



Guard

Guía del usuario



Guard: Guía del usuario

fecha de publicación Miércoles, 17. Mayo 2017 Version 2.8.0

Copyright © 2016-2017 OX Software GmbH , La propiedad intelectual de este documento es de OX Software GmbH

El documento se puede copiar en todo o en parte, siempre que cada copia incluya esta nota de copyright. La información contenida en este libro ha sido recopilada con el mayor cuidado. Sin embargo, no se pueden descartar posibles errores. OX Software GmbH, los autores y los traductores, no se responsabilizan de los posibles errores y sus consecuencias. Los nombres de programas y dispositivos utilizados en este libro puede ser marcas registradas, y se utilizan sin garantía de libre uso. Por normal general, OX Software GmbH sigue las convenciones de nomenclatura de los fabricantes. La reproducción en este libro de nombres de marcas, nombres registrados, logos, etc... (incluso sin notaciones especiales) no justifica la asunción de que tales nombres puedan ser considerados libres (respecto a las regulaciones de marcas registradas y nombres de marcas).

Tabla de contenidos

1	Acerca de esta documentación	5
2	¿Para qué sirve Guard?	7
3	Utilización del Guard	9
3.1	Configuración de <i>Guard</i>	10
3.2	Cifrado de conversaciones de correo electrónico	11
3.2.1	Lectura de correos cifrados	11
3.2.2	Cifrado de correos entrantes	12
3.2.3	Envío de correos cifrados	12
3.2.4	¿Cómo pueden leer un correo electrónico cifrado los destinatarios externos?	13
3.3	Cifrado de archivos	14
3.3.1	Cifrado de archivos	14
3.3.2	Creación de nuevos archivos cifrados	15
3.3.3	Apertura de archivos cifrados	15
3.3.4	Descarga de archivos cifrados	16
3.3.5	Descifrado de archivos	16
3.4	Cifrado de documentos de Office	17
3.4.1	Creación de nuevos documentos cifrados	18
3.4.2	Almacenamiento de documentos seleccionados en formato cifrado	18
3.4.3	Apertura de documentos cifrados	19
3.5	Cerrar la sesión de Guard	20
3.6	Ajustes de Guard	21
3.6.1	Ajustes de seguridad de Guard	22
3.6.2	Ajustes de cifrado PGP	23
3.6.3	Administración de claves	24
	Índice	27

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?](#)
- [¿Qué contenidos se incluyen en la documentación?](#)
- [Ayuda adicional](#)

¿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 archivos 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 archivos.

- Cifre sus comunicaciones por correo con otros usuarios o colaboradores externos.
- Cifre archivos 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 [archivos](#)
- cifrar [documentos de Office](#)
- 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 archivo o suba un nuevo archivo, presionando 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. Presione el icono **Menú del sistema**  situado en la parte derecha de la barra de menús. Presione el elemento del menú **Configuración**.
2. Presione 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. Presione en **Aceptar**.

3.2 Cifrado de conversaciones de correo electrónico

Existen las siguientes opciones:

- [Lectura de correos cifrados](#)
- [Cifrado de correos entrantes](#)
- [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 recordarse la contraseña de seguridad Guard. Para ello, marque Seguir conectado a **Guard**. Seleccione un rango de tiempo de la lista.

En los ajustes de cifrado PGP, puede [definir un valor predeterminado](#) para el rango de tiempo.

3. Presione 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.

Vea también

[Cifrado de correos entrantes \(p. 12\)](#)


[Envío de correos cifrados \(p. 12\)](#)

[¿Cómo pueden leer un correo electrónico cifrado los destinatarios externos? \(p. 13\)](#)

3.2.2 Cifrado de correos entrantes

Puede hacer que se cifren automáticamente todos los correos entrantes.

