

SISTEMA DE COMPARTICIÓN DE ARCHIVOS CIFRADOS

ESTRATEGIAS DE SEGURIDAD
ENTREGA FINAL

RAFAEL OLID - CARLOS PÉREZ - ÁNGELA SERNA

UNIVERSIDAD DE ALICANTE | CURSO 2018-2019

ÍNDICE DE CONTENIDO

Contenido de la entrega	2
Casos de Uso	3
Configuración del escenario inicial	3
Crear una copia de seguridad sin compartir	5
Crear una copia de seguridad compartida	7
Editar permisos de una copia de seguridad	9
Descargar y descifrar copias de seguridad	10
Tests	12
Configuración del escenario inicial	12
Subir archivos	13
Editar archivos compartidos	13
Descargar archivos	14
Manual de usuario. Demostración de uso	15
Configuración	15
Escenario inicial	15
Diferentes directorios para el mismo usuario	16
Subir archivos cifrados	16
Presentación de la vista	17
Demostración	18
Modificar permisos	19
Presentación de la vista	19
Demostración – Añadir usuarios	20
Demostración – Eliminar usuarios	21
Descargar archivos	22
Presentación de la vista	22
Demostración	23

CONTENIDO DE LA ENTREGA

El archivo entregado para esta práctica contiene los siguientes 3 archivos:

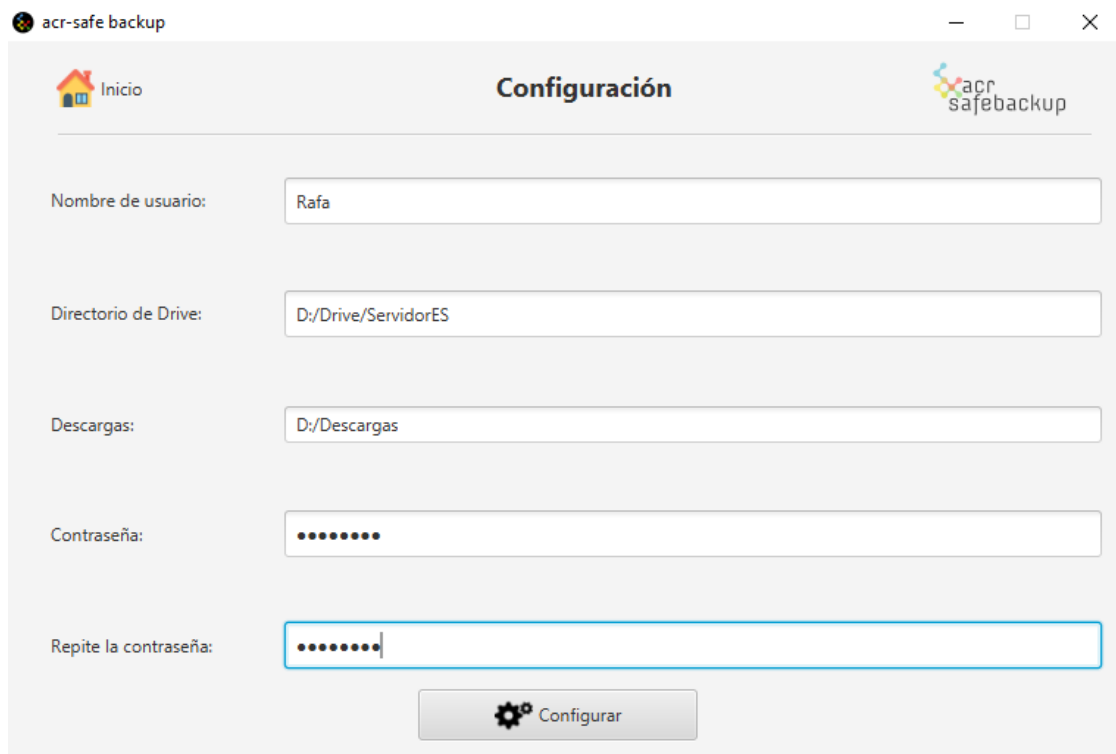
1. **Código fuente.** Se entrega el código del proyecto java con el que hemos estado trabajando para la implementación de la práctica.
2. **Archivo .jar del proyecto.** Archivo java ejecutable que contiene la aplicación para que pueda ser ejecutada a partir del comando *java -jar safeBackup.jar*. Para que el .jar funcione el ordenador debe tener instalada como mínimo la versión de java 1.7 que puede consultarse a través del comando *java -version*.
3. **Memoria.** La memoria está escrita en este documento pdf dónde se incluye la explicación sobre la implementación de los diferentes casos de uso de la aplicación, los tests que hemos realizado para comprobar el correcto funcionamiento de la aplicación y el manual de usuario.

CASOS DE USO

CONFIGURACIÓN DEL ESCENARIO INICIAL

La primera vez que un usuario utilice la aplicación podrá acceder a una vista para indicar dónde se encuentra la estructura de directorios de Google Drive. En caso de no existir el programa la creará automáticamente según lo especificado en el apartado anterior y se crearán las claves públicas y privadas del usuario.

A continuación, se muestra la interfaz desde la que un usuario puede llevar a cabo la configuración del escenario inicial; para ello introducirá un nombre de usuario, la ubicación del directorio sincronizado con Google Drive y su contraseña, además también debe introducir el directorio donde se descargarán los archivos descifrados.



Para que no sea necesario introducir estos datos cada vez que se inicia la aplicación tanto el nombre de usuario como la ruta del directorio sincronizado con Google Drive se guardarán en un fichero de texto que se almacenará en el equipo del usuario (concretamente en una carpeta oculta en el directorio personal del usuario). Sin embargo, la contraseña del usuario no se almacenará de forma física en ningún sitio y por tanto será el usuario el que tenga que introducirla de forma manual siempre que sea requerido.

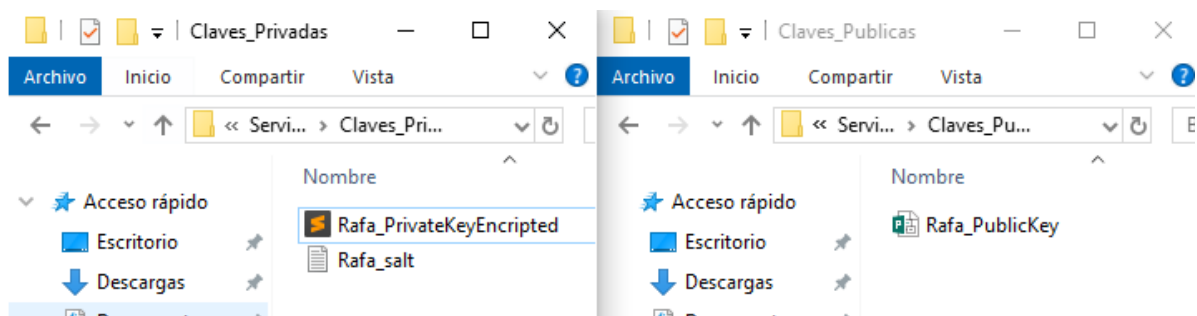
El nombre de usuario actuará como identificador del usuario para el programa, y por tanto no podrán existir dos usuarios que se identifiquen con el mismo nombre. Si introducimos un usuario con un nombre que ya se encuentra en el sistema se creará la estructura de directorios necesaria pero no se creará una nueva clave pública o privada.

Con respecto a cómo se ha realizado el proceso de creación de claves de criptografía asimétrica, se ha utilizado la clase *KeyPairGenerator* incluida en la librería

java.security para crear una pareja de claves pública y privadas basadas en RSA de 1024 bytes.

Una vez creado el par de claves RSA que utilizará el usuario, se almacenará la clave pública en el directorio de Drive y la clave privada se *'hashear'*á con la función SHA-256 a partir de la contraseña del usuario y una sal creada de forma aleatoria para el mismo usuario. Esta sal que se concatenará a la clave privada para evitar ataques de diccionario. Hecho esto, tanto la clave privada cifrada, como la sal (también cifrada) se almacenarán en el directorio de Drive para así permitir que un usuario pueda usar la aplicación desde cualquier equipo.

A continuación, se muestra un ejemplo del funcionamiento de la configuración del caso de uso expuesto. En este caso se ha introducido un nuevo usuario, el directorio de Drive, el directorio donde almacenar las descargas y la contraseña del usuario. Tras esto, se generan tanto la clave pública (en formato .pub) como la clave privada cifrada y se almacenan en sus directorios correspondientes. Cabe destacar que en este caso no ha sido necesaria la creación de ningún directorio porque ya existía toda la estructura de directorios en nuestro Drive y que solo ha sido necesaria la creación de claves.



