Guard

Guía del usuario

Guard: Guía del usuario

fecha de publicación Martes, 12. Julio 2016 Version 2.4.2

Tabla de contenidos

1 Acerca de esta documentación

La siguiente información le ayudará a hacer un mejor uso de la documentación.

¿Cuál es el público objetivo de esta documentación?

Esta documentación se dirige a usuarios que quieren usar encriptado para proteger su comunicación por correo electrónico y sus ficheros contra accesos no autorizados.

¿Qué contenidos se incluyen en la documentación?

Esta documentación incluye la siguiente información:

- En *¿Para qué sirve Guard?* encontrará una breve descripción de Guard.
- En *Utilización del Guard* encontrará instrucciones de uso de Guard.

Esta documentación describe el trabajo con una instalación y configuración típicas del software colaborativo. La versión y configuración instaladas en su caso podrían ser diferentes de lo aquí descrito.

Ayuda adicional

Se puede encontrar documentación exhaustiva sobre el software colaborativo en la Software colaborativo Guía del Usuario.

2 ¿Para qué sirve Guard?

Guard es un componente de seguridad del software colaborativo que permite cifrar correos electrónicos y ficheros.

- Cifre sus comunicaciones por correo con otros usuarios o colaboradores externos.
- Cifre ficheros individuales. Comparta los datos cifrados con otros usuarios.
- Utilice las opciones de seguridad para definir el nivel de cifrado.
- Los datos cifrados están protegidos por contraseña. Utilice la función de restablecimiento de contraseña para protegerse de las consecuencias de una pérdida de la contraseña.

3 Utilización del Guard

Aprenda a trabajar con la aplicación *Guard*.

- aplicar ajustes básicos
- cifrar Comunicaciones por correo electrónico
- cifrar ficheros
- aplicar ajustes de seguridad

3.1 Configuración de *Guard*

Antes de habilitar el uso del *Guard*, hay que hacer algunas configuraciones básicas.

- En primer lugar se tiene que introducir una contraseña de seguridad de Guard que se usará para cifrar los datos y acceder a los datos ya cifrados.
- Introduzca una dirección de correo secundaria que se usará si olvida su contraseña de seguridad de Guard. En este caso, utilice la función para restablecer la contraseña de seguridad de Guard. Se le enviará una nueva contraseña. Por razones de seguridad, se recomienda introducir una dirección de correo secundaria para este propósito. De lo contrario, la nueva contraseña se enviará a su cuenta de correo principal.

Dispone de dos opciones para hacer los ajustes básicos:

- Definir los ajustes básicos mientras utiliza por primera vez una función de cifrado.
- Definir los ajustes básicos en la página de ajustes del software colaborativo antes de usar la función de cifrado.

Cómo definir los ajustes básicos cuando se usa una función de cifrado por primera vez:

1. Active la función de cifrado cuando redacte un correo, cifre un fichero o suba un nuevo fichero, pulsando en el icono **Cifrar** que hay junto al nombre de carpeta en el árbol de carpetas.
2. De manera consecutiva se le pedirá que indique una contraseña de seguridad de Guard y una dirección de correo secundaria. Indique los datos.

Cómo definir los ajustes básicos antes de usar un cifrado por primera vez:

1. Pulse el icono **Menú del sistema** situado en la parte derecha de la barra de menús. Pulse el elemento del menú **Configuración**.
2. Pulse en **Seguridad de Guard** en la barra lateral.

   Al abrir por primera vez los ajustes de seguridad de Guard, se abre la ventana *Crear claves de seguridad de Guard*.
3. En el campo **Contraseña**, introduzca la contraseña que desea usar para cifrar sus datos.

   Confirme la contraseña en el campo **Verificar** introduciéndola de nuevo.
4. En el campo **Introduzca nuevo correo electrónico secundario**, introduzca la dirección de correo que usará para recibir una contraseña provisional para reiniciar su contraseña de seguridad de Guard.
5. Pulse en **Aceptar**.

3.2 Cifrado de conversaciones de correo electrónico

Existen las siguientes opciones:

- Lectura de correos cifrados
- Envío de correos cifrados
- ¿Cómo pueden leer un correo electrónico cifrado los destinatarios externos?

