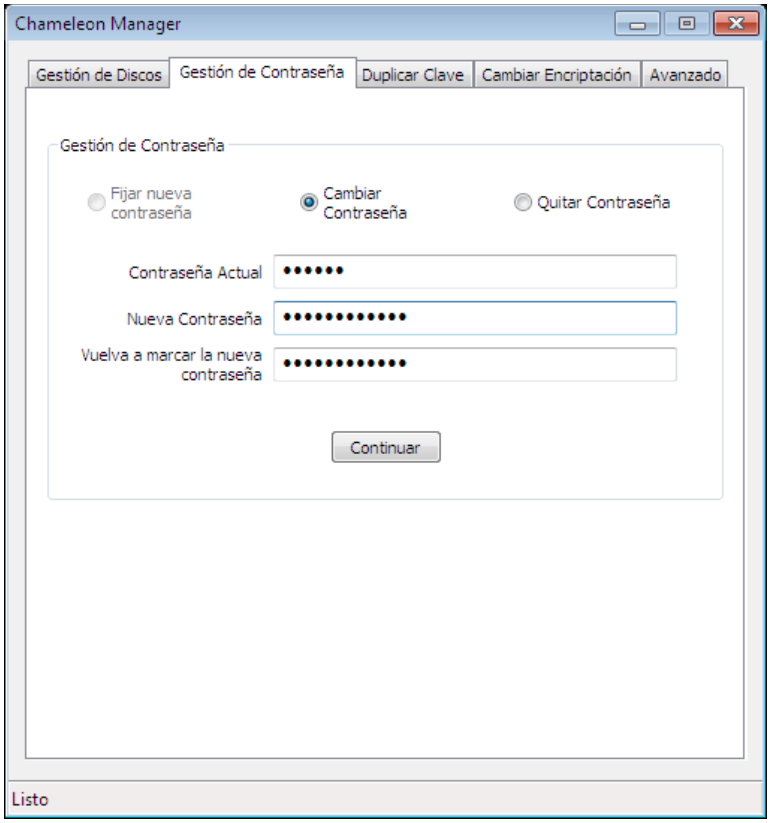
2. **Introduzca su contraseña (si está activada ya)**



3. **Inicie la aplicación Chameleon Manager**

Haga clic en Windows "Inicio" >
Todos los programas >
Chameleon >
Chameleon Manager

4. **Seleccione la pestaña "Gestión de Contraseñas".**



- Para agregar una contraseña, seleccione "Fijar nueva contraseña " e introduzca la nueva contraseña, haga clic en el botón "Continuar".

- Para cambiar su contraseña: Seleccione "Cambiar contraseña". Introduzca su contraseña actual. Escriba la nueva contraseña y verificarla. Haga clic en el botón "Continuar".

- Para eliminar la contraseña, seleccione "Wuitar Contraseña" e introduzca su contraseña, haga clic en el botón "Continuar".

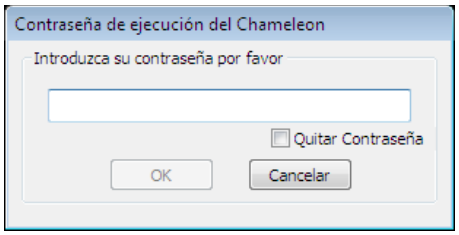
Puede cambiar la contraseña tantas veces como quiera.

8 Cómo agregar, eliminar, cambiar el tamaño y las unidades encriptadas

Puede agregar, eliminar o cambiar el tamaño de las unidades encriptadas en cualquier momento. Mientras haya suficiente espacio en el disco, no hay límite en el número de unidades encriptadas que usted puede tener asociadas con un solo dispositivo. Las unidades encriptadas se pueden crear en el disco duro interno, así como en unidades USB externas.

