

¿Qué es PGP NetShare?

El producto PGP NetShare es una herramienta de software que proporciona múltiples maneras de proteger y compartir datos.

Utilice PGP NetShare para:

- Permitir que los usuarios autorizados intercambien archivos protegidos en un espacio compartido, como un servidor, una carpeta compartida o una unidad USB extraíble.
- Utilizar parte del espacio del disco duro como un volumen de disco virtual encriptado con su propia letra de unidad.
- Crear archivos Zip encriptados y seguros.
- Colocar archivos y carpetas en un paquete comprimido único que pueda abrirse en sistemas Windows que no tengan PGP Desktop Email o PGP Desktop instalados.
- Destruir archivos y carpetas completamente para que ni siquiera un software de recuperación de archivos pueda recuperarlos.
- Borrar de manera segura el espacio libre en las unidades para que los datos eliminados sean realmente irrecuperables.

Contenidos

- ¿Qué es PGP NetShare? (página 1)
- ¿Es la primera vez que utiliza PGP NetShare? (página 1)
- Comprensión de las generalidades (página 1)
- ¿Qué estoy instalando? (página 2)
- Requisitos del sistema (página 2)
- Instalación de PGP NetShare (página 3)
- Inicio de PGP NetShare (página 3)
- La pantalla principal de PGP NetShare (página 3)
- Utilización de PGP NetShare (página 4)
- Creación de volúmenes de PGP Virtual Disk (página 4)
- Creación de un archivo de PGP Zip (página 5)
- Utilización de PGP Shred para triturar archivos (página 6)
- Cómo obtener ayuda (página 7)

¿Es la primera vez que utiliza PGP NetShare?

Utilice esta guía paso a paso para comenzar. Descubrirá que proteger los datos con PGP NetShare es tan sencillo como poner llave en una cerradura.

- Esta *Guía de inicio rápido* lo ayuda a instalar PGP NetShare y a comenzar.
- La *Guía del usuario de PGP Desktop* proporciona más información detallada sobre PGP NetShare. Si desea crear un par de llaves, en esa guía aprende lo que significa un par de llaves, cómo crearlo y cómo intercambiar llaves con otras personas para poder encriptar y compartir los datos de manera segura.

Nota: una licencia de PGP NetShare le proporciona acceso a un determinado conjunto de funciones de PGP NetShare. Otras funciones de PGP NetShare pueden requerir una licencia diferente. Consulte la sección Licencia de la *Guía del usuario de PGP Desktop* para obtener más información.

- Para la implementación, la administración y la información de cumplimiento de las políticas de PGP NetShare, consulte la *Guía del administrador de PGP Universal Server*.

Comprensión de las generalidades

Después de la instalación, PGP NetShare le solicita que cree un par de llaves PGP. Un par de llaves es la combinación de una llave privada y una llave pública.

- Conserve la *llave privada* y su contraseña en privado, tal como lo indica el nombre. Si alguien obtiene la llave privada y la contraseña, puede leer sus mensajes y suplantarlos ante otros usuarios. La llave privada descrypta los mensajes entrantes encriptados y firma los mensajes salientes.
- Por otra parte, puede compartir su *llave pública* con cualquier persona. Esta llave no tiene una contraseña. Su llave pública encripta mensajes que sólo puede descryptar su llave privada y verifica los mensajes firmados.

El anillo de llaves contiene tanto sus pares de llaves como las llaves públicas de otros, que usted utiliza para enviar mensajes encriptados. Haga clic en el cuadro de control Llaves PGP en su anillo de llaves:

- 1 El icono de un par de llaves PGP tiene dos llaves, una indica la llave privada y la otra, la pública. Por ejemplo,

en esta ilustración Alice Cameron tiene un par de llaves PGP.

- 2 Los iconos de las llaves públicas de otras personas sólo tienen una llave. La llave pública de Ming Pa, por ejemplo, se ha agregado al anillo de llaves que se muestra en esta ilustración.



¿Qué estoy instalando?

PGP NetShare utiliza licencias para proporcionar acceso a las características que usted compra. Según la licencia que tenga, se activan algunos de los integrantes o toda la familia de aplicaciones de PGP NetShare.

Este documento contiene instrucciones para visualizar las características activadas con su licencia.

