

# KEYFORTRESS™

# Guía y Manual de usuario

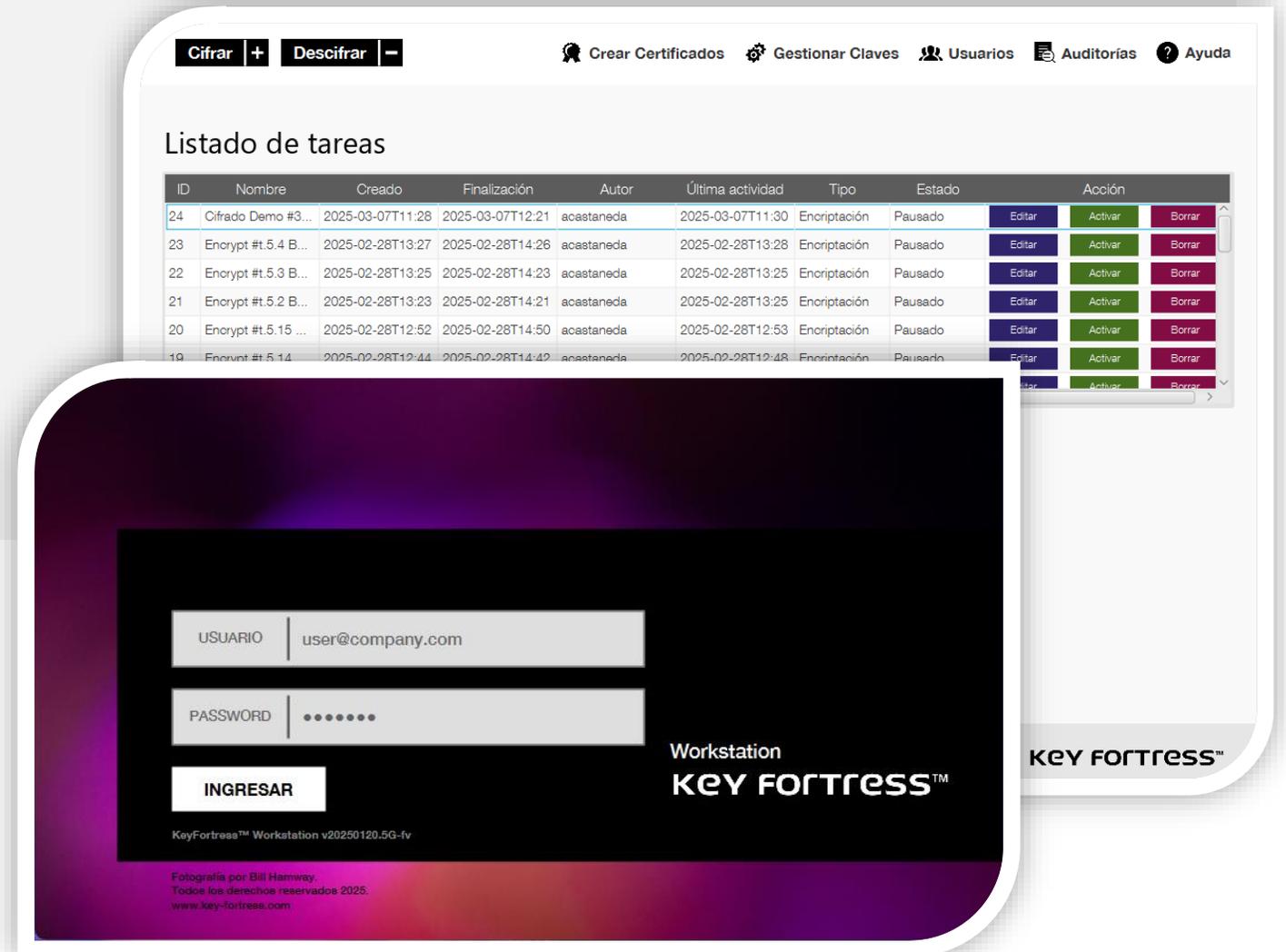
## KeyFortress Workstation

Información técnica para la gestión de su licencia de KeyFortress Workstation como administrador de la aplicación.

Este documento es una copia no controlada de la guía oficial que se encuentra disponible en: <https://www.keyfortress.com/guias/workstation>

Este documento aplica a la versión de: **KeyFortress Workstation v250321.5G**

[www.keyfortress.com](http://www.keyfortress.com)



# KeyFortress Workstation en Español

Sea bienvenido(a) al portal de información de producto y guías de uso de KeyFortress Workstation en Español.

# Keyfortress Workstation - Español

## #1 en Cifrado Masivo Automatizado (MFT)

### KeyFortress Workstation para Host-to-Host Financiero y Transferencia Segura de Archivos.

Los principales bancos de América Latina y Grandes Empresas moviendo información confidencial de forma automática y masiva, prefieren KeyFortress Workstation por su cifrado infalible, fácil adaptación a herramientas de terceros y sencillez de uso.

Disponible en:



Cifrar + Descifrar -

Crear Certificados Gestionar Claves

### Listado de tareas

ID	Nombre	Creado	Finalización	Autor	Última actividad	Tipo
24	Cifrado Demo #3.	2025-03-07T11:28	2025-03-07T12:21	acastaneda	2025-03-07T11:30	Encriptación
23	Encript #1.5.4 B.	2025-02-28T13:27	2025-02-28T14:26	acastaneda	2025-02-28T13:28	Encriptación
22	Encript #1.5.3 B.	2025-02-28T13:25	2025-02-28T14:23	acastaneda	2025-02-28T13:25	Encriptación
21	Encript #1.5.2 B.	2025-02-28T13:23	2025-02-28T14:21	acastaneda	2025-02-28T13:25	Encriptación
20	Encript #1.5.15 ...	2025-02-28T12:52	2025-02-28T14:50	acastaneda	2025-02-28T12:53	Encriptación
19	Encript #1.5.14 ...	2025-02-28T12:44	2025-02-28T14:42	acastaneda	2025-02-28T12:48	Encriptación
18	Encript #1.5.13 ...	2025-02-28T12:38	2025-02-28T14:36	acastaneda	2025-02-28T12:38	Encriptación

### Estadísticas

Mes	Número de transacciones
Enero	0
Feb	280
Marzo	20
Abr	0
Mayo	0
Jun	0
Jul	0
Agosto	0

## Acerca del producto

**KeyFortress Workstation** es un software de cifrado, descifrado y protección de escritorio diseñado para entornos y sistemas operativos de Windows y Linux.