1. **Conecta su dispositivo.**

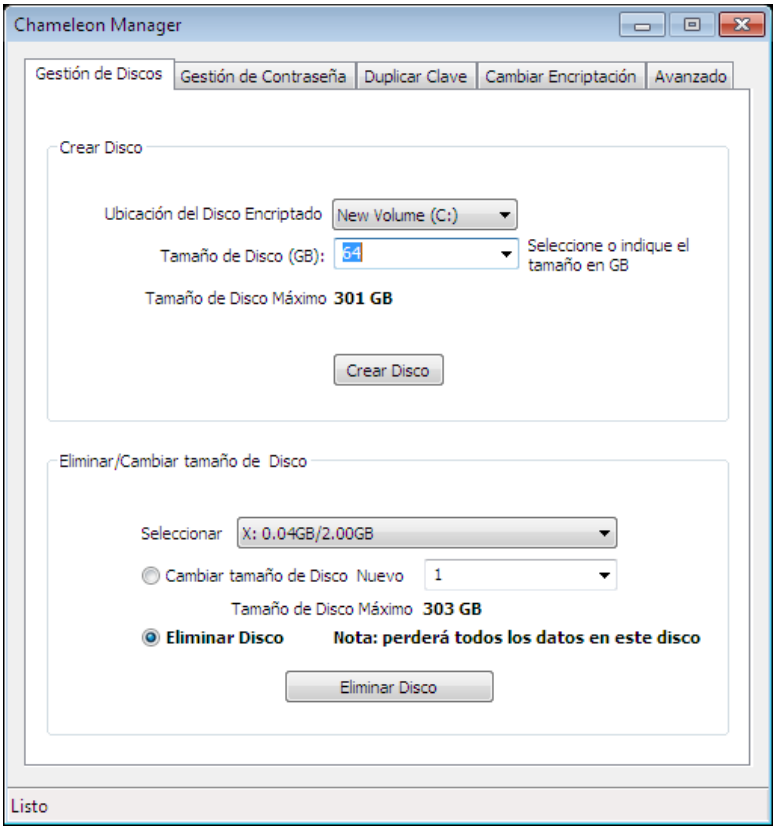
2. **Introduzca su contraseña (si está activada ya)**



3. **Inicie el Manager de Chameleon** Haga clic en Windows "Inicio" > Todos los programas > Chameleon > Chameleon Manager

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

4. **Seleccione la pestaña "Gestión de Discos".**



- Para agregar una unidad, especifique el tamaño y la ubicación de la unidad encriptada, a continuación, haga clic en el botón "Crear Disco".

- Para borrar una unidad, seleccione la unidad existente en el menú desplegable, seleccione "Eliminar Discos". Haga clic en el botón " Borrar unidad". Se le pedirá una confirmación.

- Para cambiar el tamaño de una unidad, seleccione la unidad en el menú desplegable, seleccione "Cambiar el tamaño de la unidad". Introduzca el tamaño deseado y luego haga clic en el botón "tamaño de unidad". Al reducir el tamaño de la unidad, el disco duro (C: \) debe tener suficiente espacio libre para retener temporalmente todos los contenidos de la unidad encriptada.

9 Funciones y Limitaciones Adicionales

9.1 Utilización de un dispositivo Chameleon con varios equipos

Un único dispositivo Chameleon puede utilizarse en varios equipos.

Si el software Chameleon no se ha instalado, siga la sección "2 `Instalación y configuración`" para instalarlo en otro equipo. Después del paso # 4, el instalador salta directamente al paso 7 para crear una unidad encriptada si el dispositivo ha sido inicializado ya.

Si el software Chameleon se ha instalado ya, consulte el capítulo 2"`Instalación y configuración`" Paso # 7 para crear una unidad encriptada.

9.2 Utilización de varios dispositivos con el mismo equipo

Usted puede tener varias unidades asociadas con diferentes dispositivos Chameleon en el mismo equipo y su disco duro.

Una instalación de software adicional no es necesaria. Conecte el segundo dispositivo y utilice el Manager de Chameleon para crear unidades encriptadas asociadas a este dispositivo. Si no es un duplicado, el segundo dispositivo sólo podrá acceder a sus propias unidades - y no a las unidades asociadas al primer dispositivo.