PGP NetShare es un miembro de la familia de aplicaciones PGP Desktop. Puede utilizar PGP NetShare para autorizar a los usuarios a intercambiar archivos protegidos en un espacio compartido, como un servidor corporativo, en una carpeta compartida o en un dispositivo extraíble (como una unidad USB). Los archivos encriptados de la carpeta protegida continúan apareciendo como archivos de aplicación normales para los usuarios autorizados. Cualquier persona con acceso físico a los archivos puede verlos pero no puede utilizarlos.

Otros componentes que se incluyen con PGP NetShare son:

Los **volúmenes de PGP Virtual Disk** utilizan parte del espacio del disco duro como un volumen de disco virtual encriptado con su propia letra de unidad. Un PGP Virtual Disk es el lugar perfecto para guardar archivos confidenciales; es como guardarlos en una caja fuerte. Cuando la puerta de la caja fuerte está abierta (cuando se monta el volumen), se pueden modificar los archivos guardados y extraer o colocar archivos. De lo contrario (cuando el volumen está desmontado), todos los datos están protegidos.

PGP Zip agrega cualquier combinación de archivos y carpetas a un archivo encriptado, comprimido y portátil. PGP Desktop debe estar instalado en un sistema para crear o abrir un archivo de PGP Zip. PGP Zip es una herramienta que sirve para archivar de manera segura los datos confidenciales, ya sea porque quiere distribuirlos a otras personas o realizar una copia de seguridad.

Los **Archivos de descryptación automática de PGP (SDA)** colocan los archivos y las carpetas en un paquete encriptado y comprimido que puede abrirse en sistemas Windows que no tienen el software de PGP instalado. Los SDA son la solución

perfecta para intercambiar archivos de manera segura con alguien que no tiene el software de PGP instalado.

PGP Shredder destruye completamente archivos y carpetas para que ni siquiera un software de recuperación de archivos pueda recuperarlos. Cuando se elimina un archivo colocándolo en la papelera de reciclaje de Windows (en sistemas Windows) o en la papelera (en sistemas Mac OS X), no se borra realmente, sino que permanece en la unidad y, eventualmente, se sobrescribe. Hasta ese momento, un atacante puede recuperar muy fácilmente un archivo. PGP Shredder, en cambio, sobrescribe inmediatamente los archivos varias veces. Esto es tan efectivo que ni siquiera un software de recuperación de disco sofisticado puede recuperar estos archivos. Esta característica también borra el espacio libre de las unidades para que los datos eliminados sean realmente irrecuperables.

Gestión de llaves administra las llaves de PGP, tanto los pares de llaves como las llaves públicas de otras personas. La llave privada se utiliza para descryptar los mensajes que le envían encriptados con su llave pública y para proteger los volúmenes de PGP Virtual Disk. Las llaves públicas se utilizan para encriptar mensajes para otras personas o para agregar usuarios a los volúmenes de PGP Virtual Disk.

Requisitos del sistema

PGP NetShare se puede instalar en los sistemas que ejecutan las siguientes versiones de los sistemas operativos Microsoft Windows:

- Windows XP Professional de 32 bits (Service Pack 2 o 3), Windows XP Professional de 64 bits (Service Pack 2), Windows XP Home Edition (Service Pack 2 o 3), Microsoft Windows XP Tablet PC Edition 2005 SP2, Windows Vista (todas las ediciones de 32 y 64 bits, incluido el Service Pack 2), Windows 7 (todas las ediciones de 32 y 64 bits), Windows Server 2003 (Service Pack 1 y 2).

Los sistemas operativos mencionados anteriormente serán compatibles únicamente cuando se hayan aplicado todas las reparaciones en caliente y los parches de seguridad más recientes de Microsoft.

Nota: PGP Whole Disk Encryption (PGP WDE) no es compatible con otros software de terceros que puedan desviar la protección PGP WDE en el registro de arranque maestro (MBR) y escribir o modificar el MBR. Esto incluye herramientas de desfragmentación fuera de línea que desvían la protección del sistema de archivos PGP WDE en el sistema operativo o las herramientas de restauración del sistema que reemplazan al MBR.

Requisitos de hardware

- 512 MB de RAM
- 64 MB de espacio en disco duro

Instalación de PGP NetShare:

Symantec Corporation recomienda salir de todas las aplicaciones abiertas antes de comenzar con la instalación. El proceso de instalación requiere que se reinicie el sistema.

Nota: si está utilizando PGP NetShare en un entorno gestionado por PGP Universal Server, el instalador de PGP NetShare puede configurarse con opciones o características específicas.