**KeyFortress Workstation** está activo y colabora con cientos de organizaciones para cifrar y proteger sus archivos en reposo y documentos confidenciales en el sector financiero que deban ser transferidos de un punto a otro.

### La tecnología detrás de KeyFortress Workstation

**KeyFortress Workstation** usa el estándar de criptografía asimétrica llamada PGP (Pretty Good Privacy) que es el más seguro y confiable para mantener sus archivos e información protegidos y cifrados. Sólo quien tenga la clave privada podrá acceder e ellos.

## Características técnicas

### Tecnologías Incluidas:

- OpenPGP y GnuPG (GPG) para encriptar y desencriptar archivos mediante claves públicas y privadas de certificados con el estándar PGP.
- Generación de par de llaves (pública y privada) para certificados digitales PGP.
- Almacenamiento y gestión de par de llaves para vincularlas con tareas de cifrado y descifrado.
- Servicios adicionales de Certificación SSL/TLS 1.3 para encriptar los canales que le permitan transferencias de archivos por protocolos SFTP y HTTPS.

### Performance:



- Versión para automatizar por tareas, las transferencias de archivos con servidores FTP/SFTP en procesos desatendidos o automatizados, sin intervención humana.
- Sin restricciones en la cantidad ni peso de datos o archivos cifrados.
- Incluye Cifrado y descifrado de archivos ilimitados.
- Incluye gestión ilimitada de claves públicas de terceros como bancos o clientes.
- Soporte mejorado para Windows Server +12 y Windows 8.1, 10 y 11. (Licencia Windows)
- Triggers para procesar automáticamente cifrado de archivos desde una ubicación específica.
- Escaneo automático para ubicar archivos a cifrar o descifrar, configurable por periodos de tiempo.
- Soporte de configuración en redes privadas virtuales (VPN), no requerirá apertura de puertos.
- Generación de registros de auditoría de las transacciones y accesos.
- Soporte para el desarrollo de flujos de trabajo de tareas de cifrado y descifrado.
- Soporta cifrado y entrega mediante reintentos de conexión y reanudación automática de envíos.
- Soporte de comprensión con el mismo formato del archivo original.
- Compresión de hasta -5% de su tamaño original.

## Tecnología de cifrado

- Versión exclusiva para cifrado de datos y archivos en reposo y tránsito.
- Soporte del estándar de cumplimiento FIPS 140-2 con estándares de encriptación NIST.
- Algoritmos de encriptación asimétrica:
  - DSA (sólo firma)
  - RSA
- Con tamaños de claves mínimo 2048 y máximo 4096 bits.
- Incluye herramienta de gestión y creación de certificados digitales con claves públicas y privadas PGP.
- Soporte de certificados digitales PGP (Pretty Good Privacy) propios o de terceros.
- Generación de sus propias llaves o claves públicas y privadas.

## Licenciamientos disponibles

- Licenciamiento para Windows Server & Desktop.
- Licencia Standalone (para Servidor, Workstations y/o Desktops) con pago único (lifetime license) o pago de suscripción anual.
- Licencia que incluye soporte de 12 ó 24 meses.
- Licencia válida para una o varias empresas de su grupo económico.
- Para Universidades, la licencia puede ser usada para desarrollo académico (clases y demos).
- Licencia válida para ilimitados Servidores físicos o virtualizados dentro de una misma organización.
- Licencia válida para ilimitados desktops o computadores de trabajo (Workstations).

## Cumplimiento Regulatorio

Cumplimos la regulación PCI DSS, NIST, HIPAA, SOX y de Protección de Datos Personales como GDPR y LGPD. KeyFortress™ Workstation está basado en OpenPGP y cumple las directivas IETF PS RFC 4880 y 9580.



## Funciones y capacidades



### Genera tu propio par de claves PGP

Cada tarea y proyecto requiere de medidas específicas de seguridad, por ello desde KeyFortress Workstation te ayudamos a crear certificados o claves públicas ilimitadas.



### Gestiona y automatiza tus claves y la de terceros

Convierte el caos en el orden que esperabas. Gestiona tus propios certificados y claves privadas en un solo lugar y almacena las claves públicas de tus bancos, colegas y terceros a través del inventario de claves más eficaz.



### El cifrado que trabaja por ti en automático

Ya sea que necesites cifrar un solo archivo o múltiples archivos sin intervención humana y de forma automática, KeyFortress Workstation está listo para ayudarte con estas tareas.



### Criptografía Post-Cuántica

Estamos preparados para el Futuro y en KeyFortress Workstation hemos adoptado los algoritmos recomendados por la NIST para protegerte en la era post-cuántica.



### Cifrado y descifrado en Modo Offline

No requiere conexión a Internet ni ninguna nube pública para las tareas individuales o masivas de cifrado y descifrado. Trabaja con plena privacidad sin conexión exterior.



### Tus datos, siempre contigo

Confidencialidad: Ningún archivo cifrado o descifrado con KeyFortress Workstation se comparte. Toda la información está contigo todo el tiempo.