Cómo cifrar todos los correos entrantes:

1. Presione el icono **Menú del sistema**  situado en la parte derecha de la barra de menús. Presione el elemento del menú **Configuración**.
2. Seleccione el elemento **Seguridad de Guard** en la barra lateral. Presione en **Ajustes avanzados**.
3. Asegúrese de marcar **Activar características avanzadas de PGP**. Marque **Cifrar todos los correos entrantes**.

Vea también

[Lectura de correos cifrados \(p. 11\)](#)

[Envío de correos cifrados \(p. 12\)](#)


[¿Cómo pueden leer un correo electrónico cifrado los destinatarios externos? \(p. 13\)](#)

3.2.3 Envío de correos cifrados

Existen las siguientes opciones:

- Envío de un correo 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*, presione el icono **Cifrar**  de la parte superior derecha.
También puede presionar 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, presione 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 respuesta cifrada, el destinatario tiene que tener nuestra clave pública. Puede enviar su clave pública como adjunto. Para ello, marque **Adjuntar mi clave**.
3. Presione en **Enviar cifrado**.
Cuando se envía a destinatarios externos, se muestra una ventana que permite enviar [notas para la apertura del correo cifrado \[13\]](#) 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.

Vea también

[Lectura de correos cifrados \(p. 11\)](#)

[Cifrado de correos entrantes \(p. 12\)](#)

[¿Cómo pueden leer un correo electrónico cifrado los destinatarios externos? \(p. 13\)](#)

3.2.4 ¿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. El destinatario externo recibe un correo con un enlace a la página de invitado y una contraseña creada automáticamente. El usuario inicia sesión en la página de invitado. En ese momento ya podrá crear una contraseña propia. Dependiendo de la configuración, la contraseña creada automáticamente y el enlace a la página de invitado se enviarán en correos electrónicos separados.
 - 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.

Vea también

- [Lectura de correos cifrados \(p. 11\)](#)
- [Cifrado de correos entrantes \(p. 12\)](#)
- [Envío de correos cifrados \(p. 12\)](#)

3.3 Cifrado de archivos

Existen las siguientes opciones:



- [Cifrado de archivos](#)
- [Creación de nuevos archivos cifrados](#)
- [Apertura de archivos cifrados](#)
- [Descarga de archivos cifrados](#)
- [Descifrado de archivos](#)

3.3.1 Cifrado de archivos

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

Cómo cifrar un archivo:

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

1. Seleccione uno o varios archivos en la aplicación *Ficheros*. Presione el icono **Acciones**  de la barra de herramientas. Presione en **Cifrar** en el menú.
También puede usar el icono **Acciones** . Presione **Cifrar** en el menú.
2. Si el archivo contiene múltiples versiones, se mostrará la ventana *Cifrar archivos*. Confirme que desea cifrar el archivo y borrar las versiones anteriores presionando en **Aceptar**.
Si el archivo contiene una única versión, se cifra sin más preguntas.

Vea también

- [Creación de nuevos archivos cifrados \(p. 15\)](#)
- [Apertura de archivos cifrados \(p. 15\)](#)
- [Descarga de archivos cifrados \(p. 16\)](#)
- [Descifrado de archivos \(p. 16\)](#)

3.3.2 Creación de nuevos archivos cifrados

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

Cómo crear un nuevo archivo 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. Presione en **Nuevo** en la barra de herramientas. Presione en **Añadir y cifrar archivo local**.
3. Seleccione uno o varios archivos en la ventana *Subir archivo*.
Presione sobre **Abrir**. El área de visualización mostrará el estado del progreso actual.
Para cancelar el proceso, presione en **Detalles del archivo** en la parte inferior derecha del área de visualización. Presione en **Cancelar** junto al nombre de un archivo en la ventana *Progreso de la carga*.

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


Vea también

- [Cifrado de archivos \(p. 14\)](#)
- [Apertura de archivos cifrados \(p. 15\)](#)
- [Descarga de archivos cifrados \(p. 16\)](#)
- [Descifrado de archivos \(p. 16\)](#)

3.3.3 Apertura de archivos cifrados

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

Cómo abrir un archivo cifrado:

1. En la aplicación *Ficheros*, seleccione un archivo cifrado del área de visualización. Presione 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 mi contraseña**. Seleccione un valor de la lista.
En los ajustes de cifrado PGP, puede [definir un valor predeterminado](#) para el rango de tiempo.
Presione en **Aceptar**.