Si desea no utilizar más un dispositivo en particular y en un ordenador concreto, tiene que borrar sus unidades encriptadas, usando el Manager de Chameleon en lugar de desinstalar el propio software Chameleon. La desinstalación del software Chameleon no borra las unidades encriptadas.

El software Chameleon no admite más de un dispositivo Chameleon conectado a la vez.

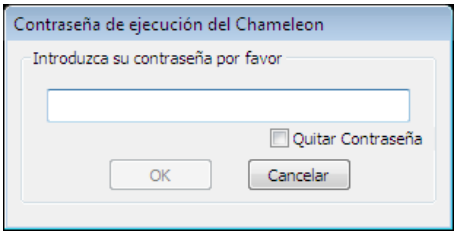
9.3 Archivo de paginación de Windows

Windows puede almacenar datos temporales en el archivo de paginación (memoria virtual). Este archivo no está normalmente encriptado y se actualiza continuamente. Facilitar el cifrado de los archivos de paginación para que Windows encripte sus archivos de paginación.

Para facilitar la encriptación del archivo de paginación:

1. **Conecte el dispositivo.**

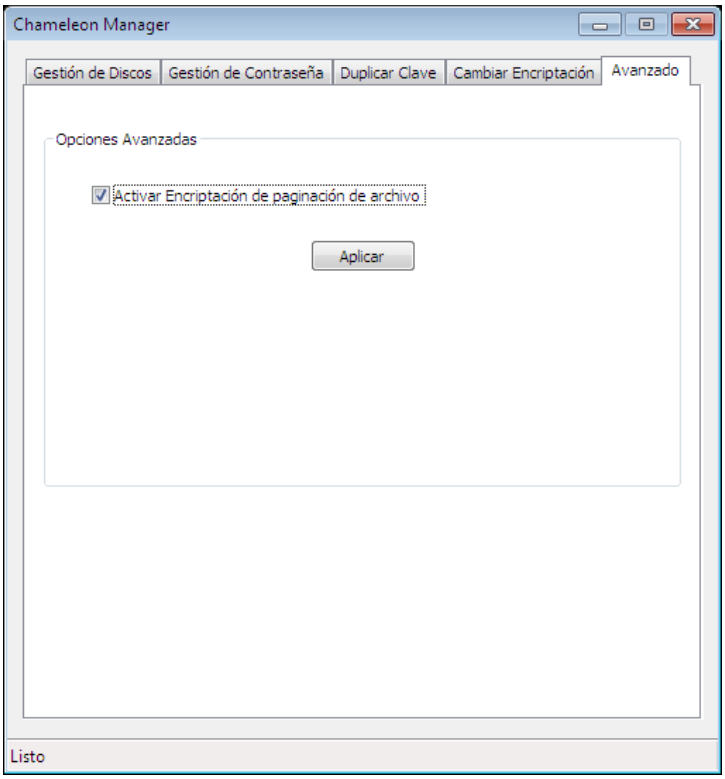
2. **Introduzca su contraseña (si está activada ya)**



3. **Inicie el Manager de Chameleon** Haga clic en Windows "Inicio" > Todos los programas > Chameleon > Chameleon Manager

4. **Seleccione la pestaña "Avanzado.**

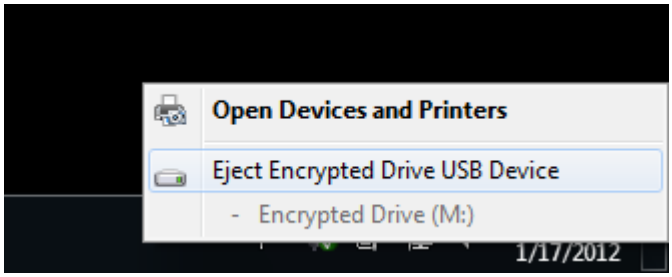
5. **Seleccione "Activar Encriptación de paginación de archivo" y luego haga clic en "Aplicar"**



Encriptar el archivo de paginación elimina una falta de seguridad potencial, pero ralentiza el ordenador ligeramente. Sólo Windows 7 es compatible con la encriptación de los archivos de paginación (desconocido por otros sistemas operativos).