## Generación de Par de Claves PGP

Cada tarea y proyecto requiere de medidas específicas de seguridad, por ello desde KeyFortress Workstation te ayudamos a crear certificados o claves públicas ilimitadas.

## Gestiona y automatiza tus claves y la de terceros

Convierte el caos en el orden que esperabas. Gestiona tus propios certificados y claves privadas en un solo lugar y almacena las claves públicas de tus bancos, colegas y terceros a través del inventario de claves más eficaz.

## El cifrado que trabaja por ti en automático

Ya sea que necesites cifrar un solo archivo o múltiples archivos sin intervención humana y de forma automática, KeyFortress Workstation está listo para ayudarte con estas tareas.

## Criptografía Post-Cuántica

Estamos preparados para el Futuro y en KeyFortress Workstation hemos adoptado los algoritmos recomendados por la NIST para protegerte en la era post-cuántica.

## Cifrado y descifrado en Modo Offline

No requiere conexión a Internet ni ninguna nube pública para las tareas individuales o masivas de cifrado y descifrado. Trabaja con plena privacidad sin conexión exterior.

## Tus datos, siempre contigo

Confidencialidad: Ningún archivo cifrado o descifrado con KeyFortress Workstation se comparte. Toda la información está contigo todo el tiempo.

## Cifrado y descifrado

The image shows two overlapping windows from the KeyFortress software. The left window is titled 'Tarea de Encriptación' (Encryption Task) and the right window is 'Tarea de Desencriptado' (Decryption Task). Both windows have a similar layout with fields for task name, key selection, notifications, subdirectories, start/end dates, frequency, retention, and file format. At the bottom of the encryption window, there are two buttons: 'Cifrar +' (Encrypt) and 'Descifrar -' (Decrypt).

**Tarea de Encriptación**

Nombre de tarea  
Asigne un nombre a la tarea de encriptación.  
Tarea Masiva #87 Cifrado - Banco of America

Llave de cifrado  
Seleccione la llave pública PGP con la que cifrará los archivos.  
BANK OF AMERICA CORP | D05C1

Notificaciones  
Seleccione al usuario que recibirá notificaciones en caso de fallas.  
ADMINKF (UserDemo@keyfortress.net)

Subdirectorios  
Indique si desea que se cifren subdirectorios de su directorio de entrada.  
 Cifrar subdirectorios

Fecha inicio  
Día y hora que empieza la tarea.  
13-03-2025 / 18:57

Fecha final  
Día y hora que finaliza la tarea.  
27-03-2025 / 18:57

Frecuencia  
Frecuencia de cifrado de archivos.  
1 minuto

Retención  
Eliminación de archivos.  
Mantenerlos

Formato de archivo  
Indique el formato o extensión del archivo resultante.  
Mantener extensión

**Cifrar +**   **Descifrar -**

**Tarea de Desencriptado**

Nombre de tarea  
Asigne un nombre a la tarea de desencriptado.  
Decrypt Demo - Bank of America

Llave de desencriptado  
Seleccione la llave privada PGP con la que desencriptará.  
BANK OF AMERICA CORP | D05C1

Contraseña de certificado  
Dígame la contraseña del certificado digital.  
.....

- Cifrado y descifrado del lado del usuario (en local).
- Creación de tareas automatizadas de cifrado y descifrado.
- Etiqueta y nombre de cada tarea de cifrado/descifrado para su identificación.
- Creación de tareas individuales no automatizadas de cifrado y descifrado.
- Drag & Drop para cifrar o descifrar archivos de forma individual.
- Selección de clave pública y privada para cifrar y descifrar:
  - Selección a través del módulo de gestión de claves.
  - Selección por explorador de Windows o archivo local.
- Configuración de usuario que recibirá notificaciones en caso de fallas.
- Notificación automática vía e-mail en caso de fallas.
- Uso de contraseña de la clave privada para descifrar archivos.
- Capacidad de cifrar directorios y subdirectorios.
- Selección de carpetas de entrada y de exportación.
- Selección de directorios SFTP (entrada y salida).
- Configuración de la fecha de inicio y finalización de cada tarea.
- Posibilidad de detener y editar tareas.
- Frecuencia de cifrado/descifrado: Cada 1 minuto y máximo 48 horas.
- Políticas de retención:
  - Mantener los archivos después de cifrados/descifrados.
  - Borrar los archivos después de cifrados/descifrados.
- Extensiones o formato de exportación de archivos: .GPG o .PGP.
- Posibilidad de mantener la misma extensión del archivo cifrado.

## Generación y administración claves PGP



- Crea certificados PGP ilimitados.
- Agrega un nombre o etiqueta para distinguir cada certificado digital.
- Configura la longitud y tamaño de las claves: 2048, 3072 y 4096 bits.
- Genera claves sólo para cifrado (RSA) o para cifrado y firmado (RSA/DSA).
- Determina la fecha de expiración de cada par de claves (certificado).
- Asigna una contraseña para tu clave privada.
- Exporta tus claves públicas para compartirlos con terceros.
- Almacén y repositorio de claves públicas y privadas.
- Importa claves públicas PGP generados en otros sistemas.
- Importa y administra claves públicas de terceros.
- Inventario de claves que muestran Nombres, validez y fechas de caducidad.
- Identificación de Fingerprints por cada par de claves.
- Revoca certificados generados con errores o vulnerados.
- Elimina claves públicas o privadas que vencieron.
- Cada certificado será generado con la extensión .ASC.