CREAR UNA COPIA DE SEGURIDAD SIN COMPARTIR

Cuando un usuario decida hacer una copia de seguridad sin compartir utilizará la opción “Subir Archivos Cifrados”. A continuación, se muestra la interfaz del usuario:

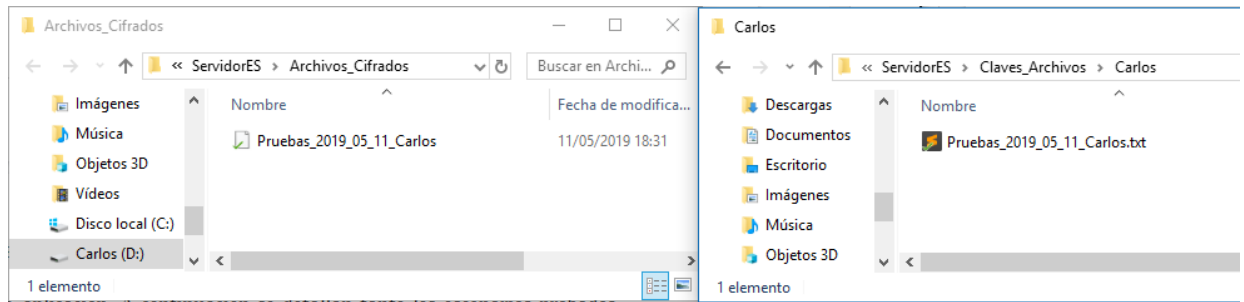


Sobre esta interfaz el usuario decidirá el directorio sobre el que quiere hacer una copia de seguridad y los usuarios con los que desea compartir esta copia de seguridad. En este caso no se va a compartir con ningún usuario.

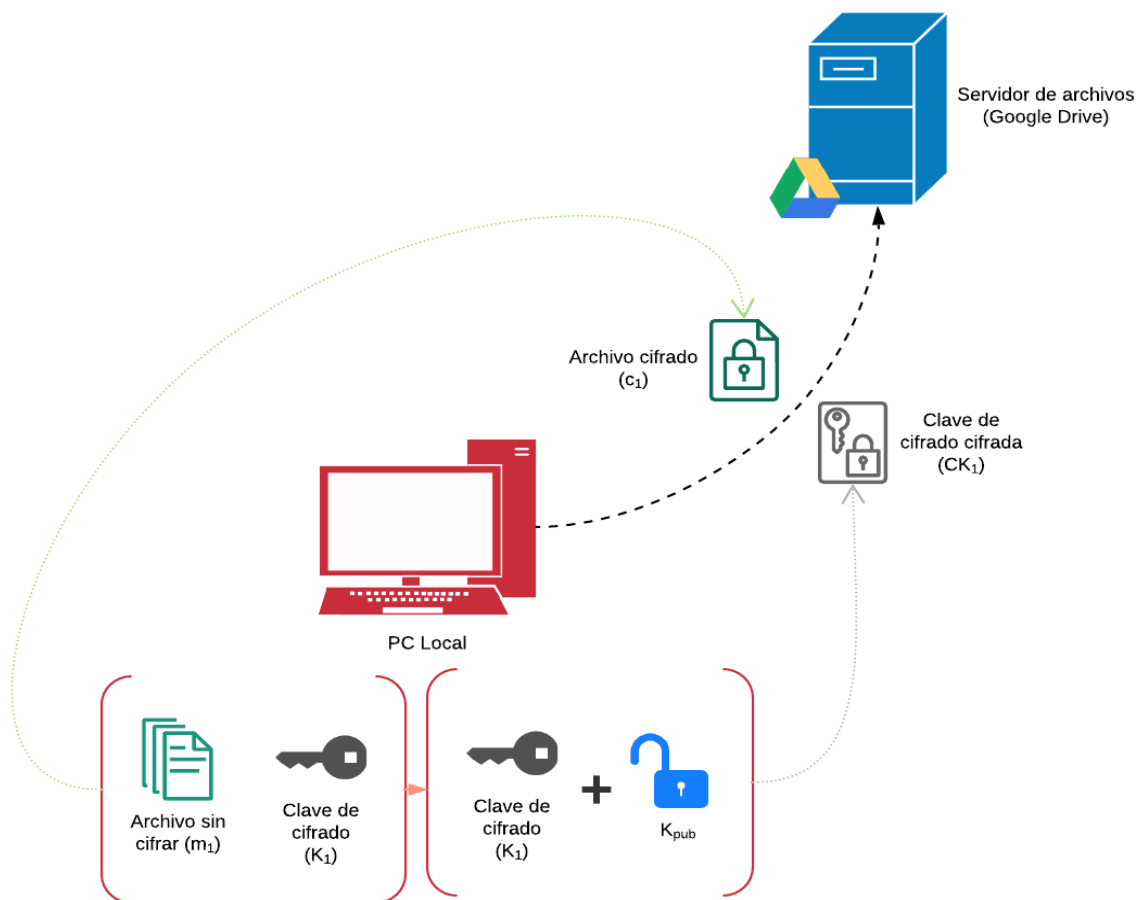
Para este proceso, la aplicación creará un archivo .zip con el contenido de la carpeta para la que se quiere hacer una copia de seguridad que se cifrará mediante el algoritmo AES a partir de una clave de cifrado keyFile generada aleatoriamente y se almacenará en el directorio ‘.../ServidorES/Archivos_Cifrados’. Debido a que el algoritmo AES necesita un vector de inicialización, y con el objetivo de que este vector de inicialización sea diferente para cada usuario, se le pedirá al usuario su contraseña para obtener este IV a partir del hash de la clave privada y su passphrase.

A continuación, la keyFile para ese archivo se cifrará mediante el sistema RSA a partir de la clave pública del usuario para almacenarse después en el directorio ‘.../ServidorES/Claves_Archivos/NombreUsuario’.

Se adjunta debajo el resultado de ejecutar este caso de uso para el usuario *Carlos* sobre un directorio de nombre *Pruebas*.



Por último, se adjunta un esquema que resume todo el proceso explicado en este apartado.



CREAR UNA COPIA DE SEGURIDAD COMPARTIDA

En el caso de que un usuario decida hacer una copia de seguridad sin compartir utilizará la opción “Subir Archivos Cifrados”.

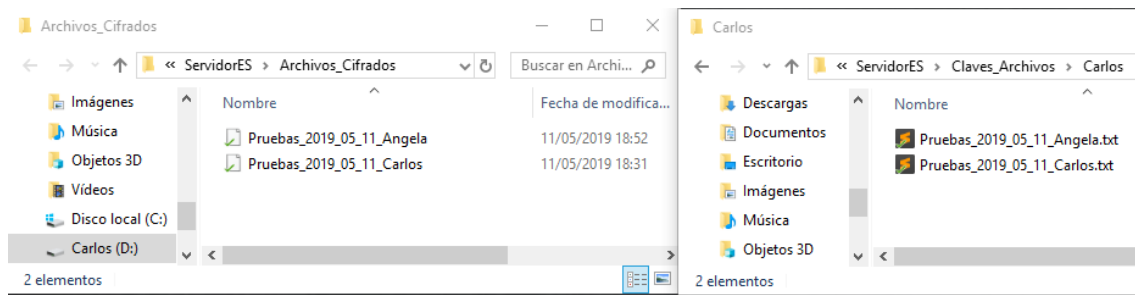


Si bien este caso de uso utiliza la misma funcionalidad que el apartado anterior, la interfaz de usuario permite subir una copia de seguridad de un directorio y compartirla con otro usuario de entre la lista de los usuarios registrados en la aplicación. Esa lista se obtendrá de las claves públicas almacenadas en el directorio ‘.../ServidorES/Claves_Públicas’.

El proceso es igual que el explicado en el apartado anterior: se generará un .zip del directorio indicado, se cifrará con el algoritmo AES a partir de una keyFile creada aleatoriamente y se cifrará esta keyFile mediante RSA con la clave pública del usuario.

Sin embargo, para la compartición se añade un paso más. Una vez se haya creado el keyFile, además de cifrarlo con la clave pública del autor de la copia de seguridad, se almacenará otra copia de la keyFile para cada usuario con el que se vaya a compartir el archivo y se cifraran estas claves con sus respectivas claves públicas.