3.2.1 Lectura de correos cifrados

Para poder leer un correo cifrado, se requiere al menos la contraseña de seguridad de Guard. El remitente de un correo cifrado puede proteger dicho correo con una contraseña adicional.

Cómo leer un correo cifrado:

1. Seleccione un correo que tenga el icono *Cifrado* . En la vista de detalle se muestra el aviso *Correo seguro. Introduzca su contraseña de Guard.*.

   Nota: Si, tras haber usado la última vez Guard, se configuró que Guard debía recordar la contraseña de seguridad, el correo se muestra inmediatamente dependiendo de la configuración.
2. Indique la contraseña de seguridad de Guard.

   Se puede definir por cuánto tiempo debe recordar la contraseña de seguridad Guard. Para ello, marque Seguir conectado a **Guard** . Seleccione un valor de la lista.
3. Pulse en **Aceptar**. El contenido se muestra en texto sencillo.

   Si el correo incluye adjuntos, se muestran las funciones para usar las versiones cifradas o descifradas de dichos adjuntos.

Nota: Sólo puede responder a este correo o reenviarlo cuando utilice un correo cifrado.

3.2.2 Envío de correos cifrados

Existen las siguientes opciones:

- Envío de un coreo cifrado. Sólo usted y los destinatarios pueden leer el contenido del correo electrónico.

  Aviso: Cuando envíe un borrador de correo cifrado, el borrador será eliminado de la carpeta *Borradores* cuando se envíe.
- Envío de un correo con una firma. La firma asegura que el destinatario podrá saber si el contenido del correo se ha modificado durante el transporte.
- Envío de un correo cifrado con firma.

Cómo enviar un correo cifrado:

1. Redacte un correo en la aplicación *Correo electrónico* como de costumbre.

   En la página *Redacta*, pulse el icono **Cifrar** de la parte superior derecha.

   También puede pulsar en **Seguridad** debajo del asunto. Marque **Cifrar**.

   Los iconos que están junto a los destinatarios indican si el mensaje se puede cifrar para este destinatario. Si pasa el cursor sobre un icono, se mostrará una descripción.

2. Para mostrar opciones adicionales, pulse en **Seguridad**. Puede usar las siguientes opciones:

   Para, además, firmar el correo, marque **Firmar**.

   En caso de que el cliente de correo electrónico del destinatario no admita PGP, pero el mensaje deba ser legible, marque **PGP incrustado**. Si utiliza esta opción, no puede enviar correos en formato HTML.

   Para permitir al destinatario del correo enviar una respuestas cifrada, el destinatario tiene que tener nuestra clave pública. Puede enviar su clave pública como adjunto. Para ello, marque **Adjuntar mi clave**.

3. Pulse en **Enviar cifrado**.

   Cuando se envía a destinatarios externos, se muestra una ventana que permite enviar notas para la apertura del correo cifrado [12] para los destinatarios externos.

   Cuando envía por primera vez un correo electrónico cifrado a un destinatario externo, este recibe un adjunto al correo electrónico con su clave pública.

3.2.3 ¿Cómo pueden leer un correo electrónico cifrado los destinatarios externos?

También puede enviar correos cifrados a los destinatarios externos que no son usuarios del software colaborativo. Al añadir un destinatario externo, Guard comprueba si hay disponible una clave pública para dicho destinatario. Dependiendo del resultado, Guard utiliza diferentes procedimientos para enviar el correo cifrado.

- Si hay una clave pública para el destinatario:
  - El mensaje se envía cifrado con esta clave. El destinatario puede leer el mensaje con su clave privada.
  - Para activar la posibilidad de que el destinatario pueda enviar una respuesta cifrada, su clave pública se envía como adjunto. El adjunto se denomina public.asc. El destinatario puede importar esta clave a su cliente de correo electrónico.
- Si no hay clave pública para el destinatario:
  - Si el usuario externo ya tiene una cuenta de invitado, recibirá un correo con el enlace a la página de inicio de sesión de su cuenta de invitado. Cuando inicie la sesión, puede leer el correo cifrado en la página de invitado. Puede enviar una respuesta cifrada desde dicha página.
  - Si no hay una cuenta de invitado, se creará una cuenta de invitado. El destinatario externo recibe un correo con unas pautas y una contraseña creada automáticamente. Además recibirá un correo adicional con el enlace a la página de invitado. En la página de invitado inicia sesión con la contraseña creada automáticamente. En ese momento ya podrá crear una contraseña propia.
  - Dependiendo de la configuración del software colaborativo, los correos de la cuenta de invitado se borran después de un número determinado de días. Para seguir disponiendo de dichos correos, el correo con el enlace a la página de invitado contiene un adjunto con el correo cifrado. El adjunto se denomina encrypted.asc. Dicho adjunto se puede cargar y leer en la página de invitado.