## Credenciales y administración de usuarios por roles

The screenshot displays the 'Gestión de Usuarios' (User Management) interface. It features a form for creating or editing a user with the following fields:

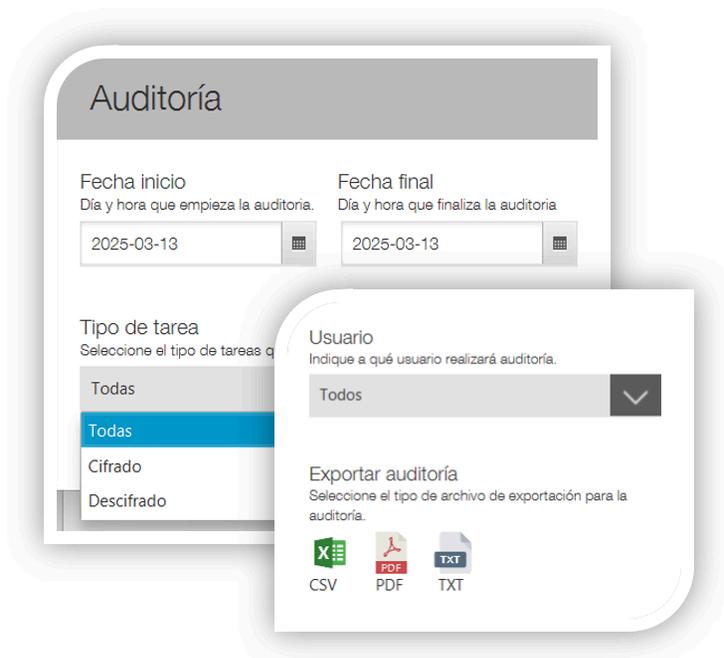
- Nombre de usuario:** Juan Alberto Perez Garcia
- Correo electrónico:** japg@keyfortress.com
- Organización:** KEYFORTRESS S.A.
- Contraseña:** (masked with dots)
- Confirme contraseña:** (masked with dots)
- Tipo de usuario:** A dropdown menu with options: Superadmin, Manager, Operator, Auditor.

A 'Guardar' (Save) button is located at the top right of the form. Below the form, a table lists existing users:

Tipo	Estado	Acción		
Superadmin	Activo	Editar	Suspender	Borrar
Superadmin	Activo	Editar	Suspender	Borrar

- Jerarquía disponible de usuarios:
  - Superadmin
  - Managers
  - Operadores
  - Auditores
- Asignación de nombres, e-mail y empresa asociada por usuario.
- Usuarios SuperAdmin para controlar toda la administración.
  - Crear a otros usuarios Managers.
  - Editar, suspender o borrar usuarios y tareas.
- Usuarios Managers con privilegios para crear, editar, suspender o borrar otros usuarios y tareas de cifrado y descifrado.
- Los usuarios SuperAdmin y Managers podrán crear ilimitados par de claves.
- Usuarios Operadores para crear ilimitadas tareas de cifrado y descifrado y supervisar las operaciones diarias.
- Usuarios Auditores podrán revisar las estadísticas e informes generados a demanda sobre las actividades de cifrado y descifrado de la plataforma.

## Auditorías e informes



- Generación de reportes de auditoría en formatos:
  - CSV o compatible con Microsoft Excel.
  - PDF/A
  - Archivos de texto plano .TXT
- La tarea de generación de informes bajo demanda es exclusiva de los usuarios Auditores, Managers o Superadmin.
- Posibilidad de seleccionar una fecha de inicio y fecha final para la generación del informe, sin límite de fechas.
- Generación de informes por tipo de actividad:
  - Informes por tareas de cifrado.
  - Informes por tareas de descifrado.
  - Informes por tareas individuales o masivas.
  - Todo tipo de tareas.
  - Reportes y auditorías por usuario.
  - Incluir la revisión de todos los usuarios.

## Versión Trial

Use y experimente KeyFortress Workstation por 15 días totalmente gratis.

Si está interesado(a) en probar KeyFortress Workstation, podrá obtener ayuda y orientación en este espacio.

**KEYFORTRESS™**

**Registro para Trial de KeyFortress Workstation**

Pruebe la plataforma #1 de Protección de Información en América Latina, gracias a nuestra tecnología de Cifrado o Encriptado PGP.

**Regístrese para obtener una versión de prueba por 15 días.**

Nombres * <input type="text"/>	Apellidos * <input type="text"/>
Tipo Identificación * <input type="text"/>	Nro. Documento * <input type="text"/>
País residencia * <input type="text"/>	Ciudad * <input type="text"/>
Teléfono Móvil * <input type="text"/>	Correo electrónico * <input type="text"/>

Formulario de Solicitud Trial

### Siga los siguientes pasos para obtener una versión de prueba.

1. Regístrese en [este formulario de solicitud](#). Utilice datos válidos porque enviaremos información importante a su correo electrónico y número de teléfono.
2. Recibirá las credenciales de acceso a su correo electrónico.
3. En el mismo mensaje anterior, recibirá el link de descarga KeyFortress Workstation Trial por 15 días.

Hola Alfredo,  
Bienvenido(a) a KeyFortress. Hemos recibido tu solicitud y queremos entregarte una versión de prueba de **KeyFortress Workstation**. Por favor, sigue las siguientes instrucciones:

- [Descarga KeyFortress Workstation \[Trial 15 días\]](#)
- [Lee nuestra Guía](#) para saber cómo instalarlo en tu sistema operativo Windows.
- Usa las siguientes credenciales:

- Para inicio de sesión y operaciones, [siga los pasos de esta sección](#).

### Políticas de la Versión Trial

- La versión trial consta de 15 días calendario de licencia de uso.
- La versión trial sólo está disponible para sistemas operativos Windows.
- Puede instalar una licencia de prueba de KeyFortress Workstation en ilimitados computadores, estaciones de trabajo o servidores durante el periodo de pruebas.
- No se podrá ampliar la licencia por más tiempo a un usuario, después de los 15 días.
- La versión trial permite el uso de todas las capacidades del software, excepto la emisión de certificados digitales PGP. Podrá solicitar un certificado de prueba por 15 días con nuestro equipo.

## Instalación en Windows OS

Siga las siguientes instrucciones para instalar KeyFortress Workstation en su servidor o estación de trabajo de Windows.