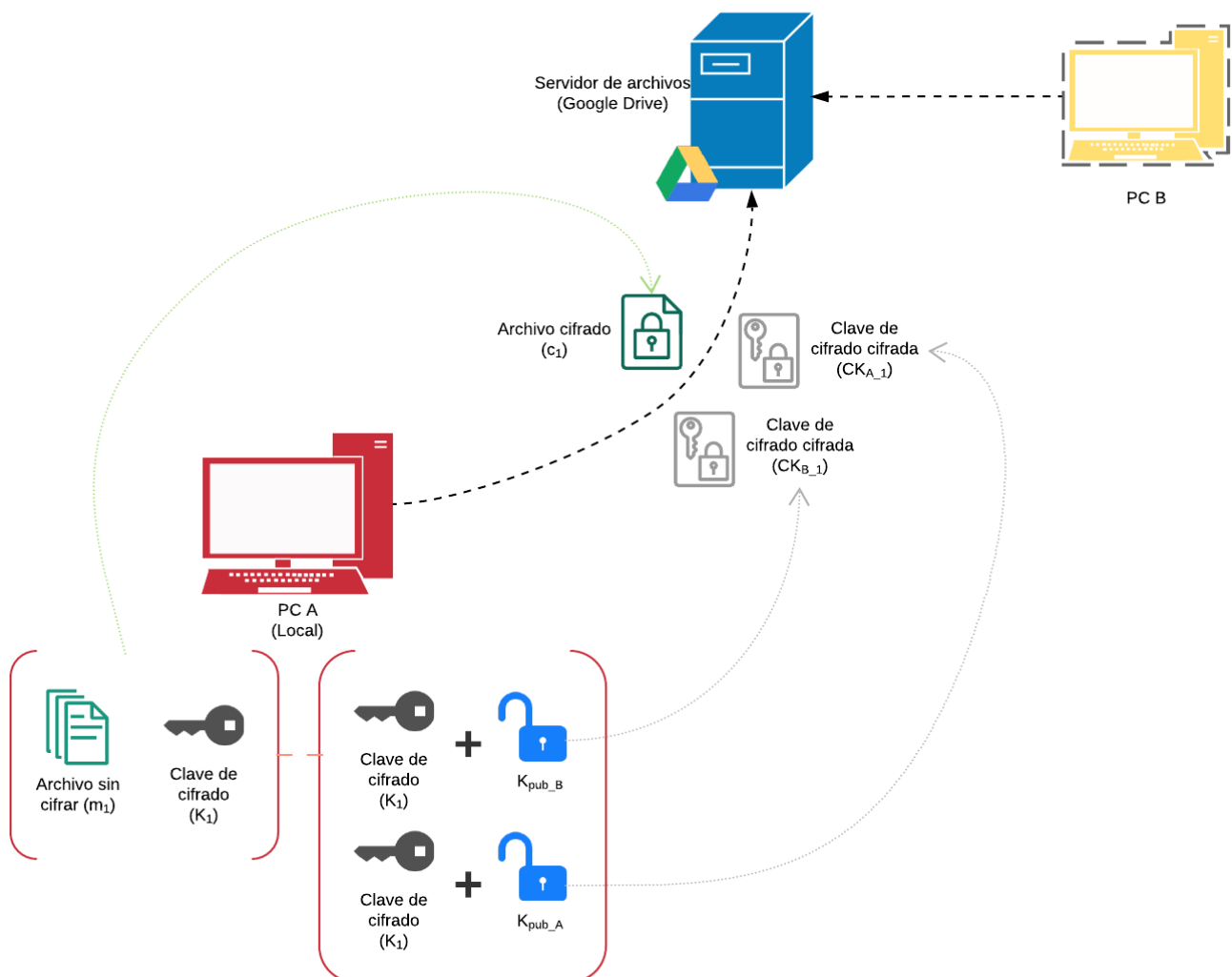
De esta forma, se consigue que una copia de seguridad almacenada una sola vez sea accesible para diferentes usuarios sin necesidad de compartir explícitamente el secreto de este archivo.



En la imagen anterior se detalla el resultado de ejecutar este caso de uso para un usuario *Angela* que decide subir una copia de seguridad del directorio *Pruebas* y compartirla con el usuario *Carlos*.

En la imagen se observa cómo se ha creado la copia de seguridad *Pruebas_2019_05_11_Angela* y como se ha creado su keyFile además de para el autor de la copia de seguridad, para el usuario con el que se comparte.

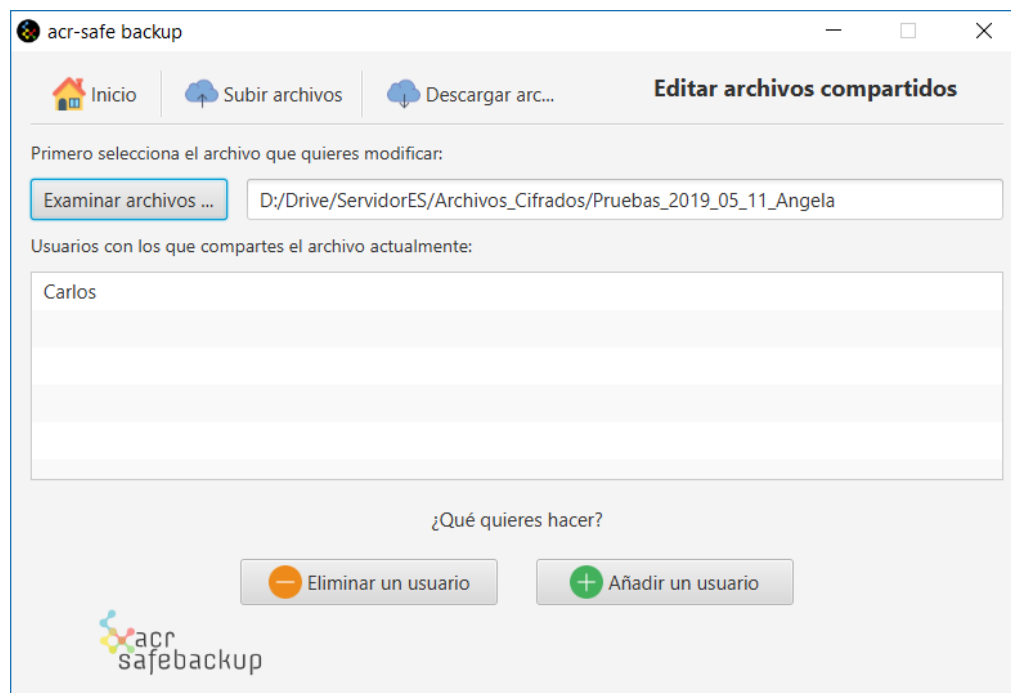
A continuación se adjunta un diagrama resumiendo todo el proceso:



EDITAR PERMISOS DE UNA COPIA DE SEGURIDAD

Una vez se ha subido una copia de seguridad a través de la aplicación, puede darse el caso de que se quieran editar los permisos de acceso de esta copia de seguridad y o bien quitarle permiso a un usuario para que no puede acceder a un determinado archivo, o bien compartirlo con otro usuario.

Para tener en cuenta esta situación, en la interfaz de usuario se ha añadido la siguiente vista:



A través de esta vista, un usuario puede elegir una de las copias de seguridad que haya realizado previamente y editar qué usuarios pueden acceder a esta copia.

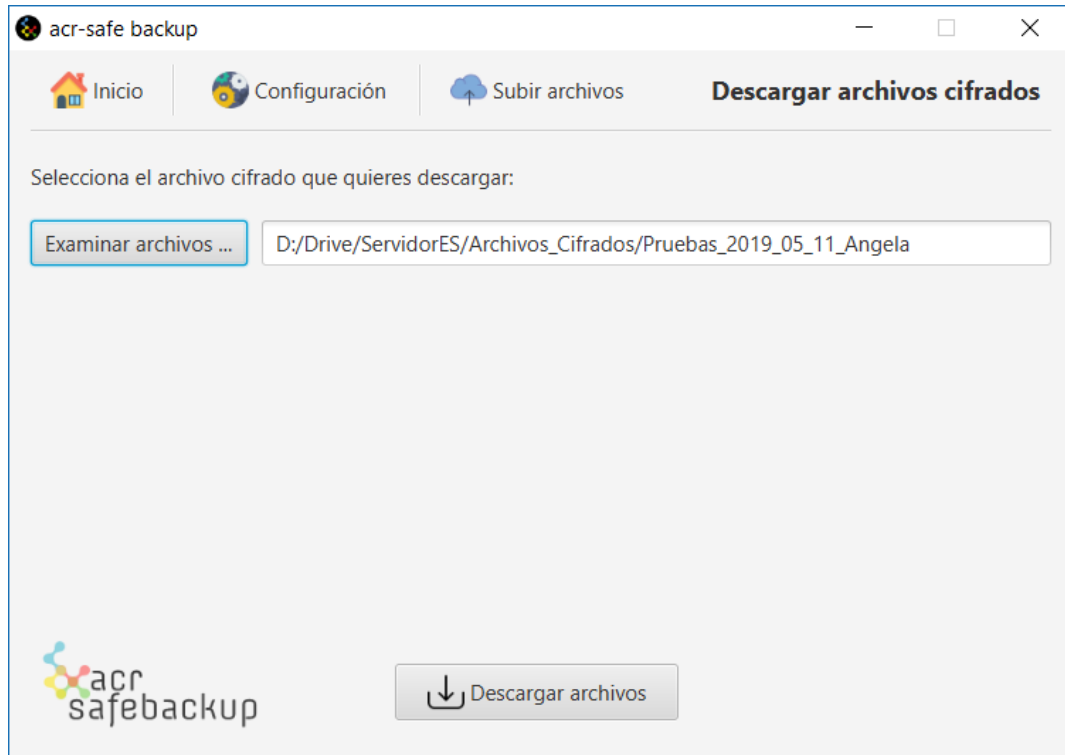
La opción eliminar un usuario permite evitar que un usuario pueda acceder a una copia de seguridad determinada. En este caso, el proceso únicamente consiste en eliminar su keyFile almacenada en el directorio `../ServidorES/Claves_Archivos/NombreUsuario`. Además, esta funcionalidad permitirá que, en caso de que el autor elimine el acceso a su propio usuario se elimine el acceso a todos los usuarios y se borre la copia de seguridad del directorio Drive.