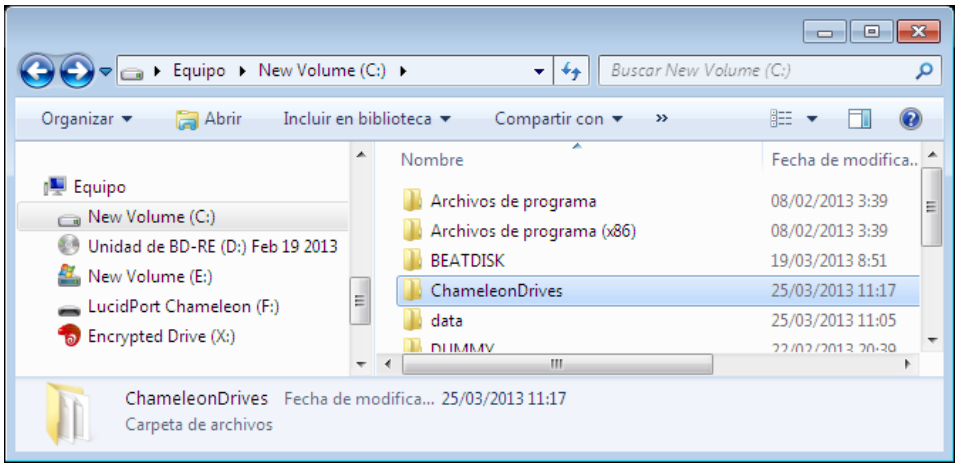
9.4 Extracción segura

Desconectar el dispositivo Chameleon mientras escribe datos en la unidad encriptada puede dañar los datos. Es similar a quitar un disco duro externo mientras se utiliza. Para estar absolutamente seguro de que no se está produciendo, utilice la función Quitar seguro de Windows antes de desenchufar el dispositivo.



9.5 Copia de seguridad de datos

Se hace una copia de seguridad de las unidades encriptadas copiando los directorios de las unidades Chameleon a otra ubicación. Este directorio se encuentra en el nivel superior de su disco duro (por ejemplo, C: \ unidades Chameleon \). Dado que las unidades encriptadas se encriptan siempre, las copias de seguridad están protegidas también. Se debe desenchufar el dispositivo Chameleon para hacer la copia de seguridad de sus datos.



Usted puede agregar el directorio Unidades Chameleon a su lista de copias de seguridad programadas.

ADVERTENCIA: No copie la copia de seguridad Unidades Chameleon directorio a nivel superior (raíz) de una unidad (por ejemplo, D: \ Unidades Chameleon). El software Chameleon no puede distinguir entre el original y la copia. Si las unidades idénticas se detectan en el nivel superior, el software Chameleon no se activará la unidad de disco. Cualquier lugar subdirectorio o red funcionará (por ejemplo D: \ Backup \ Unidades Chameleon).

10 Limited Warranty and Legal Notices

Chameleon
Copyright (c) 2011, LucidPort Technology, Inc.
485 E. Evelyn Ave
Sunnyvale, CA 94086
Tel: (408) 720-8800
Fax: (408) 720-8900

Pongase en contacto con support@marathon6.com para preguntas técnicas.
Pongase en contacto con sales@marathon6.com temas relacionados con la garantía.
Conectese a http://www.marathon6.com/chameleon para descargar las últimas actualizaciones.