3.3 Cifrado de ficheros

Existen las siguientes opciones:

- Cifrado de ficheros
- Creación de nuevos ficheros cifrados
- Apertura de ficheros cifrados
- Descarga de ficheros cifrados
- Descifrado de ficheros

3.3.1 Cifrado de ficheros

Cuando se cifra un fichero, sólo se cifrará la última versión. El resto de versiones serán eliminadas.

Cómo cifrar un fichero:

Aviso: Cuando se cifra un fichero, todas las versiones de dicho fichero serán borradas excepto la actual. Si necesita mantener una versión anterior, guárdela antes de cifrar el fichero.

1. Seleccione uno o varios ficheros en la aplicación *Ficheros*. Pulse el icono **Acciones** de la barra de herramientas. Pulse en **Cifrar** en el menú.

   También puede usar el icono **Acciones** de la parte derecha de la barra de categorías. Pulse **Cifrar** en el menú.

2. Si el fichero contiene múltiples versiones, se mostrará la ventana *Cifrar ficheros*. Confirme que desea cifrar el fichero y borrar las versiones anteriores pulsando en **Aceptar**.

   Si el fichero contiene una única versión, se cifra sin más preguntas.

3.3.2 Creación de nuevos ficheros cifrados

Puede crear un fichero cifrado nuevo mediante la subida de un fichero local con cifrado.

Cómo crear un nuevo fichero cifrado:

1. En la aplicación *Ficheros*, seleccione una carpeta en el árbol de carpetas.

   Nota: Abra una carpeta en la que tenga los permisos adecuados para crear objetos.

2. Pulse en **Nuevo** en la barra de herramientas. Pulse en **Añadir y cifrar fichero local**.

3. Seleccione uno o varios ficheros en la ventana *Subir fichero*.

   Pulse sobre **Abrir**. El área de visualización mostrará el estado del progreso actual.

   Para cancelar el proceso, pulse en **Detalles del fichero** en la parte inferior derecha del área de visualización. Pulse en **Cancelar** junto al nombre de un fichero en la ventana *Progreso de la carga*.

Consejo: También se puede crear un nuevo fichero cifrado arrastrándolo desde su escritorio hasta la ventana de la aplicación *Ficheros* y soltándolo allí, en la parte superior.

3.3.3 Apertura de ficheros cifrados

Puede abrir y leer un fichero cifrado. El fichero permanece cifrado en el servidor.

Cómo abrir un fichero cifrado:

1. En la aplicación *Ficheros*, seleccione un fichero cifrado del área de visualización. Pulse en el icono **Ver** de la barra de herramientas.
2. Se abre la ventana *Indicar la contraseña de seguridad de Guard*. Indique la contraseña de seguridad de Guard.

   Puede configurar por cuánto tiempo se debe recordar la contraseña de seguridad de Guard. Para ello, marque **Recordar contraseña**. Seleccione un valor de la lista.

   Pulse en **Aceptar**.

3.3.4 Descarga de ficheros cifrados

Puede descargar un fichero cifrado para leerlo o editarlo en local. El fichero permanecerá cifrado en el servidor.

Cómo descargar un fichero cifrado:

1. En la aplicación *Ficheros*, seleccione un fichero cifrado en el área de visualización. Pulse el icono **Ver** de la barra de herramientas.

   Nota: Si en vez de ello pulsa en **Descargar** en la ventana emergente, la descarga del fichero permanecerá cifrada.
2. Se abre la ventana *Indicar la contraseña de seguridad de Guard*. Indique la contraseña de seguridad de Guard.