Para instalar PGP NetShare

- 1 Busque el programa de instalación de PGP NetShare que descargó.
Es posible que el administrador de PGP haya distribuido el programa de instalación mediante la herramienta de implementación de Microsoft SMS.
- 2 Haga doble clic en el instalador.
- 3 Siga las instrucciones en pantalla.
- 4 Reinicie el sistema cuando se le indique.
- 5 Cuando se reinicie el sistema, siga las instrucciones que aparecen en pantalla para configurar PGP NetShare.

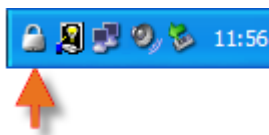
Licencia

Para ver qué funciones admite su licencia, abra PGP NetShare y seleccione **Ayuda > Licencia**. Las funciones con una marca de verificación son compatibles con la licencia activa.

Inicio de PGP NetShare

Para iniciar PGP NetShare, utilice cualquiera de los siguientes métodos:

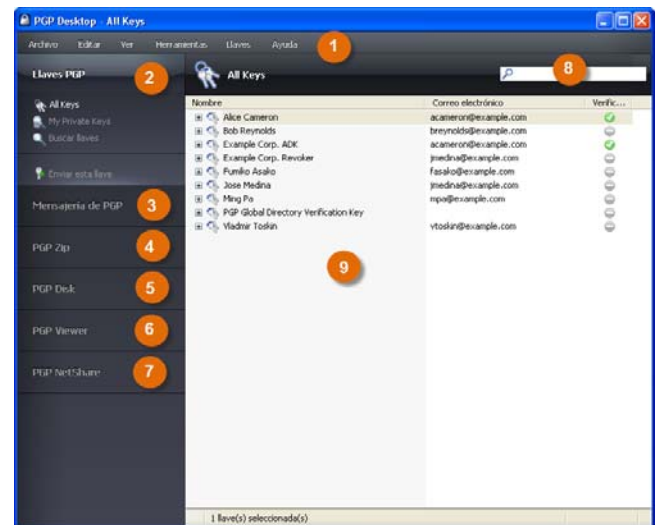
- Haga doble clic en el icono de PGP.



- Haga clic con el botón secundario en el icono de PGP y luego seleccione **Abrir PGP NetShare**.
- En el menú **Inicio**, seleccione **Programas > PGP > PGP NetShare**.

La pantalla principal de PGP NetShare

La ventana de la aplicación PGP NetShare es la interfaz principal del producto.



La pantalla principal de PGP NetShare incluye:

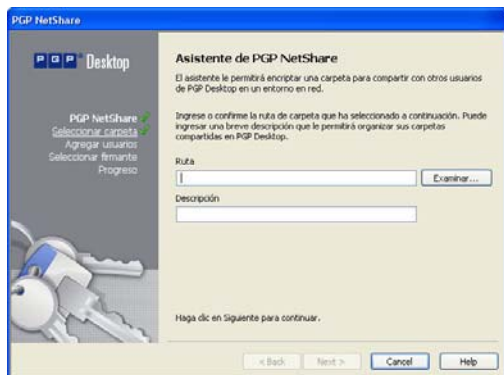
- 1 **La barra de menú.** Proporciona acceso a los comandos de PGP NetShare. Los menús de la barra de menú cambian según el cuadro de control seleccionado.
- 2 **El cuadro de control Llaves PGP.** Permite controlar las llaves PGP.
- 3 **El cuadro de control Mensajería de PGP.** Permite controlar la mensajería de PGP.
- 4 **El cuadro de control PGP Zip.** Permite controlar PGP Zip y el Asistente de PGP Zip, que ayuda a crear nuevos archivos de PGP Zip.
- 5 **El cuadro de control de PGP Disk.** Permite controlar PGP Disk.
- 6 **El cuadro de control PGP Viewer.** Le permite descryptar, verificar y mostrar mensajes *fuera* del flujo de correos.
- 7 **El cuadro de control PGP NetShare.** Permite controlar PGP NetShare.
- 8 **El área de trabajo de PGP NetShare.** Muestra la información del cuadro de control seleccionado y las acciones que puede realizar con él.
- 9 **Cuadro de búsqueda de llaves PGP.** Se usa para buscar llaves en el anillo de llaves. A medida que escribe texto en el cuadro, PGP NetShare muestra los resultados de búsqueda según el nombre o la dirección de correo electrónico.

Cada cuadro de control se expande para mostrar las opciones disponibles y se contrae para ahorrar espacio (sólo se muestra el título del cuadro de control). Para expandir un cuadro de control, haga clic en el título.