**KeyFortress Workstation** es una aplicación diseñada para Estaciones de Trabajo (Workstations), Servidores o Computadores Personales con el soporte de sistemas operativos Windows.

### Sistemas Operativos soportados:

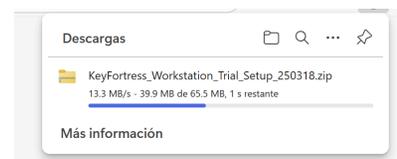
- Windows 8.1, 10 y 11, Windows Server 2012+

### Requisitos mínimos:

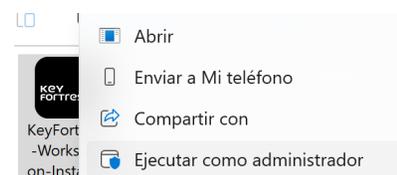
- Memoria RAM mínima 4GB.
- Espacio en Disco 10 GB.
- Base de datos no requerida.
- No requiere conexión a Internet para operaciones de cifrado y descifrado pero si para login.

### Instalando KeyFortress Workstation

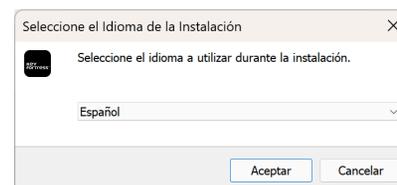
1. Descargue la Versión Trial, Versión Anual o Vitalicia (Lifetime license) de KeyFortress Workstation.



2. Una vez que haya descargado la aplicación de instalación, proceda descomprimir el archivo que viene por defecto en formato o extensión ".Zip".
3. Haga doble clic sobre el archivo instalador ".exe" o clic derecho y Seleccione "Ejecutar como administrador"

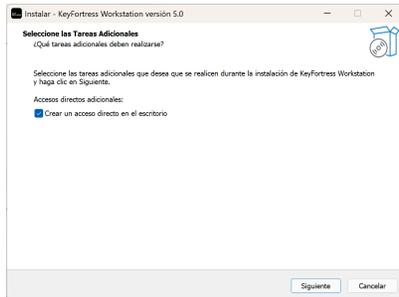


4. Si obtiene una alerta de "Editor desconocido" seleccione "Instalar de todas formas".
5. Aparecerá una ventana para seleccionar el idioma de la instalación. Elija Español.

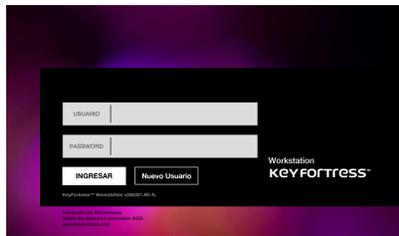


## Operaciones con el software

- Si lo prefiere, cree un acceso directo en el escritorio de su computador, estación de trabajo o servidor.



- Siga las instrucciones de instalación, haciendo clic en el botón "Continuar" o "Siguiente" en cada paso.
- Listo para instalar haciendo clic en el botón "Instalar".
- Al finalizar la instalación, obtendrá un mensaje de confirmación y la ventanilla de Login.



## Primer ingreso y login

Sepa cómo ingresar a la aplicación de KeyFortress Workstation

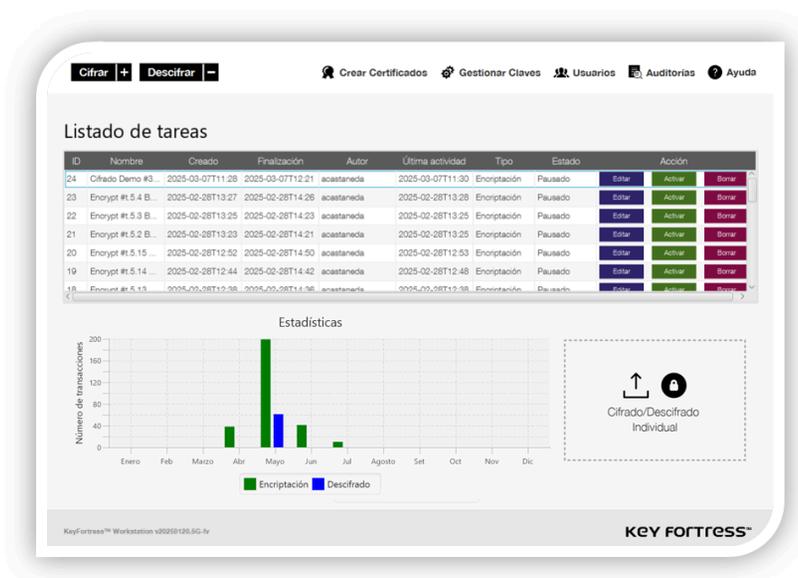


- Ahora que ya tiene instalado KeyFortress Workstation en su servidor, workstation o computador, es momento de ingresar y utilizar su licencia.
- Recibirá su usuario y password (credenciales) de forma automática por e-mail al [solicitar una versión de prueba o trial](#) o unas horas después de comprar su licencia anual o vitalicia. En caso no las haya recibido, póngase en contacto con nuestro equipo, por nuestros [canales de soporte premium](#).
- **Ingrese el USUARIO en el campo indicado y la contraseña en el campo PASSWORD, haga clic en el botón "INGRESAR" y estará dentro.**
- Después de su primer ingreso, podrá cambiar tanto su usuario como su contraseña.

## Dashboard y Menú

Conoce el panel de control de KeyFortress Workstation y realiza operaciones de cifrado y descifrado.

Inmediatamente después de hacer login o ingresar con tus credenciales en **KeyFortress Workstation**, obtendrás la vista del panel de control o dashboard de la plataforma.