   Puede configurar por cuánto tiempo se debe recordar la contraseña de seguridad de Guard. Para ello, marque **Recordar contraseña**. Seleccione un valor de la lista.

   Pulse en **Aceptar**.
3. Pulse el icono **Acciones** en el visor. Pulse en **Descargar descifrado**.

3.3.5 Descifrado de ficheros

Puede eliminar el cifrado de un fichero descifrándolo.

Cómo descifrar un fichero:

1. En la aplicación *Ficheros*, seleccione un fichero cifrado en el área de visualización. Pulse en el icono **Acciones** de la barra de herramientas. Pulse en **Eliminar cifrado** en el menú.
2. Se abre la ventana *Indicar la contraseña de seguridad de Guard*. Indique la contraseña de seguridad de Guard.

   Puede configurar por cuánto tiempo debería ser válida la contraseña de seguridad de Guard. Para ello, marque **Recordar contraseña**. Seleccione un valor de la lista.

   Pulse en **Aceptar**.

3.4 Cerrar la sesión de Guard

Puede cerrar la sesión de Guard sin cerrar el software colaborativo. Para abrir posteriormente un correo, fichero o carpeta cifrados, tendrá que introducir la contraseña de seguridad de Guard de nuevo.
Nota: Esta función solo está disponible si marca **Recordar contraseña** al abrir un correo o un fichero cifrados.

Cómo cerrar la sesión de Guard:

1. Pulse el icono **Menú de sistema** situado a la derecha de la barra de menú.
2. Pulse **Cerrar sesión de Guard** en el menú.

3.5 Ajustes de Guard

Existen las siguientes opciones:

- Para gestionar su contraseña de seguridad de Guard, use los ajustes de seguridad de Guard.
- Para cambiar los ajustes predeterminados para el envío de correos seguros, utilice los Ajustes de cifrado PGP.
- Puede administrar sus claves PGP.

3.5.1 Ajustes de seguridad de Guard

Existen las siguientes opciones:

- cambiar la contraseña de seguridad de Guard
- Si se ha perdido la contraseña de seguridad de Guard, se puede solicitar una contraseña de seguridad provisional de Guard reiniciándo la contraseña de seguridad de Guard.
- cambiar la dirección de correo secundaria

Cómo cambiar la contraseña de seguridad de Guard

1. Pulse el icono **Menú de sistema** situado a la derecha de la barra de menús. Pulse el elemento del menú **Configuración**.
2. En la barra lateral, pulse en Seguridad de **Guard**.
3. En el campo **Introduzca contraseña de seguridad actual de Guard** situado debajo de *Contraseña*, introduzca la contraseña que ha estado utilizando hasta ahora para cifrar sus datos.

   En el campo **Introduzca nueva contraseña de seguridad de Guard**, introduzca la contraseña que quiere utilizar para cifrar sus datos de ahora en adelante.

   Confirme la contraseña en el campo the password in the **Verifique la nueva contraseña de seguridad de Guard** escribiéndola otra vez.
4. Pulse en **Cambiar contraseña de seguridad de Guard**.

Cómo reiniciar la contraseña de seguridad de Guard:

1. Pulse en el icono **Menú del sistema** de la parte derecha de la barra de menús. Pulse en el elemento del menú **Configuración**.
2. En la barra lateral, pulse en Seguridad de **Guard**.
3. Pulse en **Reiniciar contraseña de seguridad de Guard**. Se le enviará una contraseña nueva a su cuenta de correo secundaria.

   Si no se ha indicado una dirección de correo secundaria, la nueva contraseña se le enviará a su dirección de correo principal.
4. Esta nueva contraseña es ahora su contraseña de seguridad actual de Guard. Debería cambiarla inmediatamente.

Cómo cambiar su dirección de correo secundaria para el restablecimiento de la contraseña de cifrado:

1. Pulse el icono **Menú del sistema** situado a la derecha de la barra de menús. Pulse en el elemento del menú **Configuración**.
2. En la barra lateral, pulse en Seguridad de **Guard**.
3. Introduzca la contraseña para cifrar sus datos en el campo **Introduzca contraseña de seguridad actual de Guard**, debajo de *Correo secundario*.

   En el campo **Introduzca nuevo correo electrónico secundario**, introduzca la dirección de correo que usará para recibir una contraseña provisional para reiniciar su contraseña de seguridad de Guard.