Vea también

- [Cifrado de archivos \(p. 14\)](#)
- [Creación de nuevos archivos cifrados \(p. 15\)](#)
- [Descarga de archivos cifrados \(p. 16\)](#)
- [Descifrado de archivos \(p. 16\)](#)

3.3.4 Descarga de archivos cifrados

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

Cómo descargar un archivo cifrado:

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


Nota: Si en vez de ello presiona en **Descargar** en la ventana emergente, la descarga del archivo 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 mi contraseña**. Seleccione un valor de la lista.

En los ajustes de cifrado PGP, puede [definir un valor predeterminado](#) para el rango de tiempo.

Presione en **Aceptar**.

3. Presione el icono **Acciones**  en el visor. Presione en **Descargar descifrado**.

Vea también

[Cifrado de archivos \(p. 14\)](#)

[Creación de nuevos archivos cifrados \(p. 15\)](#)


[Apertura de archivos cifrados \(p. 15\)](#)

[Descifrado de archivos \(p. 16\)](#)

3.3.5 Descifrado de archivos

Puede eliminar el cifrado de un archivo descifrándolo.

Cómo descifrar un archivo:

1. En la aplicación *Ficheros*, seleccione un archivo cifrado en el área de visualización. Presione en el icono **Acciones**  de la barra de herramientas. Presione 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 mi contraseña**. Seleccione un valor de la lista.

En los ajustes de cifrado PGP, puede [definir un valor predeterminado](#) para el rango de tiempo.

Presione en **Aceptar**.

Vea también

[Cifrado de archivos \(p. 14\)](#)

[Creación de nuevos archivos cifrados \(p. 15\)](#)

[Apertura de archivos cifrados \(p. 15\)](#)

[Descarga de archivos cifrados \(p. 16\)](#)

3.4 Cifrado de documentos de Office

Existen las siguientes opciones:

- [Creación de nuevos documentos cifrados](#)
- [Almacenamiento de documentos seleccionados en formato cifrado](#)
- [Apertura de documentos cifrados](#)

Otras opciones disponibles en la aplicación *Ficheros*:

- [cifrar](#) documentos ya existentes
- [descifrar](#) documentos

3.4.1 Creación de nuevos documentos cifrados

Al crear un documento nuevo, se tiene la opción de crear un documento que se guarde cifrado.

Cómo crear un nuevo documento cifrado:

1. Dependiendo de si quiere crear un documento de texto, hoja de cálculo o presentación cifrados, seleccione una de las aplicaciones *Texto*, *Hojas de cálculo* o *Presentaciones*.
2. En la barra de menú de Office, presione en uno de los botones entre **Nuevo documento de texto (cifrado)**, **Nueva hoja de cálculo (cifrada)**, **Nueva presentación (cifrada)**.
3. 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 mi contraseña**. Seleccione un valor de la lista.
En los ajustes de cifrado PGP, puede [definir un valor predeterminado](#) para el rango de tiempo.
Presione en **Aceptar**.

Vea también

[Almacenamiento de documentos seleccionados en formato cifrado \(p. 18\)](#)

[Apertura de documentos cifrados \(p. 19\)](#)

[Cifrado de archivos \(p. 14\)](#)

3.4.2 Almacenamiento de documentos seleccionados en formato cifrado

Cuando se ha abierto un documento de texto, hoja de cálculo o presentación, se puede guardar dicho documento en formato cifrado.