### Descripción del Menú Principal



- **Botón Cifrar:** Haciendo clic en esta opción, accederás a un entorno donde podrás configurar las tareas de cifrado automatizado que ofrece la plataforma.
- **Botón Descifrar:** Haciendo clic en esta opción, accederás a un entorno donde podrás configurar las tareas de descifrado o desenscriptado automatizada que ofrece la plataforma.
- **Crear Certificados:** En esta sección, accederás a un formulario para crear tu par de claves o llaves PGP (pública y privada).
- **Gestionar Claves:** En esta sección podrás administrar tus propias claves públicas o privadas así como importar y utilizar claves públicas PGP de terceros.
- **Usuarios:** En esta sección podrás administrar tu perfil de usuario, editar tu contraseña, o incluso los perfiles de otros usuarios de tu equipo.
- **Auditorías:** En esta sección podrás configurar los reportes de auditoría por usuario, por tipo de transacción, etc en formatos como CSV, TXT y PDF.
- **Ayuda:** Accederás directamente al portal de Guía y Manuales de Usuarios, es decir este mismo sitio web.



Esta sección permite que hagas "Drag & Drop" de archivos para cifrar o descifrar sin requerir automatizar una tarea. Esta opción es útil para cifrar o descifrar archivos individuales.

### Sección de Estadísticas



En esta sección se dibujarán de forma automática las estadísticas de transacciones tanto de cifrado como de descifrado que procese KeyFortress Workstation.

### Sección Cifrado/Descifrado Individual

## Primeros pasos

Prepara y configura la plataforma para adecuarla a tu forma de trabajo o los requisitos técnicos de tu proyecto.

**Antes de iniciar las operaciones de cifrado y descifrado, te sugerimos:**

1. [Actualiza o cambia el usuario y contraseña de tu licencia.](#)
2. [Añade personas a tu equipo de trabajo](#) (en caso estés usando la versión de servidor).
3. [Crea tu primer par de claves PGP](#) (pública y privada).
4. [Importa y gestiona claves públicas PGP de terceros.](#)
5. Comienza a operar KeyFortress Workstation:
  - a. [Crea tareas de cifrado automático.](#)
  - b. [Crea tareas de descifrado automático.](#)
6. [Exporta tu primer informe de actividades o uso.](#)

Cada paso o sugerencia contiene un link, haz clic en el para dirigirte hacia las instrucciones sugeridas.

## Actualizar usuario y contraseña

Como medida de seguridad en tu licencia de KeyFortress Workstation, sugerimos cambiar tanto el usuario como la contraseña que ha recibido.

1. En el menú principal ubicado en la parte superior de KeyFortress Workstation, ubica la opción "Usuarios". Haz clic en el.

### Usuarios

2. Aparecerá una ventana con el título de "Gestión de Usuarios".
3. En la parte inferior podrás ver el listado de usuarios activos en tu cuenta. Selecciona el usuario por defecto.



4. Haz clic en el botón "Editar".
5. Aparecerá la información del usuario en la parte superior de tu pantalla.

<b>Nombre de usuario</b> Asigna o edita el nombre de usuario. <input type="text" value="usuario1"/>	<b>Contraseña</b> Asigna una contraseña para este usuario. <input type="password" value="*****"/>
<b>Correo electrónico</b> Escribe el correo electrónico del usuario. <input type="text" value="demo@keyfortress.com"/>	<b>Confirme contraseña</b> Repite la contraseña del usuario para confirmarla. <input type="password" value="*****"/>
<b>Organización</b> Selecciona el nombre de su empresa u organización. <input type="text" value="KEYFORTRESS SA"/>	<b>Tipo de usuario</b> Indique qué tipo de permisos tendrá este usuario. <input type="text" value="Superadmin"/>

6. Podrás cambiar el nombre de usuario a un de tu preferencia. Igualmente podrás cambiar la contraseña.
7. Haz clic en el botón "Guardar" y habrás finalizado.

## Añadir personas a tu equipo

Si nos mantenemos en la misma sección de Usuarios, podremos agregar a otras personas que serán parte de nuestro equipo de trabajo. Sugerimos este paso si la instalación de **KeyFortress Workstation** se ha realizado en una estación de trabajo compartida o un servidor.

1. Haz clic en la opción de Usuarios del menú principal.
2. Aparecerá una ventana con el título "Gestión de Usuarios".

3. Aparecerá un formulario vacío, puedes llenarlo con la información del usuario que desees crear. Importante designarle un rol o "Tipo de Usuario" de acuerdo a la función que desempeñarán.
4. Te sugerimos ver la sección de "[Credenciales y administración de Usuarios por roles](#)" para un mejor entendimiento de los roles.
5. El usuario y contraseña creado no se enviará de forma automática al correo del nuevo usuario. Comparte las credenciales con tu colega de una forma segura o usando [KeyFortress Handvault](#) ➤

## Crear un par de claves PGP

La creación del par de claves PGP, es decir un certificado PGP con una clave pública y otra clave privada es indispensable para iniciar las operaciones de cifrado y descifrado en KeyFortress Workstation.

Algunos artículos sobre el significado, conceptos y características de los certificados digitales PGP.