Por otro lado, la opción de añadir un usuario es más compleja. El proceso consiste en conseguir la keyFile de esa copia de seguridad y cifrarla con la clave pública del nuevo usuario. Para conseguir esa keyFile se descifrá la keyFile del autor de la copia de seguridad y se cifrará posteriormente para el nuevo usuario tal y como se ha indicado en los casos de uso anteriores.

En este proceso se le pedirá al usuario su contraseña para poder descifrar la Clave privada encriptada con SHA-256 y después poder descifrar la keyFile encriptada con RSA.

DESCARGAR Y DESCIFRAR COPIAS DE SEGURIDAD

El último caso de uso consiste en la descarga y descifrado de las copias de seguridad subidas con la aplicación. A continuación, se adjunta la interfaz de la aplicación para este escenario:

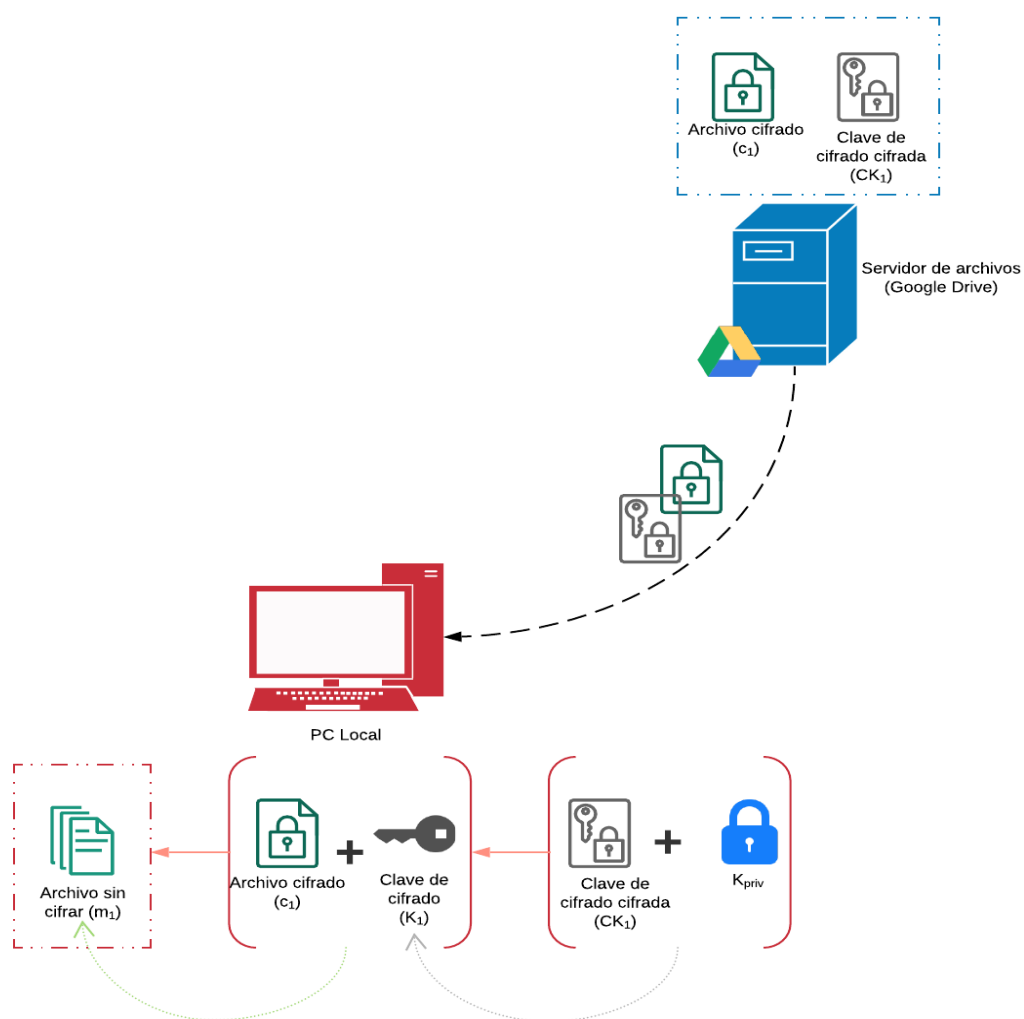


Una vez el usuario haya seleccionado el archivo de la copia de seguridad, se le requerirá su contraseña de usuario para empezar con el proceso de descarga.

En primer lugar, se descifrá la clave privada cifrada con SHA-256 a partir de la sal almacenada en el directorio de Drive y la contraseña introducida manualmente. Con esta clave privada se descifrá la keyFile del usuario cifrada con RSA y se descifrá el archivo cifrado con AES.

Al final de este proceso la copia de seguridad se almacenará como un .zip en el directorio que el usuario haya configurado en el primer caso *Configuración del escenario inicial*.

En la página siguiente se muestra un diagrama detallado para resumir el proceso de descarga.



TESTS

Para comprobar el correcto funcionamiento de la aplicación se han diseñado una serie de tests que ponen a prueba las diferentes funcionalidades de la práctica. Algunas de las comprobaciones que se han planteado tienen en cuenta las limitaciones o comprobaciones que pone la propia interfaz de la aplicación, así que no se han escrito dichos tests como parte del código del programa. A continuación, se detallan las diferentes comprobaciones que se han tenido en cuenta, divididas en las diferentes funcionalidades de la aplicación, así como el resultado obtenido.

CONFIGURACIÓN DEL ESCENARIO INICIAL

1. **Configurar el escenario inicial dejando campos vacíos.** En este caso la interfaz debería mostrar una ventana de error alertando que se deben rellenar todos los campos del formulario.
2. **Configurar un escenario para un usuario con caracteres especiales como “_”.** Este es un caso relevante porque podría dar problemas debido a que podría interferir con la forma de nombrado de archivos y dar errores en diferentes funcionalidades. Se debería mostrar un mensaje de error pidiendo solo utilizar caracteres alfanuméricos.
3. **Configurar el escenario inicial para un usuario que ya se ha configurado.** Esta situación puede darse cuando un usuario ya haya configurado el escenario inicial en otro ordenador, así que en este caso se mostrará un mensaje diciendo que ya se ha configurado el escenario para ese usuario, se harán los cambios necesarios para que se reconfigure la aplicación para dicho usuario, pero no se sobrescribirán las claves. De esta forma, evitamos que otra persona pueda “romper” un usuario que no es suyo.
4. **Introducir un directorio que no existe como directorio de Drive o como directorio de Descargas.** Se controla que los directorios introducidos tanto en un campo como en otro existan; en caso contrario se muestra un mensaje de error.
5. **Se introducen contraseñas diferentes o menores que el límite establecido.** En cualquiera de estos dos casos se mostrará un mensaje de error informando de que las contraseñas deben tener mínimo 8 caracteres y deben introducirse las dos iguales a modo de comprobación.
6. **Se introducen los directorios a mano y se escriben con “\”.** Este caso podría dar errores a la hora de gestionar ese String, para evitarlo no se mostrará ningún mensaje de error, pero se cambiarán los caracteres “\” por “/” antes de guardarlos en la aplicación.