LucidPort Technology, Inc. le garantiza que el Chameleon estará libre de defectos en materiales y mano de obra bajo un uso normal durante el período de garantía de 90 días a partir de su fecha de compra. Su factura o recibo de entrega es su comprobante de fecha de compra. Es posible que se deba presentar la prueba de compra como condición para recibir el servicio de garantía.
Si LucidPort Technology, Inc. recibe, durante el período de garantía, el aviso de un defecto en el Chameleon, LucidPort Technology, Inc. reparará o reemplazará el producto, a discreción de LucidPort Technology, Inc. 's. LucidPort Technology, Inc. no tendrá obligación de reparar, sustituir o reembolsar hasta que regrese su aparato al LucidPort Technology, Inc.. Si el Chameleon tiene fallos repetitivos, LucidPort Technology, Inc. Elige de proporcionar un reemplazo que sera el mismo o equivalente en rendimiento o bien un reembolso del precio de su compra en lugar de un reemplazo.

En la medida permitida por la ley local, LucidPort Technology Inc., y cualquier producto o piezas de repuesto, pueden contener materiales nuevos y usados equivalentes a los nuevos en rendimiento y fiabilidad. Los productos de sustitución o parte también tendrán una funcionalidad al menos igual a la del producto o pieza que sustituye. Los productos de reemplazo y las piezas tienen garantía de estar libre de defectos en materiales o mano de obra durante 90 días. LucidPort Technology, Inc., a su entera discreción, podrá subcontratar o contratar a un tercero para proporcionar los servicios de garantía.

Pérdida de datos es una consecuencia frecuente de la reparación. LOS DATOS ALMACENADOS CON EL CHAMELEON NUNCA ESTÁN CUBIERTOS POR LA GARANTÍA.

Esta garantía limitada no se aplica a las piezas desechables o consumibles o de cualquier producto en el que se ha abierto el chasis o si está dañado o defectuoso (A) debido a un accidente, mal uso, abuso, contaminación, infección por virus, impropio o inadecuado mantenimiento o calibración o otras causas externas, (B) software, interfaces, piezas o consumibles no suministrados por LucidPort Technology, Inc., (C) preparación o mantenimiento inadecuado, (D) pérdida o daños durante el transporte, o (E) la modificación o servicio por excepto LucidPort Technology, Inc. o de una tecnología LucidPort, Inc. proveedor de servicio autorizado.

EN LA MEDIDA EN QUE LO PERMITA LA LEGISLACIÓN LOCAL, EN NINGÚN CASO LUCIDPORT TECHNOLOGY, INC SERÁ RESPONSABLE DE LOS DAÑOS CAUSADOS POR EL PRODUCTO O EL FRACASO DEL FUNCIONAMIENTO DEL MISMO, INCLUYENDO CUALQUIER DAÑO DIRECTO, INDIRECTO, ESPECIAL, INCIDENTAL, CONSECUENTE O PUNITIVO DE NINGÚN TIPO, YA SEA POR CONTRATO, AGRAVIO (INCLUYENDO NEGLIGENCIA) O CUALQUIER OTRA TEORÍA LEGAL, Y YA SEA ADVERTIDO DE LA POSIBILIDAD DE TALES DAÑOS. LUCIDPORT TECHNOLOGY, INC NO SE HACE RESPONSABLE POR CUALQUIER RECLAMO HECHO POR TERCEROS O POR USTED PARA TERCEROS.

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com

La tecnología de cifrado AES en el Chameleon es clasificada por el gobierno de Estados Unidos como un elemento ECCN 5A002 y pueden ser exportados bajo la Excepción de licencia ENC, sec. 740.17 (b) (3) del Reglamento de la Administración de Exportaciones ("EAR"). El Chameleon no se puede utilizar ni exportar o reexportar a (o a un ciudadano o residente de) Cuba, Irán, Corea del Norte, Sudán o Siria. No hay otras aprobaciones o autorizaciones del gobierno de EE.UU. obligatorias.

485 E. Evelyn Ave., Sunnyvale, CA 94086
Tel: (408)720-8800 Fax: (408)720-8900
www.lucidport.com