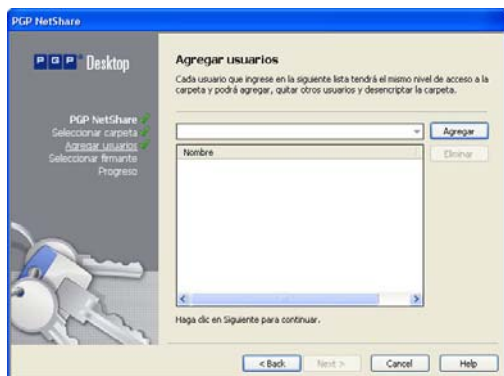
Utilización de PGP NetShare

La función PGP NetShare permite el intercambio de archivos protegidos entre los usuarios autorizados. Primero, debe crear una carpeta protegida y especificar aquellos usuarios que están autorizados para utilizar los archivos.

- 1 Haga clic en **Agregar carpeta** en el cuadro de control de PGP NetShare. Se muestra la pantalla Seleccionar carpeta.



- 2 Haga clic en **Examinar** y seleccione la carpeta que desea proteger.
- 3 En el campo **Descripción**, escriba una descripción para la Carpeta protegida que está creando o déjelo en blanco para utilizar el nombre predeterminado.
- 4 Haga clic en **Siguiente**. Se muestra la pantalla Agregar usuarios.



- 5 Para especificar los usuarios de los archivos de la Carpeta protegida, haga clic en el icono de flecha hacia abajo, seleccione un usuario y haga clic en **Agregar**. No olvide agregarse usted mismo si desea tener acceso a los archivos de la Carpeta protegida.

PGP NetShare no les notifica a los usuarios que tienen acceso a las carpetas protegidas; el encargado de hacerlo es el creador de la nueva Carpeta protegida.

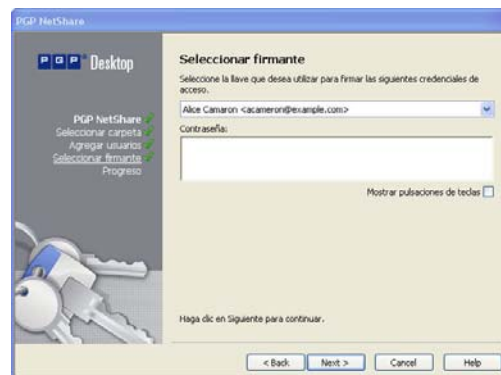
- 6 Para asignar roles a los usuarios, haga clic con el botón secundario en el nombre del usuario y seleccione el rol:
 - **Administrador:** Puede crear un solo administrador por carpeta protegida de PGP NetShare. Los usuarios que tienen este rol obtienen el derecho total de lectura y escritura en la carpeta, pueden agregar y

quitar usuarios, asignar roles a los demás usuarios, y convertir a otro usuario en Administrador.

- **Gestión del grupo:** Puede crear tantos Administradores de grupo como sean necesarios para cada carpeta protegida de PGP NetShare. Los usuarios que tienen este rol obtienen el derecho total de lectura y escritura en la carpeta, pueden agregar y quitar usuarios, y asignar roles a los demás usuarios.
- **Usuario:** Puede crear tantos usuarios como sean necesarios para cada carpeta protegida de PGP NetShare. Mediante este rol, se obtiene el derecho total de lectura y escritura en la carpeta.

Puede cambiar el rol de un usuario en cualquier momento, después de crear la carpeta protegida. Haga clic en la carpeta protegida de PGP NetShare y haga clic con el botón secundario en el nombre de usuario para cambiar el rol.

- 7 Haga clic en **Siguiente**. Se muestra la pantalla Seleccionar firmante.