SUBIR ARCHIVOS

1. **Intentar subir un archivo con el campo de examinar vacío.** Esta situación se comprueba desde la propia interfaz donde se verifica que el campo examinar se haya completado.
2. **Intentar subir un archivo que no existe.** Esta situación no puede darse porque en la interfaz se ha desactivado el campo para introducir el archivo que se desea subir de forma que solo pueda introducirse a través del botón examinar.
3. **Se introduce manualmente el archivo a cifrar y se introduce la ruta con “\” en lugar de “/”.** De la misma forma que en el escenario de configurar el escenario, se cambian automáticamente las “\” por “/”.
4. **Se intenta cifrar un archivo que tiene el carácter “_” en el nombre.** Este escenario podría dar problemas debido a que cuando se sube un archivo después se le pone como nombre “NombreArchivo_NombreUsuario”. Sin embargo, el código tal y como está planteado no presenta problemas en este escenario.
5. **Se sube un archivo que ya se ha subido al servidor.** Para permitir que se puedan almacenar varias copias de seguridad de un mismo directorio, se guardan con la fecha de subida. De esta forma si se suben varias copias de seguridad en diferentes días se almacenarán todas y si se suben el mismo día se almacenará sólo la última.
6. **Se sube un archivo compartido con otro usuario.** Este es un escenario normal en el cual se subirá el archivo cifrado una sola vez y la clave de cifrado del archivo se subirá una vez para cada usuario encriptándola con la clave pública del mismo.
7. **Se intenta compartir un archivo varias veces con el mismo usuario.** Este escenario no puede darse debido a como está planteada la interfaz de la aplicación; gal seleccionar de entre un listado de los usuarios “registrados” no puedes repetir varias veces al mismo usuario.
8. **Se sube un archivo con la contraseña incorrecta.** En este caso se muestra un error indicándole al usuario que la contraseña es incorrecta y se vuelve a mostrar el diálogo para introducir la contraseña.

EDITAR ARCHIVOS COMPARTIDOS

1. **Intentar editar los permisos sin introducir previamente un archivo en el campo examinar.** Tal y como está planteada la interfaz esta opción no puede darse debido a que si no se rellena el campo examinar no se activan los botones para editar los permisos.

2. **Intentar editar un archivo que no existe.** Esta opción se controla desde la interfaz; al pinchar en ‘examinar’ se selecciona un archivo de entre los existentes en el equipo.
3. **Se introduce un archivo que existe, pero no pertenece al servidor de la aplicación (directorio de Drive introducido al configurar el escenario inicial).** En la interfaz se muestra una ventana de alerta indicando que el archivo indicado debe estar entre los archivos que se han subido a la interfaz.
4. **Se intenta editar un usuario que pertenece a otro usuario.** En este caso se muestra un mensaje de error indicando que solo se pueden editar los archivos de los cuáles se es el autor.
5. **Al editar los permisos de un archivo te eliminas a ti mismo como uno de los usuarios que tiene acceso.** En este caso además de eliminar tu clave de acceso al archivo se borrará la de todos los usuarios y el propio archivo. De esta forma, se gestiona que no queden archivos que no puedan ser borrados desde la aplicación y se evita que el usuario tenga que borrar manualmente estos archivos.
6. **Intentar borrar un usuario que no tiene acceso o añadir a uno que ya tiene acceso.** Este escenario no puede darse debido a que la propia interfaz, en el caso de borrar usuarios muestra solo a aquellos que ya tienen permiso, y en el caso de añadir, a aquellos que aún no lo tienen.

DESCARGAR ARCHIVOS

1. **Se intenta descargar un archivo sin rellenar el campo de examinar archivo.** La aplicación gestiona que el campo debe ser rellenado antes de intentar descargar el archivo.
2. **Se intenta descargar un archivo que no pertenece al servidor.** Se muestra un mensaje de error indicando que el archivo a descargar debe pertenecer a la carpeta “Archivos_Cifrados” del servidor de la aplicación.
3. **Intentar descargar un archivo correcto pero sin introducir la contraseña.** Este escenario no puede darse debido a que la propia interfaz no desbloquea el botón “Aceptar” hasta que no se ha rellenado el campo de la contraseña.
4. **Intentar descargar un archivo correcto pero con una contraseña incorrecta.** Se muestra una alerta indicando que no se ha podido descargar el archivo indicado para que el usuario vuelva a introducir la contraseña.
5. **Se intenta descargar un archivo para el que no tienes acceso.** Se muestra un error indicando que no se ha podido descargar el archivo indicado.

- 6. Se intenta descargar un archivo correcto con la contraseña correcta.**
Tanto en un caso como en otro tras introducir la contraseña correcta se indicará mediante un mensaje que la descarga se ha hecho correctamente y se descargará un .zip con la copia de seguridad indicada.

MANUAL DE USUARIO. DEMOSTRACIÓN DE USO

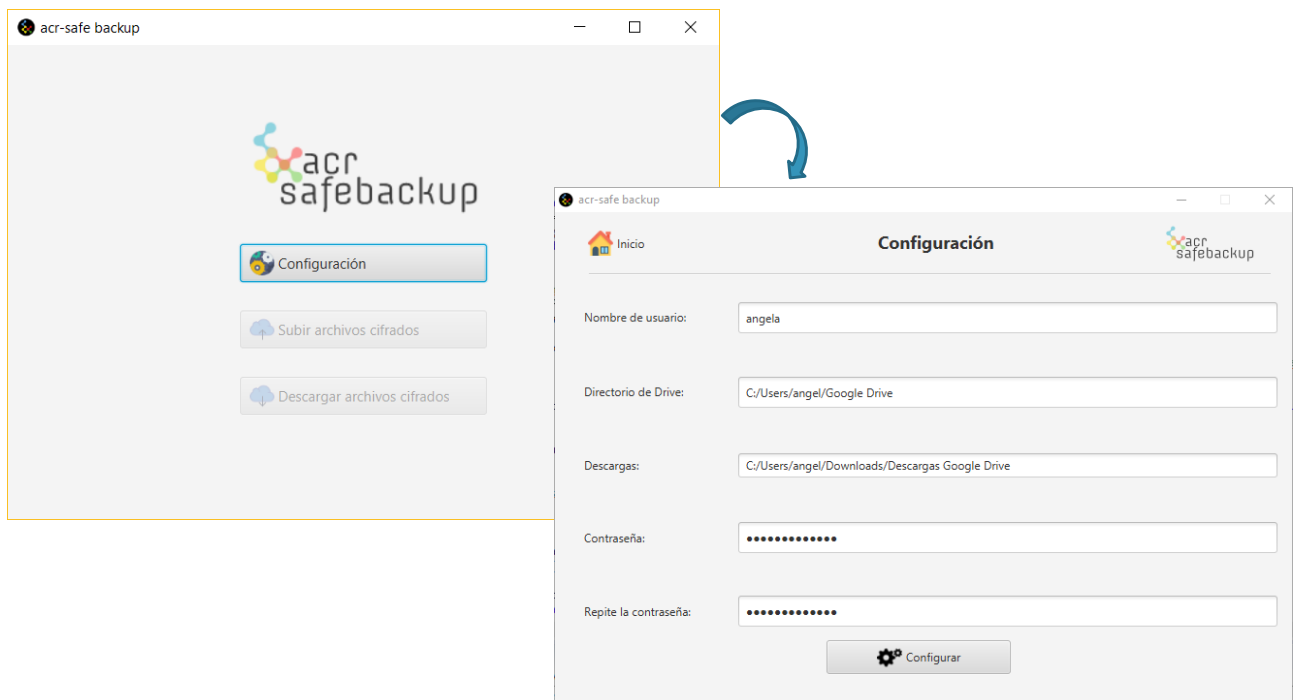
A continuación, se realiza la demostración de los diferentes casos de uso que se pueden dar en la aplicación. En primer lugar, se explica la configuración necesaria para poder utilizar la aplicación y posteriormente se exponen los casos de subir y descargar un archivo.

CONFIGURACIÓN

ESCENARIO INICIAL

La primera vez que se ejecute la aplicación veremos que solo está disponible la opción de configuración, una vez configurada podremos utilizar la aplicación en su totalidad.