1. Haz clic en la opción de "Crear Certificados" del menú principal.

## Crear Certificados

2. Aparecerá una ventana con un formulario con el título "Generar Certificados".



3. Llena el formulario según lo solicitado.
4. Asistencia y conceptos claves para el llenado del formulario:

- a. **Common Name:** Escribe el nombre del titular del certificado digital PGP. Es un campo referencial y donde podrás escribir de forma libre.
  - b. **Longitud:** Puedes elegir la longitud de la clave de cifrado, mientras más alta es más segura pero podría no ser compatible con el tercero con quien compartirás tu clave pública. El estándar más aceptado es el tamaño de 2048 bits.
  - c. **Expiración:** Con KeyFortress Workstation podrás elegir la fecha exacta en que deba expirar el certificado. Siempre será necesario configurar una fecha. Fecha límite de 15 años.
  - d. **Correo electrónico:** Escribe la dirección de e-mail del titular de este certificado. Si es un certificado para ti o tu organización puedes crear ilimitados par de claves.
  - e. **Tipo de clave:** Por defecto es RSA/RSA tanto para cifrado como para la generación de las claves.
  - f. **Contraseña y Confirmar contraseña:** Debes escribir una contraseña de al menos 8 dígitos alfanumérica. Utiliza símbolos solo si el software de descifrado que usará es el mismo KeyFortress Workstation.
  - g. **Almacenar:** Desplegará la opción de...
    - i. Mantener guardado: El par de claves que genere se guardará automáticamente en la sección de "Gestionar Claves". para re-utilizarla en próximas operaciones de cifrado o descifrado.
    - ii. Sólo exportar: Exportará el par de claves en un directorio de tu servidor o computado y no se guardará dentro de la plataforma. En caso desees usar el certificado digital PGP o par de claves generado con éste método, tendrás que importarla como una clave de terceros.
    - iii. Directorio de exportación: Selecciona el directorio donde exportarás el par de clave sólo si seleccionaste la opción de "Sólo exportar".
5. Una vez finalizado el llenado, haz clic en el botón "Generar" para crear el par de claves.
  6. Visualizarás un mensaje de confirmación de certificado emitido o certificado generado con éxito.
  7. Revisa la sección de "Gestionar Claves" para verificar que tu par de claves se encuentra generado. Esta opción en caso hayas seleccionado "Mantener guardado".

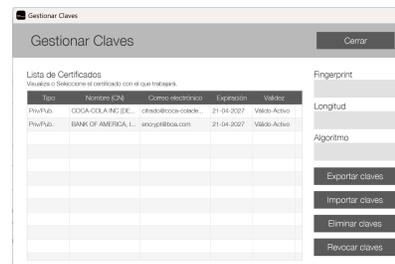
## Importar y gestiona claves públicas PGP de terceros

Ya sea que necesites importar las claves públicas PGP de terceros o tus propios certificados PGP generados por otros medios; en esta sección podrás importarlas y almacenarlas dentro de la plataforma de forma local para utilizarlas en las operaciones de cifrado y descifrado.

1. Haz clic en la opción "Gestionar Claves" del menú principal.

### Gestionar Claves

2. Aparecerá una ventana con el título "Gestionar Claves"



3. En la parte izquierda de la ventana, aparecerán listados los certificados o claves públicas y privadas que hayas importado previamente. Esta sección podría aparecer vacía si no has generado ningún par de claves previamente. En la parte superior derecha aparece un menú dinámico que se llena con la información del certificado o par de claves que elijas en un determinado momento. En la parte inferior derecha, aparece un menú de opciones para operar los certificados y claves.
4. **Opciones del menú interno**
  - a. **Exportar claves:** Podrás exportar una clave pública, privada o ambas seleccionándola y haciendo clic en este botón. Para exportar ambas, necesitarás recordar la contraseña del certificado. Para exportar claves públicas no requiere el uso de contraseña.
  - b. **Importar claves:** Haz clic en este botón en caso desees importar claves públicas de terceros. Al hacer clic en este botón, aparecerá el navegador de Windows para seleccionar la clave pública que desees importar.
  - c. **Eliminar claves:** Permite eliminar de esta sección el certificado o clave pública PGP previamente seleccionada.
  - d. **Revocar claves:** Si previamente generaste un certificado digital PGP (par de claves), con esta opción y botón podrás anularla o revocarla, sin necesidad de eliminarla de esta vista.

## Crear tareas de cifrado automático

Es hora de cifrar y proteger tus archivos. En esta sección aprenderás a configurar una tarea automatizada de cifrado con **KeyFortress Workstation**.

1. Haz clic en el botón de "Cifrar".



2. Aparecerá una ventana con un formulario para configurar una tarea de cifrado automatizado con el título "Tarea de Encriptación".

3. Vamos a conocer qué significa cada uno de los campos solicitados.
  - a. Nombre de tarea:
  - b. Estado de tarea:
  - c. Llave de cifrado:
  - d. Fecha Inicio/Final:
  - e. Notificaciones:
  - f. Frecuencia:
  - g. Retención:
  - h. Subdirectorios:
  - i. Formato de Archivo:
  - j. Directorio de entrada:
  - k. Directorio de salida:
4. Cuando hayas finalizado el llenado de todos los campos, haz clic en el botón "Guardar" y la tarea de cifrado automático se habrá creado con éxito.
5. Verifica en el Dashboard que la tarea se encuentre activa y funcionando.

## Crear tareas de descifrado automático

Vamos a descifrar los archivos que previamente has protegido o que algún tercero te envió cifrado con tu propia clave pública PGP.

1. Haz clic en el botón de "Descifrar".



2. Aparecerá una ventana con un formulario para configurar una tarea de descifrado automatizado con el título "Tarea de Desencriptado".

3. Vamos a conocer qué significa cada uno de los campos solicitados para crear una tarea de descifrado.
  - a. Nombre de tarea:
  - b. Estado de tarea:
  - c. Llave de desencriptado:
  - d. Fecha Inicio/Final:
  - e. Contraseña de certificado:
  - f. Notificaciones:
  - g. Frecuencia:
  - h. Retención:
  - i. Subdirectorios:
  - j. Directorio de entrada:
  - k. Directorio de salida:
4. Cuando hayas finalizado el llenado de todos los campos, haz clic en el botón "Guardar" y la tarea de descifrado automático se habrá creado con éxito.
5. Verifica en el Dashboard que la tarea se encuentre activa y funcionando.

## Crear informes de actividades o uso

Desde la sección de Auditorías podremos crear los informes o reportes de uso en diferentes formatos como CSV, TXT o en formato ejecutivo PDF.