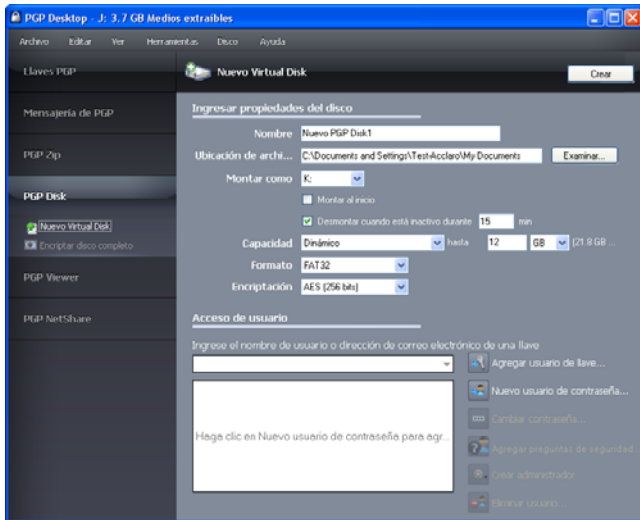


- 8 Seleccione una llave privada del anillo de llaves local e ingrese la frase de contraseña apropiada (si la frase de contraseña no está almacenada en caché). Esta llave se utiliza para asegurar la información de la configuración de PGP NetShare para la carpeta protegida y sus archivos.
- 9 Haga clic en **Siguiente**. Se muestra la pantalla Progreso. Los archivos de la Carpeta protegida especificada se encriptan, y los usuarios especificados están autorizados para utilizar los archivos. Aquí encontrará una lista de los archivos que, quizá, se hayan omitido, como por ejemplo, los archivos de sistema.
- 10 Haga clic en **Finalizar**.

Creación de volúmenes de PGP Virtual Disk

La función de volúmenes de PGP Virtual Disk utiliza parte del espacio del disco duro como un volumen de disco virtual encriptado con su propia letra de unidad. Puede crear usuarios adicionales para un volumen, de modo que las personas que autorice también puedan tener acceso al volumen.

- 1 Haga clic en **Nuevo disco virtual**, en el cuadro de control de PGP Disk.



- 2 Escriba un **Nombre** para el volumen.
- 3 Especifique una **Ubicación de archivo de disco** para el volumen.
- 4 Para especificar las preferencias de montaje, haga lo siguiente:
 - seleccione una letra de unidad para el volumen en el menú **Montar como**.
 - seleccione **Montar al inicio** para que el nuevo volumen se monte automáticamente al inicio.
 - seleccione **Desmontar cuando la computadora está inactiva durante x minutos** para que el volumen se desmonte automáticamente cuando la computadora ha estado inactiva durante la cantidad de minutos especificada.
- 5 Desde **Capacidad**, seleccione **Dinámico (puede cambiar de tamaño)** si desea que el tamaño del volumen aumente a medida que agrega archivos o **Tamaño fijo** si desea que el volumen mantenga siempre el mismo tamaño.
- 6 Especifique un **Formato** de sistema de archivos para el volumen.
- 7 Especifique un algoritmo de **Encriptación** para el volumen.
- 8 Haga clic en **Agregar usuario** para agregar usuarios que autentican mediante una criptografía de llave pública o haga clic en **Nuevo usuario de contraseña** para agregar usuarios que autenticarán mediante frases de contraseña.
- 9 Haga clic en **Crear**.

Utilice la sección **Acceso de usuario** para controlar a los usuarios existentes de un volumen de PGP Virtual Disk:

- 1 Haga clic en **Agregar llave de usuario** para agregar usuarios que autentican mediante criptografías de llave pública.
- 2 Haga clic en **Nuevo usuario de contraseña** para agregar usuarios que autentican mediante frases de contraseña.

- 3 Seleccione un usuario de frase de contraseña y haga clic en **Cambiar frase de contraseña** para cambiarla.
- 4 Seleccione un usuario y haga clic en **Crear administrador** para otorgarle derechos administrativos.
- 5 Seleccione un usuario y haga clic en **Eliminar** para eliminarlo.

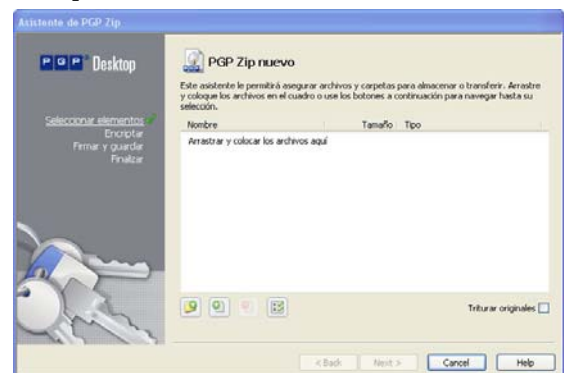
Creación de un archivo de PGP Zip

Los archivos de PGP Zip le permiten colocar cualquier combinación de archivos y carpetas en un archivo portátil comprimido. Existen cuatro tipos de archivos de PGP Zip:

- **Llaves de destinatario.** Encripta el archivo con las llaves públicas. Sólo el titular de las llaves privadas correspondientes puede abrir el archivo. Este es el tipo de archivo de PGP Zip más seguro. Los destinatarios deben contar con el software de PGP (para Windows o Mac OS X).
- **Frase de contraseña.** Encripta el archivo con una frase de contraseña que debe darse a conocer a los destinatarios. Los destinatarios deben contar con el software de PGP (para Windows o Mac OS X).
- **Archivo de desencryptado automático de PGP.** Encripta el archivo con una frase de contraseña. No es necesario que los destinatarios utilicen el software de PGP para abrir el archivo, pero la computadora debe tener Microsoft Windows. La frase de contraseña debe darse a conocer a los destinatarios.
- **Sólo firma.** Firma el archivo, pero no lo encripta, lo que le permite demostrar que usted es el remitente. Los destinatarios deben contar con el software de PGP (para Windows o Mac OS X) para abrir y verificar el archivo.

Los tipos de archivos de PGP Zip de sólo firma y frase de contraseña se describen detalladamente en la *Guía del usuario de PGP Desktop*; aquí se describen brevemente.

- 1 Haga clic en **Nuevo PGP Zip**, en el cuadro de control de PGP Zip.



- 2 Arrastre y coloque los archivos y las carpetas que desea ubicar en el archivo, o selecciónelos con los botones.
- 3 Seleccione **Enviar los archivos originales a PGP Shredder cuando haya finalizado** si desea que los

archivos y las carpetas originales que puso en el archivo se trituren una vez creado el archivo.

- 4 Haga clic en **Siguiente**.
- 5 Seleccione el tipo de archivo de PGP Zip que desea:
 - **Llaves de destinatario**
 - **Frase de contraseña**
 - **Archivo de desencriptado automático de PGP**
 - **Sólo firma**
- 6 Haga clic en **Siguiente**.

Los archivos de **Frase de contraseña** y **Sólo firma** se describen detalladamente en la *Guía del usuario de PGP Desktop*.

Consulte la sección adecuada en las siguientes páginas para el tipo de archivo de PGP Zip que especificó.

Llaves de destinatario

Se muestra la pantalla Agregar llaves de usuario.

- 1 Haga clic en **Agregar** y utilice la pantalla Selección de usuario para seleccionar las llaves públicas de aquellas personas que usted quiera que tengan permiso para abrir el archivo. Si desea poder abrir el archivo usted mismo, asegúrese de incluir su llave pública.
- 2 Haga clic en **Siguiente**.
- 3 Elija una llave privada del sistema local que se utiliza para firmar el archivo.
- 4 Especifique un nombre y una ubicación para el archivo. El nombre predeterminado es el nombre del primer archivo o carpeta del archivo. La ubicación predeterminada es la de los archivos y las carpetas que se colocan en el archivo.
- 5 Haga clic en **Siguiente**. Se crea el archivo de PGP Zip. La pantalla Finalizado muestra información sobre el nuevo archivo.
- 6 Haga clic en **Finalizar**.

Nota: el tipo de frase de contraseña de archivo de PGP Zip es muy similar a las llaves de destinatario; la diferencia es que para proteger el archivo se utiliza una contraseña en lugar de una llave.

Nota: el tipo de sólo firma del archivo de PGP Zip es similar a las llaves de destinatario; la diferencia es que debido a que el archivo solamente está firmado y no encriptado, no debe seleccionar las llaves públicas.

Archivo de desencriptado automático de PGP

Se muestra la pantalla Crear una contraseña.

- 1 Escriba una contraseña para el archivo de desencriptado automático (SDA) de PGP Zip y vuelva a escribirla para confirmarla.
- 2 Haga clic en **Siguiente**.
- 3 Elija una llave privada del sistema local que se utiliza para firmar el archivo.

- 4 Especifique un nombre y una ubicación para el archivo. El nombre predeterminado es el nombre del primer archivo o carpeta del archivo. La ubicación predeterminada es la de los archivos y las carpetas que se colocan en el archivo.
- 5 Haga clic en **Siguiente**. Se crea el PGP SDA.
- 6 Haga clic en **Finalizar**.

Utilización de PGP Shred para triturar archivos

La función PGP Shredder destruye archivos y carpetas por completo para que ni siquiera los software de recuperación de archivos más sofisticados puedan recuperarlos. Si bien los iconos de PGP Shredder y de la papelera de reciclaje de Windows aparecen en su escritorio, sólo PGP Shredder sobrescribe inmediatamente los archivos que usted especifica para que no puedan recuperarse.

Puede triturar archivos con cualquiera de los siguientes métodos:

- Mediante el icono de PGP Shredder.
- Mediante la barra de herramientas de PGP.
- Mediante el menú de acceso directo de PGP.