Cómo guardar el documento seleccionado en formato cifrado:

1. Abra un documento en la aplicación *Texto*, *Hojas de cálculo* o *Presentaciones*.
2. En la barra de herramientas **Archivo**, presione en **Guardar en Drive**. Seleccione **Guardar como (cifrado)**.
Se abre la ventana *Guardar como (cifrado)*. Seleccione una carpeta y un nombre de archivo. Presione en **Aceptar**.
3. 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 mi contraseña**. Seleccione un valor de la lista.
En los ajustes de cifrado PGP, puede [definir un valor predeterminado](#) para el rango de tiempo.
Presione en **Aceptar**.

Vea también

[Creación de nuevos documentos cifrados \(p. 18\)](#)

[Apertura de documentos cifrados \(p. 19\)](#)

[Cifrado de archivos \(p. 14\)](#)

3.4.3 Apertura de documentos cifrados

Puede abrir un documento cifrado para hacer lo siguiente:

- leer o editar el documento
- descargar el documento en formato descifrado
- imprimir el documento como pdf en formato descifrado

El documento permanece cifrado en el servidor.



Cómo abrir un documento cifrado:

1. Abra un documento en la aplicación *Texto*, *Hojas de cálculo* o *Presentaciones*.
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 mi contraseña**. Seleccione un valor de la lista.

En los ajustes de cifrado PGP, puede [definir un valor predeterminado](#) para el rango de tiempo.

Presione en **Aceptar**.

3. Puede usar las siguientes funciones:
 - Editar el documento. Se puede encontrar información en la guía del usuario de *Documentos*.
 - Para descargar el documento en formato descifrado, presione el icono **Descargar**  de la barra de herramientas.
 - Para guardar el documento como pdf en formato descifrado, presione el icono **Guardar como pdf** .

Vea también

[Creación de nuevos documentos cifrados \(p. 18\)](#)

[Almacenamiento de documentos seleccionados en formato cifrado \(p. 18\)](#)


[Cifrado de archivos \(p. 14\)](#)

3.5 Cerrar la sesión de Guard

Puede cerrar la sesión de Guard sin cerrar el software colaborativo. Para abrir posteriormente un correo, archivo 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 archivo cifrados.

Cómo cerrar la sesión de Guard:

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

3.6 Ajustes de Guard

Existen las siguientes opciones:


- Para administrar 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](#).

3.6.1 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 [reiniciando](#) la contraseña de seguridad de Guard.
- [cambiar](#) la dirección de correo secundaria


Cómo cambiar la contraseña de seguridad de Guard

1. Presione el icono **Menú de sistema**  situado a la derecha de la barra de menús. Presione el elemento del menú **Configuración**.
2. Presione en **Seguridad de Guard** en la barra lateral.
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. Presione en **Cambiar contraseña de seguridad de Guard**.

Cómo reiniciar la contraseña de seguridad de Guard:

1. Presione en el icono **Menú del sistema**  de la parte derecha de la barra de menús. Presione en el elemento del menú **Configuración**.
2. Presione en **Seguridad de Guard** en la barra lateral.
3. Presione 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. Presione el icono **Menú del sistema**  situado a la derecha de la barra de menús. Presione en el elemento del menú **Configuración**.
2. Presione en **Seguridad de Guard** en la barra lateral.
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.
Presione en **Cambiar correo**.


Vea también

- [Ajustes de cifrado PGP \(p. 23\)](#)
- [Administración de claves \(p. 24\)](#)

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

Están disponibles los siguientes ajustes.

Recordar contraseña de manera predeterminada

Define el rango de tiempo predeterminado durante el que Guard recordará la contraseña. Se puede cambiar este valor predeterminado cuando se le pida su contraseña de Guard.

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 todas las características PGP.

Cifrar todos los correos entrantes

Determina si se cifran todos los correos entrantes con PGP de manera predeterminada.

PGP ajustado inicialmente a PGP incrustado en nuevos correos

Determina si el cifrado PGP se hace incrustado. Utilice este ajuste solo si el cliente de correo de algún destinatario no admite PGP, y aún así el mensaje debe ser legible. Si utiliza esta característica, no puede enviar correos en formato html.

Vea también

[Ajustes de seguridad de Guard \(p. 22\)](#)


[Administración de claves \(p. 24\)](#)

3.6.3 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. Presione el icono **Menú del sistema**  situado en la parte derecha de la barra de menús. Presione el elemento del menú **Configuración**.
2. Seleccione el elemento **Seguridad de Guard** en la barra lateral. Presione 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 archivos.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.
- Las claves caducadas se muestran en rojo.

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 creando 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. Presione 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. Presione 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. Presione 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, presione en **Subir clave privada**. Seleccione un archivo 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, presione en **Subir solo una clave pública**. Seleccione un archivo que contenga una clave pública.
 - Para crear un nuevo par de claves, presione 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*, presione 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. Presione el icono **Detalles** . Se abre la ventana *Detalles de clave*. Para ver las firmas de la clave, presione en **Firmas**.


Cómo borrar una clave:

1. En los ajustes, [abra](#) la página para administrar las claves.
2. Presione el icono **Borrar** . Se abrirá la ventana *Borrar clave privada*.
3. Dispone de las siguientes opciones:
 - Para revocar una clave privada, presione en **Revocar**. Introduzca la contraseña de la clave privada. Si es necesario, seleccione una razón para revocar la clave. Presione en **Revocar**.
 - Para borrar una clave privada, presione en **Borrar**. Introduzca la contraseña de la clave privada. Presione 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. Presione el icono **Descargar**  que hay junto a una clave de la lista de claves privadas que aparecen debajo de *Sus claves*.

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. Presione el icono **Editar** . 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.
Presione en **Aceptar**.

Cómo subir una clave pública de un colaborador externo:

1. En los ajustes, [abra](#) la página para administrar las claves.
2. Presione el icono **Añadir** . Seleccione un archivo que contenga una clave pública.

Vea también

[Ajustes de seguridad de Guard \(p. 22\)](#)
[Ajustes de cifrado PGP \(p. 23\)](#)

Índice

A

- Abrir documentos cifrados, 19
- Ajustes de Guard
 - cambiar la contraseña, 22
 - Restablecer la contraseña, 22
- Ajustes PGP de Guard
 - Activar características avanzadas de PGP, 23
 - Cifrar todos los correos entrantes, 23
 - De manera predeterminada, añadir firma a correos salientes, 23
 - De manera predeterminada, enviar cifrado al redactar un correo electrónico, 23
 - PGP ajustado inicialmente a PGP incrustado en nuevos correos, 23
 - Recordar contraseña de manera predeterminada, 23
- Almacenamiento de documentos seleccionados en formato cifrado, 18
- Apertura de archivos cifrados, 15
- Archivos cifrados
 - abrir, 15
 - descargar, 16
 - descifrar, 16

C

- Cambiar la contraseña, 22
- Cerrar la sesión
 - cambiar la contraseña, 20
- Cifrado de archivos, 14
- Cifrar
 - Almacenamiento de documentos seleccionados en formato cifrado, 18
 - Archivos, 14
 - cifrar documentos de Office, 17
 - Conversación de correo electrónico, 11
 - crear nuevo documento cifrado, 18
 - crear nuevos archivos cifrados, 15
- Cifrar conversaciones de correo electrónico, 11
- Cifrar documentos de Office, 17
- Correos cifrados
 - acceso para destinatarios externos, 13
 - bloquear, 12
 - cifrar entrantes, 12
 - enviar, 12
 - leer, 11
- Crear nuevos archivos cifrados, 15
- Crear nuevos documentos cifrados, 18

D

- Descarga de archivos cifrados, 16
- Descifrar archivos, 16
- Documentación, 5
- Documento cifrado
 - abrir, 19

G

- Guard, 7, 9
 - administrar claves, 24
 - ajustes, 21
 - Ajustes de cifrado PGP, 23
 - ajustes de seguridad, 22
 - cerrar la sesión, 20
 - configurar, 10

R

- Restablecer la contraseña, 22