1. Haz clic en la opción "Auditorías"



2. Aparecerá una ventana con el título "Auditorías"

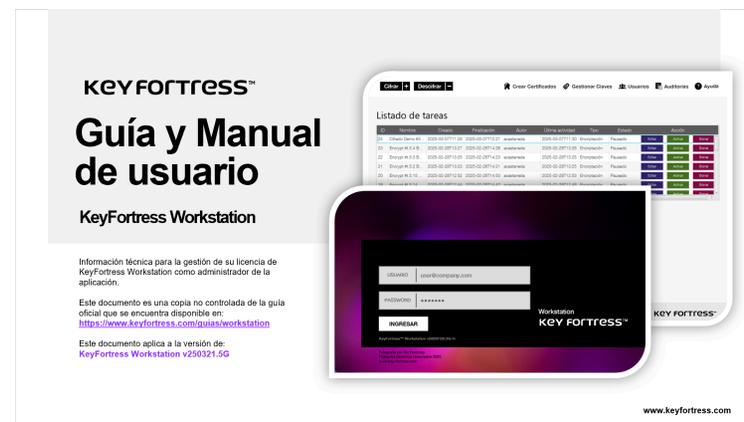


3. Descripción de los campos de Auditorías:
  - a. **Fecha Inicio:** Puedes seleccionar la fecha (día y año) en la que iniciaría la revisión del reporte.
  - b. **Fecha Final:** Puedes seleccionar la fecha (día y año) en la que finalizaría la revisión del reporte.
  - c. **Usuario:** Podrías hacer una auditoría sobre un usuario específico, el cual se desplegará y mostrará al hacer clic en el campo seleccionado o incluso sobre todos los usuarios activos en esta licencia.
  - d. **Tipo de Tarea:** Podrás generar el informe sobre tareas de cifrado, descifrado o sobre ambas.
  - e. **Exportar auditoría:** Al hacer clic en el ícono que corresponde a CSV, TXT o PDF se generará automáticamente la tarea con los campos anteriores previamente llenados. El informe se exportará a tu carpeta de Descargas.
4. Una vez que hayas finalizado la generación de tu informe, puedes hacer clic en el botón "Cerrar" para volver al Dashboard.

## Guía y manual de usuario en PDF

Descargue la versión completa en PDF de esta guía con las instrucciones de uso y administración para KeyFortress Workstation.

- **Descargar Guía y Manual en PDF**



## Canales de Soporte Técnico

En este espacio podrá encontrar todas las formas de soporte y asistencia técnica, gratuita o como parte del plan adquirido con su licencia.

### Asistencia Técnica Gratuita

- [Comunidad Talks - Foros de Discusión ↗](#)

### Asistencia Técnica Premium (Incluida en su licencia)

- Teléfonos en Colombia, Perú, México, Brasil y USA.
  - **Brasil:** +55 (11) 27709930
  - **Colombia:** +57 (601) 5804470
  - **México:** +52 (55) 71002770
  - **Perú:** +51(01) 5104040
- [Agendamiento para orientación personalizada ↗](#).
- [Helpdesk & E-mail - Solicitudes de Soporte por Tickets ↗](#).

### Horarios de atención (GMT-5)

Canal de atención	Planes disponibles
Central Telefónica	<p><b>Plan Básico:</b> Lun. a Vie. de 09:00 a 17:00 hr. No feriados.</p> <p><b>Plan Extendido:</b> Lun. a Sáb. de 08:00 a 18:00 horas. No feriados.</p> <p><b>Plan 24/7:</b> Cualquier horario los 365 días del año. Inc. Feriados.</p>
Correo Electrónico: <b>helpdesk@keyfortress.com</b>	Atención 24/7/365 en cualquiera de los planes.
Asistencia o Instalación Técnica Remota	<p><b>Básico:</b> Lun. a Vie. de 09:00 a 17:00 hr. No feriados</p> <p><b>Plan Extendido:</b> Lun. a Sáb. de 08:00 a 18:00 horas. No feriados.</p> <p><b>Plan 24/7:</b> Cualquier horario los 365 días del año. Inc. Feriados.</p>
Helpdesk - Mesa de Ayuda: <b>keyfortress.com/helpdesk</b>	Atención 24/7/365 en cualquiera de los planes.

### Service Level Agreement (SLA)

Categoría Incidente	Identificador	Descripción	Tiempo Respuesta
<b>Incidente Menor</b>	<b>ITM</b> 	Cuando alguna funcionalidad no se encuentra desarrollando plenamente sin afectar la plataforma total o alguna aplicación de terceros y/o su organización conectada a ella.	48 horas
<b>Incidente Urgente</b>	<b>ITU</b> 	Cuando el servicio ha dejado de operar parcialmente o alguna de sus funciones no está operativa sin afectar otras operaciones.	24 horas
<b>Incidente Grave</b>	<b>ITG</b> 	Cuando el servicio ha dejado de operar totalmente y alguno o todos sus sistemas han dejado de operar. Tiempo de respuesta máximo.	6 horas

# América Latina



## KEYFORTRESS™

### **Bogotá, Colombia**

+57 (601) 5804470  
Cr. 11a #93a-46, Oficina 303  
Chapinero, Bogotá D.C.

Contacto:  
[co-office@keyfortress.com](mailto:co-office@keyfortress.com)

### **Lima, Perú**

+51 (01) 5104040  
Av. Juan de Arona 755, Of. 101  
San Isidro, Lima

Contacto:  
[pe-office@keyfortress.com](mailto:pe-office@keyfortress.com)

### **São Paulo, Brasil**

+55 (11) 27709930  
Rua Gomes de Carvalho 911  
Vila Olímpia, São Paulo

Contacto:  
[br-office@keyfortress.com](mailto:br-office@keyfortress.com)