Trituración de archivos mediante el icono de PGP Shredder

Para triturar archivos con el icono de PGP Shredder

- 1 En el escritorio de Windows, arrastre los archivos y las carpetas que desee triturar a PGP Shredder. Aparece un cuadro de diálogo preguntándole si desea triturar los archivos.
- 2 Haga clic en **Sí**. Se trituran los archivos y las carpetas especificados.



Trituración de archivos con la barra de herramientas de PGP

Para triturar archivos con la barra de herramientas de PGP

- 1 En la ventana de la aplicación principal de PGP NetShare, seleccione **Herramientas > Triturar archivos**. Aparecerá el cuadro de diálogo Abrir.
- 2 Seleccione los archivos del sistema que desea triturar y luego haga clic en **Abrir**. Aparece un cuadro de diálogo de confirmación en el que se le solicita que confirme que desea triturar (eliminación segura) los archivos o las carpetas de la lista.

- 3 Haga clic en **Sí**. Los archivos se eliminan de forma segura del sistema.

Trituración de archivos con el menú de acceso directo de PGP Shredder

Para triturar archivos en el Explorador de Windows

- 1 En el Explorador de Windows, haga clic con el botón secundario en los archivos o las carpetas que desea triturar. Aparece un cuadro de diálogo de confirmación en el que se le solicita que confirme que desea triturar (eliminación segura) los archivos o las carpetas de la lista.
- 2 Haga clic en **Sí**. Los archivos se eliminan de forma segura del sistema.

Nota: si no utiliza la función PGP Shredder con frecuencia, puede quitar el icono de PGP Shredder del escritorio mediante las Opciones de PGP. Para hacer esto, seleccione **Herramientas > Opciones**, seleccione la ficha Disco, desactive la opción **Colocar el icono de PGP Shredder en el escritorio** y haga clic en **Aceptar**.

Nota: también puede utilizar las Opciones de PGP para controlar la cantidad de pasos realizados al triturar (mientras más pasos se hagan, más seguro es, pero lleva más tiempo), para determinar si se van a triturar los archivos de la papelera de reciclaje de Windows al vaciarla y si se va a mostrar el cuadro de diálogo de advertencia al realizar la trituración.

Trituración del espacio libre

La función Espacio libre de PGP Shred tritura el espacio libre de las unidades por completo para que los datos eliminados no sean recuperables realmente. Tenga en cuenta que el término “espacio libre”, en realidad, es un nombre poco adecuado. La función Espacio libre de PGP Shred sobrescribe las partes del disco duro que Windows indica que están vacías. De hecho, ese espacio podría estar vacío o podría contener archivos que Windows informó que han sido eliminados.

Cuando se colocan los archivos en la papelera de reciclaje de Windows y ésta se vacía, no se eliminan realmente. Windows actúa como si no hubiera nada allí y eventualmente los sobrescribe. Hasta que no se sobrescriban esos archivos, un atacante puede recuperarlos fácilmente. La función Espacio libre de PGP Shred sobrescribe el “espacio libre” para que los archivos ni siquiera puedan recuperarse con un software de recuperación del disco.

Para triturar espacio libre en los discos

- 1 Abra PGP NetShare.
- 2 Seleccione **Herramientas > Espacio libre de PGP Shred**.
- 3 En la pantalla Introducción, lea la información y haga clic en **Siguiente**.
- 4 En el campo **Triturar unidad** de la pantalla Recopilando información, seleccione el disco o el volumen que desea

triturar, y la cantidad de pasos que desea que el espacio libre de PGP Shred realice.

Las pautas recomendadas para los pasos son:

- 3 pasos para uso personal.
 - 10 pasos para uso comercial.
 - 18 pasos para uso militar.
 - 26 pasos para máxima seguridad.
- 5 Elija **Borrar estructuras de datos internos de NTFS** (no está disponible en todos los sistemas) y haga clic en **Siguiente**.
Esta opción tritura archivos pequeños (con menos de 1 K) en estructuras de datos internos que, de lo contrario, no podrían triturarse.
 - 6 En la pantalla Realizar trituración, haga clic en **Comenzar trituración**.

Nota: haga clic en **Programación** para programar una trituración del espacio libre en lugar de hacerla ahora. El Programador de tareas de Windows debe estar instalado en el sistema.

La duración de la sesión de trituración depende de la cantidad de pasos especificados, de la velocidad del procesador, de la cantidad de aplicaciones que se están ejecutando, etcétera.