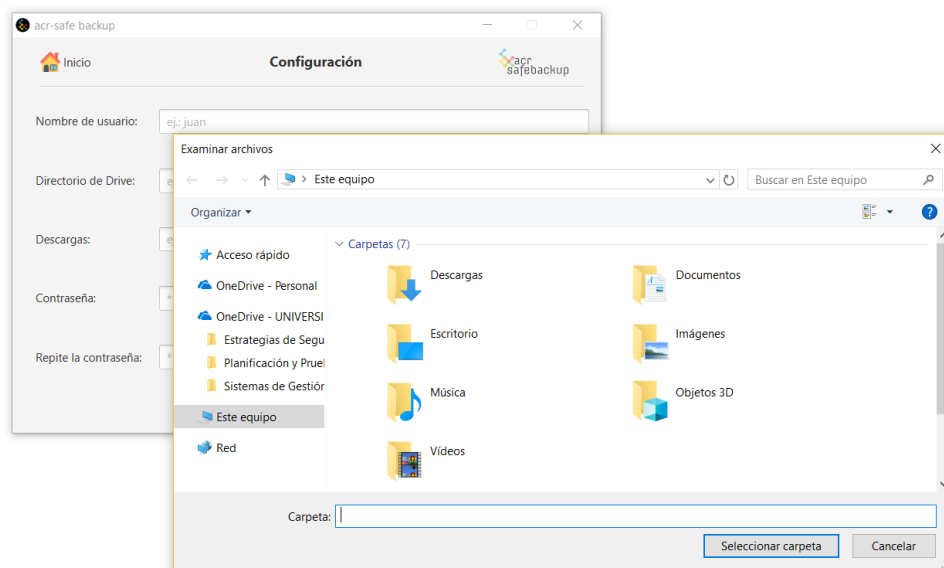
Al hacer click en el botón de configuración nos lleva a un formulario donde debemos rellenar todos los campos.



Cuando intentamos configurar la aplicación nos encontramos con algunas restricciones en los campos del formulario:

- Ningún campo puede estar vacío o ser únicamente espacios en blanco
- El nombre de usuario no puede contener ‘_’
- La contraseña no puede ser únicamente numérica y, además, se exige un mínimo de 8 caracteres.

* Observación: al intentar introducir el directorio donde se encuentra nuestra carpeta de Google Drive o el directorio donde se descargarán automáticamente los archivos descifrados, si pinchamos en el campo de introducción de texto nos aparece una ventana nueva donde podremos seleccionar cualquier fichero de nuestro sistema.



Al configurar la aplicación por primera vez se crean los directorios necesarios con los que trabajará. Si accedemos a la ubicación establecida para Google Drive observamos que se ha creado una nueva carpeta bajo el nombre “ServidorES”. Dentro de esta carpeta se generan los directorios necesarios: `archivos_cifrados`, `claves_archivos`, `claves_publicas` y `claves_privadas`.

Para evitar (en la medida de lo posible) malas acciones por parte de los usuarios en lo referido a las claves, etc. sólo será visible la carpeta “`archivos_cifrados`”; las demás se crearán con visibilidad oculta.

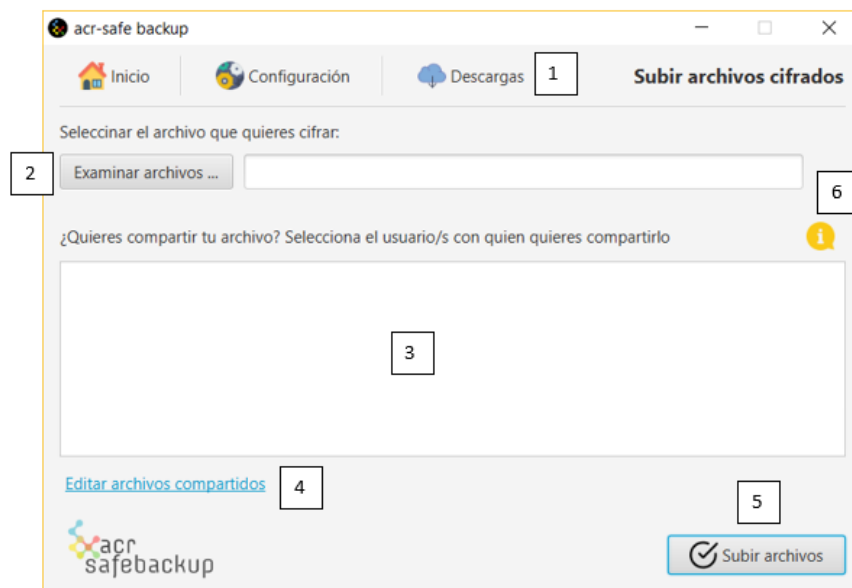
DIFERENTES DIRECTORIOS PARA EL MISMO USUARIO

La aplicación está pensada de manera que si tenemos dos dispositivos sincronizados con nuestra carpeta de Google Drive podemos hacer uso de esta en ambos dispositivos. Para ello, cuando queramos configurarla en el 2º dispositivo a la hora de la configuración debemos establecer el mismo nombre de usuario y contraseña (si ponemos otra contraseña no será actualizada) con las nuevas localizaciones.

SUBIR ARCHIVOS CIFRADOS

Tras realizar la configuración, seremos redirigidos automáticamente a la vista que nos permitirá subir los archivos. El fichero seleccionado por el usuario no estará cifrado, es la aplicación la que se encarga de cifrarlo y subirlo directamente a nuestra carpeta de Google Drive.

PRESENTACIÓN DE LA VISTA



1 > Menú de navegación superior que nos permite navegar entre las diferentes pantallas (o vistas) que tiene la aplicación. Se encuentra en todas las vistas excepto en la pantalla inicial y en el formulario de configuración.

2 > Botón de examinar ficheros: al pinchar en este botón se abre un diálogo para que el usuario seleccione el fichero que quiere subir de su sistema.

3 > Lista de usuarios con los que se puede compartir el archivo. Dado que la aplicación trabaja con la carpeta que tenemos sincronizada en Google Drive, si dicha carpeta la compartimos con más personas podremos seleccionar de forma concreta quién podrá descifrar los archivos compartidos.

4 > Icono informativo. Al pasar por encima del icono (sin necesidad de clickar en él) aparece un recuadro con ayuda para seleccionar varios usuarios. Esto puede hacerse con CTRL o utilizando SHIFT; igual que cuando seleccionamos varios ficheros en el sistema.

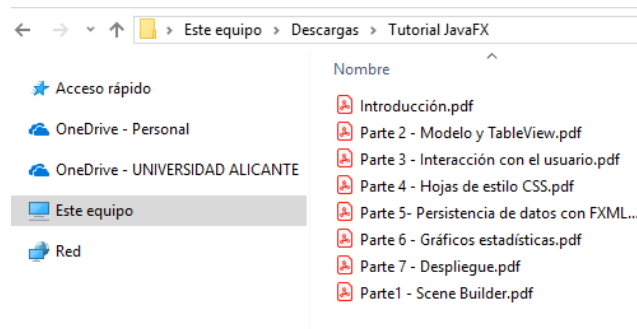
5 > Link para modificar los permisos de los usuarios a los que compartimos el archivo. Al clickar en el link accederemos a una pantalla donde podremos añadir o eliminar usuarios de un archivo determinado. Esta funcionalidad se comenta más detenidamente en páginas siguientes.

6 > Botón de subir archivos: al pinchar en el botón se realizan todas las comprobaciones necesarias y solicita la contraseña al usuario; si todo es correcto se procede al cifrado del archivo. En caso de que se produzca algún error (por ejemplo, al abrir el archivo seleccionado) se mostrará un mensaje alertando al usuario. Si todo va bien, cuando se haya cifrado y subido el archivo se mostrará un mensaje informando al usuario. A partir de ese momento puede acceder a la vista de descargas desde el menú superior y descargar el archivo que acaba de cifrar.

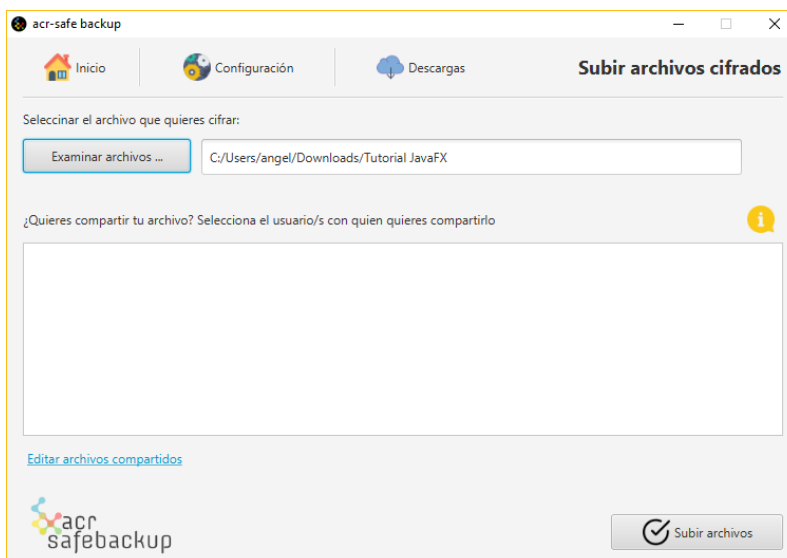
DEMOSTRACIÓN

Para esta demostración vamos a subir un fichero que contiene varios archivos PDF (Tutorial JavaFX) y accederemos a la carpeta de Google Drive para ver que realmente se ha cifrado.