   Pulse en **Cambiar correo**.

3.5.2 Ajustes de cifrado PGP

Los ajustes de cifrado PGP definen los ajustes preestablecidos que están disponibles al redactar correos. Al redactar un correo nuevo, los ajustes predeterminados se pueden modificar antes de enviar el correo.

Cómo cambiar los ajustes de cifrado PGP:

1. Pulse el icono **Menú del sistema** situado en la parte derecha de la barra de menús. Pulse el elemento del menú **Configuración**.
2. Seleccione el elemento Seguridad de **Guard** en la barra lateral. Pulse en **Ajustes avanzados**.
3. Cambie un ajuste debajo de *Ajustes de cifrado PGP*.

Están disponibles los siguientes ajustes.

De manera predeterminada, enviar cifrado al redactar un correo electrónico

Determina si un correo nuevo se cifra con PGP de manera predeterminada.

De manera predeterminada, añadir firma a correos salientes

Determina si un correo nuevo se cifra con PGP de manera predeterminada.

Activar características avanzadas de PGP

Determina si se muestran las características PGP, tales como la gestión de claves.

PGP ajustado inicialmente a PGP incrustado en nuevos correos

Para mostrar este ajuste, marque la casilla de verificación **Activar características avanzadas de PGP**.
Determina si el cifrado PGP va incrustado. Utilice estos ajustes solo si el cliente de correo de alguno de los destinatarios no admite PGP y el mensaje debería ser legible a pesar de ello. Si se utiliza este ajuste, no se pueden enviar correos en formato html.

3.5.3 Administración de claves

Para enviar o recibir mensajes cifrados no suelen ser necesarias las funciones de administración de claves. Aún así, dichas funciones pueden ser necesarias en los siguientes casos:

- Quiere usar sus claves PGP de Guard en otros clientes de correo, por ejemplo en clientes locales.
- Tiene claves PGP de otras aplicaciones PGP. Quiere usar dichas claves en Guard.
- Tiene la clave pública de un colaborador externo. Para leer mensajes cifrados de dicho colaborador sin tener que acceder a un servidor de claves, querrá importar la clave pública del colaborador en Guard.
- Quiere proporcionar su clave pública a un destinatario para darle acceso de lectura a sus mensajes cifrados sin necesidad de acceder a un servidor de claves.

Cómo abrir la página para administrar sus claves:

1. Pulse el icono **Menú del sistema** situado en la parte derecha de la barra de menús. Pulse el elemento del menú **Configuración**.
2. Seleccione el elemento **Seguridad de Guard** en la barra lateral. Pulse en **Ajustes avanzados**.
   Marque **Activar características avanzadas de PGP**.

La página contiene los siguientes elementos.

- Opciones para definir los ajustes predeterminados de Guard
- Sección *Sus claves*. Contiene funciones para administrar sus claves PGP privadas y públicas.
  Sus claves públicas ya existentes se mostrarán debajo de *Su lista de claves*. La lista de claves contiene dos claves:
  - Una clave maestra. Entre otras cosas, esta clave se utiliza para firmar sus correos.
  - Una subclave. Esta clave se utiliza para cifrar y descifrar correos y ficheros.

  La diferencia entre la clave maestra y la subclave es una de las características de la tecnología de cifrado PGP. Cada clave maestra y cada subclave contienen una clave pública y una clave privada. Dependiendo de las necesidades, Guard utiliza automáticamente la clave correspondiente.
- Sección *Claves públicas*. Muestra las claves públicas compartidas por usted o por otros usuarios. Si la clave pública de un usuario aparece en esta lista, puede asumir que dicho usuario puede descifrar los correos cifrados que usted le envíe.

Están disponibles las siguientes funciones:

- descargar su clave pública
- enviar su clave pública por correo
- añadir nuevas claves a las ya existentes subiendo claves locales o nuevas claves de Guard
- convertir una clave en la clave actual
- mostrar detalles de una clave
- borrar una clave
- descargar su clave privada
- añadir una cuenta de correo adicional a una clave
- subir una clave pública de un colaborador externo

Cómo descargar su clave pública:

1. En los ajustes, abra la página para administrar las claves.
2. Pulse en **Descargar clave pública PGP** debajo de *Sus claves*.

Cómo enviar su clave pública por correo electrónico:

1. En los ajustes, abra la página para administrar las claves.
2. Pulse en **Enviar su clave pública PGP por correo electrónico** debajo de *Sus claves*.

Cómo añadir una nueva clave a sus claves:

1. En los ajustes, abra la página para administrar las claves.
2. Pulse el icono **Añadir** + situado junto a *Su lista de claves* que hay debajo de *Sus claves*. Se abrirá la ventana *Adición de claves*.
3. Tiene las siguientes posibilidades:
   - Para añadir una clave privada, pulse en **Subir clave privada**. Seleccione un fichero que contenga una clave privada. Se abrirá la ventana *Subir claves privadas*.

     Para subir la clave nueva, introduzca su contraseña de seguridad de Guard. Indique una nueva contraseña para la clave nueva.
   - Para añadir una clave pública, pulse en **Subir solo una clave pública**. Seleccione un fichero que contenga una clave pública.
   - Para crear un nuevo par de claves, pulse en **Crear nuevas claves**. Se abre la ventana *Crear claves de seguridad de Guard*.

     Introduzca una contraseña para la nueva clave. Confirme la contraseña.

     La nueva clave consiste en una clave maestra y su correspondiente subclave.

   La nueva clave se introducirá en la parte superior de su lista de claves. La nueva clave se convierte en la clave actual.

Cómo hacer de una clave la actual:

Puede usar esta función si su lista de claves contiene más de una clave maestra y subclave. Desde ese momento, la clave actual se utilizará para el cifrado.

1. En los ajustes, abra la página para administrar las claves.
2. Debajo de *Su lista de claves*, pulse la casilla de verificación que hay junto a una clave ubicada debajo de **Actual**. Cuando convierta una clave maestra en la clave actual, la correspondiente subclave se marcará como actual también y viceversa.

Cómo mostrar los detalles de una clave:

Puede obtener los detalles de las claves. Los detalles de una clave son especialmente importantes para los usuarios con conocimientos de PGP.

1. En los ajustes, abra la página para administrar las claves.
2. Pulse el icono **Detalles** que hay en la parte derecha de la barra de categorías. Se abre la ventana *Detalles de clave*. Para ver las firmas de la clave, pulse en **Firmas**.

Cómo borrar una clave:

1. En los ajustes, abra la página para administrar las claves.
2. Pulse el icono **Borrar** de la parte derecha de la barra de categorías. Se abrirá la ventana *Borrar clave privada*.
3. Dispone de las siguientes opciones:
   - Para revocar una clave privada, pulse en **Revocar**.

     Introduzca la contraseña de la clave privada. Si es necesario, seleccione una razón para revocar la clave.

     Pulse en **Revocar**.
   - Para borrar una clave privada, pulse en **Borrar**.

     Introduzca la contraseña de la clave privada.

     Pulse el botón **Borrar**.

   Cuando se borra una clave maestra, se borrará también su correspondiente subclave.

Cómo descargar su clave privada:

Precaución: La descarga de una clave privada en su máquina puede ser un riesgo de seguridad. Asegúrese de que ninguna otra persona puede tener acceso a su clave privada.

1. En los ajustes, abra la página para administrar las claves.
2. Pulse el icono **Descargar** de la parte derecha de la barra de categorías.

Cómo añadir una cuenta de correo adicional a una clave:

Cuando añada IDs de usuario adicionales a una clave, puede utilizar la clave para varias cuentas de correo.

1. En los ajustes, abra la página para administrar las claves.
2. Pulse el icono **Editar** de la parte derecha de la barra de categorías. Se abrirá la ventana *Añadir ID de usuario*.
3. Introduzca un nombre para la ID de usuario. Introduzca la dirección de correo que quiere usar para esta clave.

   Introduzca su contraseña para esta clave.

   Pulse en **Aceptar**.

Cómo subir una clave pública de un colaborador externo:

1. En los ajustes, abra la página para administrar las claves.
2. Pulse el icono **Añadir** + que hay en la parte derecha de la barra de categorías. Seleccione un fichero que contenga una clave pública.

Índice

A

C

D

F

G

R