- 7 Cuando la sesión de trituración se haya completado, haga clic en **Siguiente**.
- 8 En la pantalla de finalización, haga clic en **Finalizar**.

Soporte técnico

El soporte técnico de Symantec tienen centros de soporte técnico en todo el mundo. La tarea principal del soporte técnico es responder las consultas específicas sobre la funcionalidad y las características del producto. El grupo de soporte técnico también crea contenido para la Base de conocimientos en línea. El grupo de soporte técnico trabaja en forma conjunta con otras áreas funcionales de Symantec para responder preguntas oportunamente. Por ejemplo, el grupo de soporte técnico trabaja junto a Product Engineering y Symantec Security Response para proporcionar servicios de alerta y actualizaciones de definición de virus.

El soporte técnico de Symantec incluye lo siguiente:

- Una variedad de opciones de soporte técnico que ofrecen la posibilidad de seleccionar la cantidad de servicios adecuada para cualquier tipo de organización
- Soporte telefónico o basado en la red que proporciona respuestas rápidas e información actualizada
- Garantía de actualización que proporciona actualizaciones de software
- Soporte técnico global adquirido durante el horario comercial según hora local o las 24 horas del día, los 7 días de la semana

- Ofertas de servicio de primera calidad que incluyen Servicios de Administración de Cuentas

Para obtener información sobre las ofertas de soporte técnico de Symantec, puede visitar nuestro sitio web en la siguiente URL:

www.symantec.com/business/support/

Se proporcionarán todos los servicios de soporte técnico conforme al acuerdo de soporte técnico y la política de soporte técnico de la empresa que esté vigente en ese momento.

Cómo comunicarse con el soporte técnico

Los clientes con un acuerdo de soporte vigente pueden tener acceso a la información de soporte técnico en la siguiente URL:

www.symantec.com/business/support/

Antes de ponerse en contacto con el soporte técnico, asegúrese de cumplir con los requisitos del sistema enumerados en la documentación del producto. Además, debe estar frente a la computadora que tiene problemas, en caso de que sea necesario replicar el problema.

Cuando se comunique con el soporte técnico, deberá tener a su alcance la siguiente información:

- Nivel de lanzamiento de producto
- Información de hardware
- Memoria disponible, espacio en disco e información de NIC (tarjeta de interfaz de red)
- Sistema operativo
- Versión y nivel de parche
- Topología de red
- Información del enrutador, de la puerta de enlace y de la dirección IP
- Descripción del problema:
 - Mensajes de error y archivos de registro
 - Solución de problemas que se ejecutó antes de ponerse en contacto con Symantec
 - Cambios de software recientes y cambios de red

Licencia y registro

Si el producto Symantec requiere un registro o clave de licencia, ingrese a la página web de soporte técnico en la siguiente URL:

www.symantec.com/business/support/

Servicio de atención al cliente

La información de servicio de atención al cliente está disponible en la siguiente URL:

www.symantec.com/business/support/

El servicio de atención al cliente está disponible para resolver las inquietudes que no son técnicas, como los siguientes tipos de problemas:

- Preguntas relacionadas con las licencias o los números de serie de los productos
- Actualizaciones de registro de productos, como cambios de dirección o nombre
- Información general del producto (características, disponibilidad de idioma, distribuidores locales)
- Información más reciente sobre las mejoras y las actualizaciones del producto
- Información sobre los contratos de soporte técnico y garantías de actualización
- Información sobre Symantec Buying Programs
- Asesoramiento sobre las opciones de soporte técnico de Symantec
- Inquietudes de preventa que no sean técnicas
- Problemas relacionados con los CD-ROM o manuales

Recursos del acuerdo de soporte técnico

Si desea ponerse en contacto con Symantec por un acuerdo de soporte técnico actual, comuníquese con el equipo de administración de acuerdos de soporte técnico de su región:

Pacífico Asiático y Japón customercare_apac@symantec.com

Europa, Oriente Medio, África semea@symantec.com

América del Norte, Latinoamérica supportsolutions@symantec.com

Derechos de autor y marcas comerciales

Copyright (c) 2011 Symantec Corporation. Todos los derechos reservados. Symantec, el logotipo de Symantec, PGP, Pretty Good Privacy y el logotipo de PGP son marcas comerciales o marcas comerciales registradas de Symantec Corporation o sus afiliadas en los Estados Unidos y en el resto de los países. Los demás nombres pueden ser marcas comerciales de sus respectivos dueños.