El archivo en cuestión que se va a utilizar se ve de la siguiente manera antes de cifrarlo:



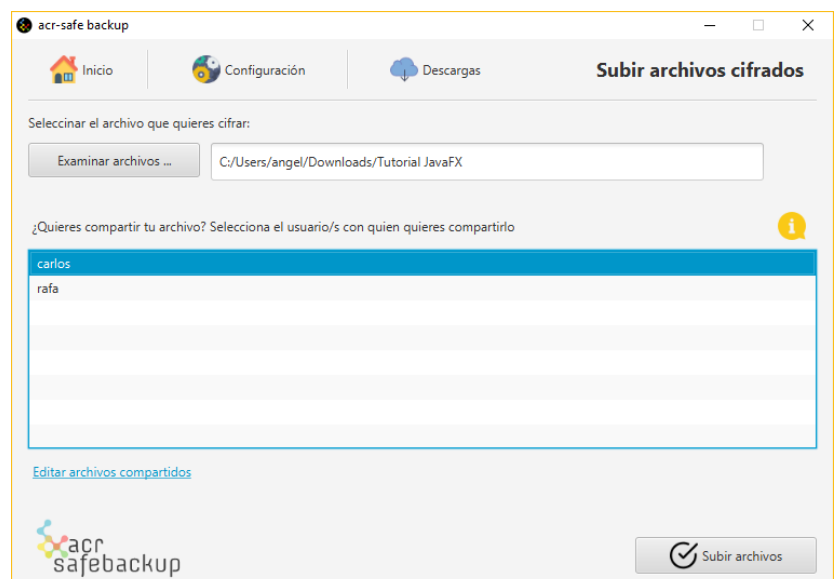
En primer lugar seleccionamos el archivo de nuestro sistema que queremos subir haciendo uso del botón 'Examinar archivos ...'.



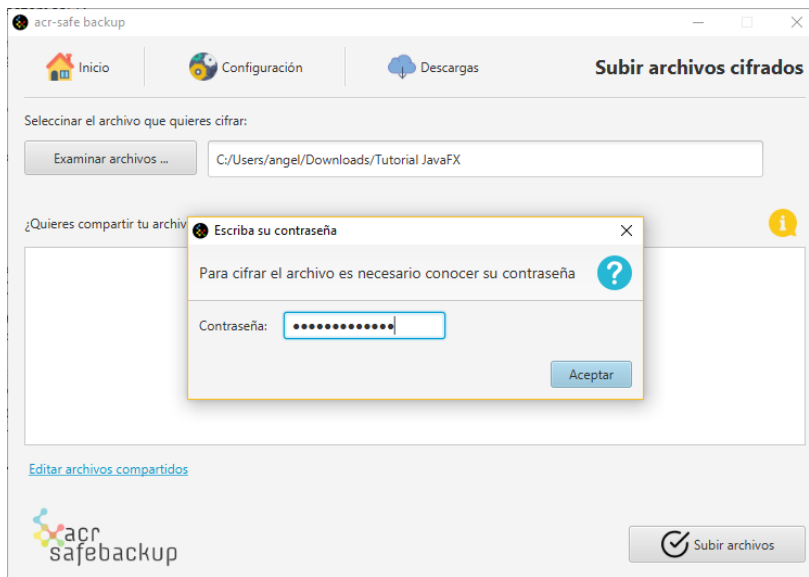
Vemos que en la lista de usuarios no aparece ninguno dado que la carpeta no se ha compartido todavía.

En el siguiente apartado se muestra cómo añadir usuarios de forma manual.

En el caso de que sí haya más usuarios en la carpeta se mostrarán en la lista y podremos seleccionar aquellos que queramos.



El siguiente paso, dado que no hay usuarios a los que compartir, es subir el archivo. Cuando clicamos en el botón nos pide que ingresemos la contraseña:



Si todo funciona correctamente nos aparece un mensaje de éxito para informar al usuario que todo ha ido correctamente. En caso contrario se muestra un mensaje de error, notificando el error que se ha producido.

Una vez cifrado, cuando accedamos a la carpeta e intentemos abrir el archivo veremos que está cifrado.

MODIFICAR PERMISOS

Si hemos subido un archivo y no lo hemos compartido con nadie y queremos añadir a alguien o por el contrario queremos quitarle los permisos de acceso a un usuarios debemos utilizar esta vista.

PRESENTACIÓN DE LA VISTA



1 > Menú de navegación superior.

2 > **Botón de examinar archivos.** Permite al usuario seleccionar el archivo cifrado sobre el que quiere realizar algún cambio en los permisos otorgados a otros usuarios (es decir, añadir otros usuarios en la copia compartida del archivo o eliminar a alguno existente).

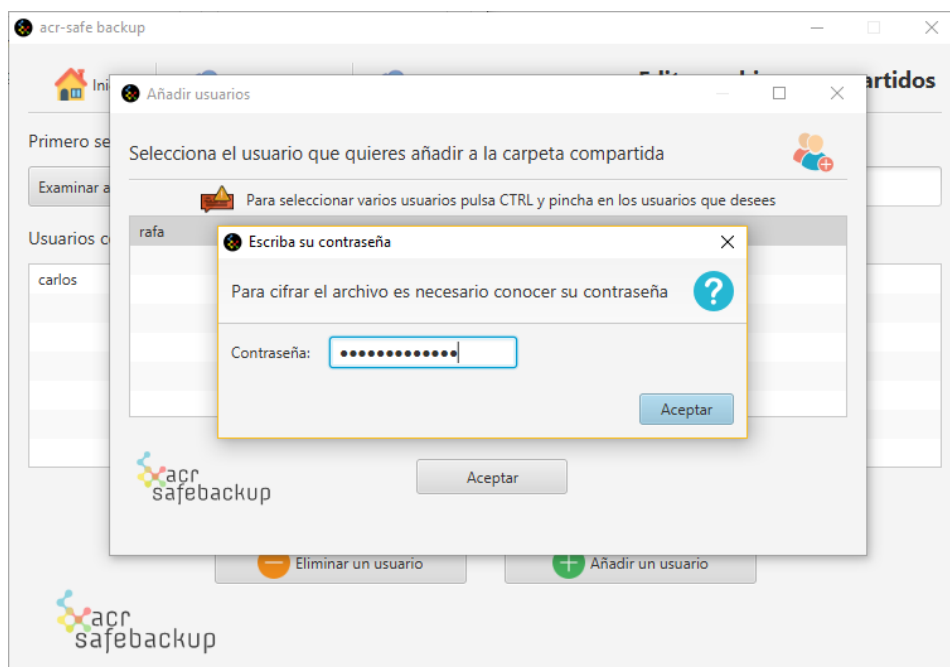
3 y 4 > **Botones que permiten realizar las funciones de eliminar a un usuario** de manera que ya no tenga acceso a la copia cifrada del archivo compartido (3) **o añadir a otro usuario** para compartir el archivo con el también (4). Estos dos botones no se activan hasta que el usuario selecciona el archivo sobre el que quiere realizar cambios.

5 > **Lista de usuarios con los que se comparte el archivo.** Esta lista se actualizará si se añade o se elimina algún usuario.

DEMOSTRACIÓN – AÑADIR USUARIOS

Cuando queremos añadir un nuevo usuario al archivo debemos hacer clic en el botón 'Añadir usuario'. Entonces no aparecerá un cuadro de diálogo con una lista de los usuarios disponibles y con los que no hemos compartido dicho archivo. Seleccionamos uno o varios y pulsamos aceptar. A partir de ese momento se generan los archivos cifrados de la clave cifrados con la clave pública del otro usuario para que puedan descargarlo y ver su contenido.

Primero seleccionamos los usuarios que queremos añadir y pulsamos aceptar. Acto seguido, debemos introducir la contraseña.

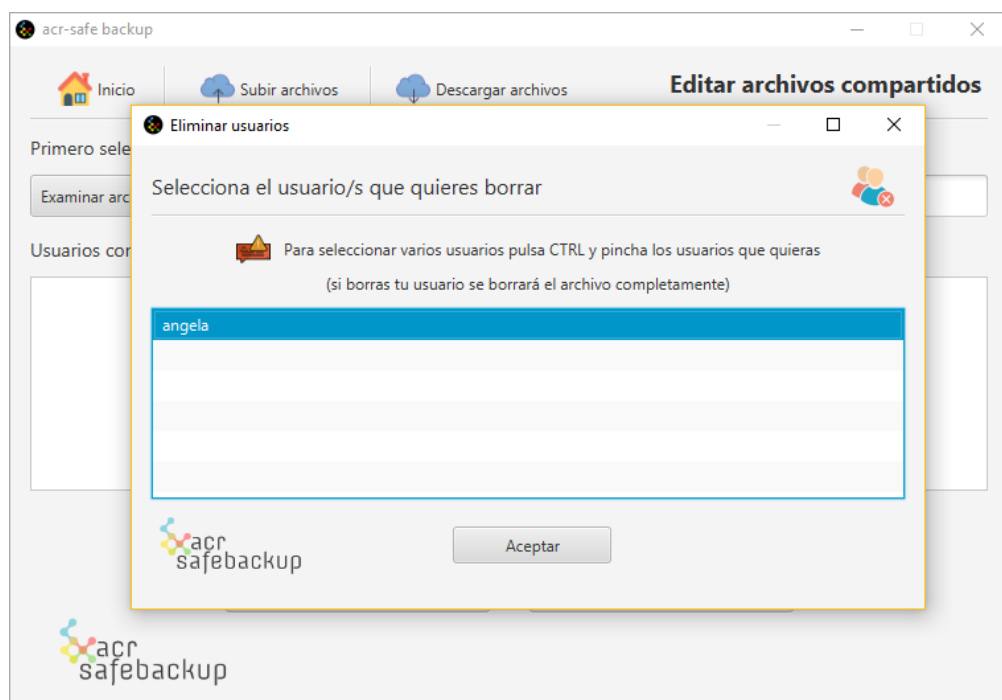


Si todo va bien seremos redirigidos a la vista anterior (vista de editar permisos) y veremos que la lista de usuarios con los que se comparte el archivo se ha actualizado:

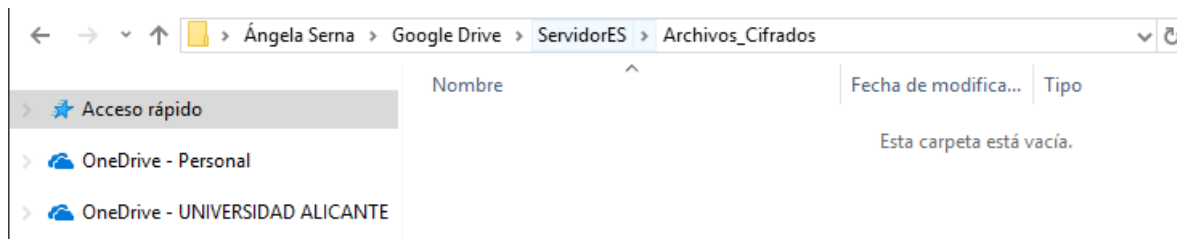


DEMOSTRACIÓN – ELIMINAR USUARIOS

A la hora de eliminar usuarios se pueden dar dos casos: que el usuario seleccionado sea no propietario en cuyo caso se le quitan los permisos y listo o, por el contrario, que sea el propietario del archivo. En este último caso no solo se elimina el usuario, sino que también se elimina el archivo. Es decir, cuando en la selección de usuarios se selecciona al propietario de este se elimina por completo el archivo (el archivo en sí, las claves generadas, etc.) y, por lo tanto, nadie podrá acceder a él.



Si accedemos ahora a la carpeta de archivos_cifrados observaremos que está vacía.

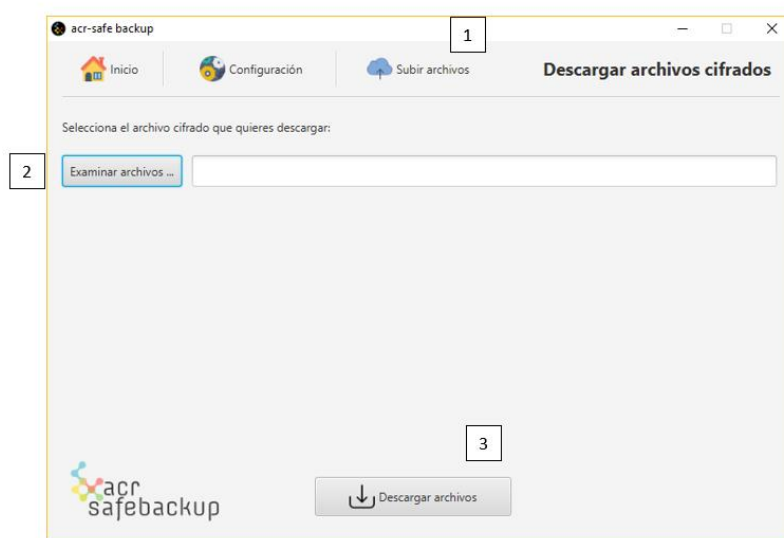


DESCARGAR ARCHIVOS

Una vez que el usuario ha subido algún fichero cifrado a la carpeta correspondiente, será capaz de descargarlo directamente descifrado puesto que la aplicación se encarga de descifrarlo y descargarlo automáticamente en el directorio establecido en el formulario de configuración.

Cualquier intento de descargar un archivo que no se haya cifrado previamente por la aplicación (esto es que pertenezca a cualquier otro directorio del sistema o que se encuentre en la carpeta correspondiente pero no se haya cifrado previamente por la aplicación).

PRESENTACIÓN DE LA VISTA



1 > Menú de navegación superior.

2 > Botón de examinar archivos: al pinchar en este botón se abre un diálogo en el directorio de la carpeta que contiene los archivos cifrados para que el usuario seleccione el archivo que quiere descargar.

3 > Botón de descarga de archivos. Al hacer clic en el botón se realiza de forma automática el descifrado y el guardado del archivo (en formato .zip) en el directorio establecido previamente por el usuario.

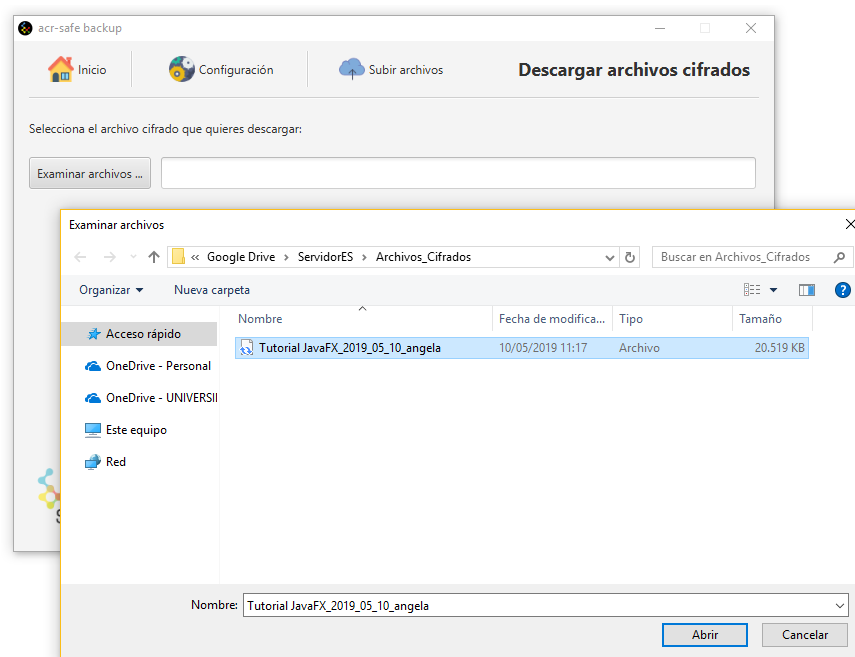
Al igual que pasa en la pantalla de subir archivos, aquí también se realizan las comprobaciones pertinentes y se solicita la contraseña al usuario. Si se produce algún error, como puede ser que la contraseña no sea correcta, un mensaje de error alerta al

usuario y, en caso contrario, cuando el archivo se haya descifrado y almacenado en el sistema sale un mensaje informando del éxito de la operación.

DEMOSTRACIÓN

Para esta parte de la demostración vamos a realizar la descarga del archivo que se ha subido en la primera demostración (Tutorial JavaFX) y accederemos al directorio establecido como descargas para comprobar que todo ha ido correctamente. En este caso tenemos que ver un .zip generado en el directorio correspondiente y que al extraerlo podemos acceder a su contenido sin problemas.

Al igual que en el caso de subir archivos, para descargar alguno ya cifrado primero debemos seleccionar dicho archivo de los que están presentes en la carpeta “archivos_cifrados”.



Una vez que hayamos introducido la contraseña (como cada vez que se realiza alguna operación sobre los archivos) si todo ha ido correctamente no aparece un mensaje informativo y al acceder a la carpeta de destino podremos comprobar el archivo:

