

UNIVERSIDAD DE ALMERÍA
ESCUELA SUPERIOR DE INGENIERÍA
INGENIERÍA EN INFORMÁTICA



***Herramienta de encriptación adicional para almacenamientos
virtuales***

Alumno: Eduardo Ballesta Caparrós

Directores: Leocadio González Casado

Juan Álvaro Muñoz Naranjo

Fecha: 21 de Diciembre de 2011

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

P.F.C: *Herramienta de encriptación adicional para almacenamientos virtuales.*

Agradecimientos a Leocadio González Casado y Juan Álvaro Muñoz Naranjo por su trabajo y apoyo incondicional.

1. INTRODUCCIÓN A LA HERRAMIENTA KONENCRIPCIÓN	5
1.1. MOTIVACIONES	5
1.2. CLOUD COMPUTING	6
1.2.1. Breve historia de la aparición del Cloud Computing	8
1.2.2. Tipos de servicios que ofrece Cloud Computing	8
1.2.3. Ventajas y desventajas del Cloud Computing	10
1.3. HERRAMIENTAS ACTUALES PARA ALMACENAMIENTO VIRTUAL	12
1.3.1. Dropbox, Ubuntu One y SpiderOAK	12
1.3.2. Servicios ofertados	12
1.4. HERRAMIENTAS COMPLEMENTARIAS DE SEGURIDAD	18
1.4.1. SecretSync	19
1.4.2. TrueCrypt	20
1.4.3. Ubuntu One Encrypt/Decrypt	20
2. DESCRIPCIÓN DE LOS OBJETIVOS	22
2.1. PROBLEMAS LEGALES DE DROPBOX	22
2.2. PROBLEMAS ACTUALES DE SEGURIDAD DE DROPBOX	24
2.2.1. Problemas de suplantación de identidad	24
2.2.2. Confianza Transitiva	25
2.2.3. Ausencia de cifrado	27
2.2.4. Falta de funcionalidad de las herramientas complementarias de seguridad	28
2.3. SOLUCIÓN DE PROBLEMAS	28
2.3.1. Establecer contraseña de KonEncriptación diferente a la de Dropbox	28
2.3.2. Sistema de cifrado local	29
2.3.3. Validación de confianza transitiva	30
2.3.4. Integración con Dropbox	30
2.4. HERRAMIENTAS DE DESARROLLO	31
2.4.1. Herramientas criptográficas empleadas	31
2.4.2. Otro tipo de herramientas utilizadas	32
3. GESTIÓN DE ARCHIVOS CIFRADOS	34
3.1. ESTRATEGIAS DE CIFRADO	34
3.1.1. Validación de parámetros de inicio de sesión	34
3.1.2. Generación de claves asimétricas basadas en contraseña	36
3.1.3. Generación de claves simétricas	36
3.1.4. Envoltura de la clave simétrica con clave pública	37
3.1.5. Desenvoltura de clave simétrica con clave privada	38
3.1.6. Cifrado de la información con clave simétrica	38
3.2. CIFRADO Y DESCIFRADO DE ARCHIVOS	39
3.2.1. ESTRUCTURA DE UN ARCHIVO CIFRADO	39
3.2.2. Proceso de cifrado de archivos	40
3.2.3. Proceso de descifrado de archivos	41
3.3. POLÍTICAS DE ACCESO	42
3.4. GESTIÓN DE PETICIONES DE ACCESO	43
4. DISEÑO E IMPLEMENTACIÓN DE LA HERRAMIENTA KONENCRIPCIÓN	56
4.1. DISEÑO DEL MENÚ CONTEXTUAL DE DROPBOX	56
4.2. CONCESIÓN DE PERMISOS MEDIANTE LA AGENDA DE USUARIOS	61
4.3. VERIFICACIÓN DE LA CORRECTA CORRESPONDENCIA ENTRE DROPBOX Y KONENCRIPCIÓN	64
4.4. CONSIDERACIONES SOBRE LA EDICIÓN, ELIMINACIÓN Y RENOMBRAMIENTO DE ARCHIVOS Y DIRECTORIOS	67

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

4.5.	USO DE THREADS EN LA EJECUCIÓN DE OPERACIONES	68
4.6.	USO DE DAEMONS.....	68
4.7.	IMPLEMENTACIÓN	70
4.7.1.	Clases	70
4.7.2.	APIS externas utilizadas	73
5.	MANUAL DE USUARIO	78
5.1.	REQUISITOS.....	78
5.2.	INSTALACIÓN	78
5.5.	ELEMENTOS DE LA VENTANA PRINCIPAL DE LA APLICACIÓN	90
5.6.	OPERACIONES ENTRE DIRECTORIOS	98
5.7.	OPERACIONES LOCALES.....	101
5.8.	OPERACIONES INTEGRADAS DE DROPBOX	128
5.9.	OTRAS OPERACIONES.....	136
5.10.	SALIDA DE LA APLICACIÓN	145
5.11.	DESINSTALACIÓN	145
6.	BIBLIOGRAFÍA	148
6.1.	REFERENCIAS.....	148
6.2.	GLOSARIO DE TÉRMINOS	151

1. Introducción a la herramienta KonEncriptación

La aplicación desarrollada en este Proyecto Final de Carrera, *KonEncriptación*, pretende dar solución a uno de los principales problemas de seguridad que tiene actualmente la mayoría del software de almacenamiento virtual en la nube: *la falta de seguridad de la información almacenada local y remotamente*. Para ello *KonEncriptación* ofrece la posibilidad a los usuarios de la herramienta de trabajar con la información en claro, sin cifrar, en un directorio local y mantenerla cifrada en el directorio asociado a la cuenta de *Dropbox*. La herramienta ofrece además un abanico de operaciones de edición de archivos y directorios con los que el usuario podrá trabajar cómoda y directamente desde *KonEncriptación*.

KonEncriptación utiliza también una técnica de gestión de cifrado para grupos mediante peticiones de acceso, novedosa para este tipo de software, y con la que se permite compartir información cifrada entre usuarios con los que se comparten carpetas. Además, esta técnica se ha complementado con una agenda de usuarios colaboradores que facilita la gestión de las claves de usuarios y el trabajo colaborativo con ellos.

Por último, hacer hincapié en que hoy en día es difícil encontrar software adicional de cifrado que se integre con servicios de almacenamiento virtual y *KonEncriptación* lo está completamente con *Dropbox*. Se ha escogido para el desarrollo de *KonEncriptación* a *Dropbox* debido a que es uno de los servicios de almacenamiento virtual más conocidos y más controvertidos en cuanto a seguridad se refiere.

1.1. Motivaciones

Hoy en día la gran mayoría de servicios disponibles en el mercado que ofrecen almacenamiento virtual en la nube, ya sea de manera gratuita o mediante pago, incluyen sus propios métodos de seguridad, integridad y transporte de la información desde nuestro equipo a la nube y viceversa, así como almacenamiento en la misma. Además, para ofrecer mayor confianza al usuario, los desarrolladores de estas aplicaciones redactan cláusulas donde indican que ellos no podrán nunca tener acceso a los datos alojados sino únicamente a los metadatos. Para usuarios domésticos donde, en la mayoría de los casos, la privacidad de su información no es siempre un aspecto crucial, aplicaciones tan conocidas como: ***Dropbox, Ubuntu One o SpiderOAK*** son muy atractivas por su comodidad y facilidad de uso. Además, estas aplicaciones permiten al usuario mantener un pequeño back up de su información más relevante en la nube de manera actualizada y sin ningún tipo de preocupación. Pero, *¿qué sucedería si alguien accediera a la cuenta de un usuario y tuviera acceso a sus datos?* En el caso de una gran empresa que utilice este tipo de sistema para almacenar información muy valiosa en la nube sería una situación muy comprometida. Según estudios realizados por la Universidad de California sobre servicios de *Cloud Computing*, o *computación en la nube*, se han detectado ataques contra la memoria compartida de algunos servidores con el robo o la destrucción de información como objetivo [1]. Las previsiones de uso de servicios de almacenamiento virtual apuntan a un gran crecimiento de éstos, que con toda seguridad irá acompañado de un mayor número de ataques.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Estos problemas descritos han provocado que los usuarios con mayores conocimientos informáticos utilicen técnicas de encriptación complementarias para poder tener así la información más protegida, como se verá con más detalle en el **apartado 1.4**. *TrueCrypt* es un ejemplo de ello. Se trata de una herramienta de encriptación usada para el cifrado adicional en software de almacenamiento virtual. Sin embargo, el hecho de que el almacenamiento en la nube no sea para *TrueCrypt* uno de sus objetivos originales la hace poco flexible de cara al usuario para esta finalidad. Además, actualmente existe una única herramienta asociada específicamente a un software de almacenamiento virtual que también será analizada en el **apartado 1.4**, *SecretSync*. Su finalidad es ofrecer una mayor seguridad y opacidad de la información ante posibles ataques externos o ante el acceso y uso indebido de dicha información por parte de los mismos administradores del servicio de almacenamiento virtual. Se trata de una herramienta básica y fácil de utilizar, pero no resuelve todos los problemas afrontados en este proyecto.

Por otra parte, prácticamente todos los almacenes virtuales estudiados utilizan métodos de sincronización selectiva y continua, para mantener actualizados los datos del usuario con la nube. Es decir, cada vez que se está editando un fichero y se guardan las modificaciones, los datos modificados se sincronizan con el servidor. Esta forma de sincronización es efectiva en los casos en la que la información pertenece a un solo usuario y es editada únicamente por él, pero conlleva problemas cuando son varios usuarios los que pueden trabajar con una carpeta compartida y editar su contenido de forma concurrente. El problema de las aplicaciones que ofrecen este tipo de servicio es que dan la sensación de ser una herramienta colaborativa cuando no lo son del todo. A diferencia de las herramientas colaborativas, cada usuario trabaja con una copia local que luego se sincronizará con el servidor, prevaleciendo siempre la última modificación realizada. Esto lleva a que el usuario siempre esté en constante riesgo de perder su trabajo cuando trabaja con archivos compartidos al mismo tiempo que otros usuarios. La solución ofrecida por *Dropbox* para este tipo de problemas es un repositorio Web donde mantiene un historial de todos los cambios realizados en los últimos 30 días y donde permite a sus usuarios deshacer cambios en sus ficheros o carpetas modificados en caso de que haya ocurrido algún tipo de desastre como: modificación indeseada, corrupción de archivos, recuperación de archivos eliminados o edición simultánea. En el caso de edición simultánea, *Dropbox* también genera un archivo donde indica al usuario que ha habido conflictos en la edición cuando ambos dejen de usar ese archivo.

Todos estos problemas descritos en este apartado son los que nos han motivado a buscar las soluciones que se proponen a lo largo de este proyecto y que han sido plasmadas e integradas en la herramienta KonEncriptación.

1.2. Cloud Computing

El término “la *nube*”, como la mayoría del mundo conoce, es sinónimo de Internet. Si traducimos *Cloud Computing* al español como **computación en la nube** y nos ceñimos a esta traducción su significado sería: **ofrecer servicios de computación en Internet** [6].

Realmente estamos ante una nueva tecnología que ha roto con el modelo de aplicación tradicional existente mediante el ofrecimiento de servicios similares, gratuitos o no, en Internet.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Actualmente, existen diferentes empresas especializadas en este campo que ofrecen distintos tipos de servicios a sus clientes. Además, todos estos servicios se encuentran localizados en *centros de datos (Clouds privadas)* que pertenecen a dichas empresas. Mediante estos servicios se ofrecen diversos tipos de ventajas, como no tener que ocuparse del mantenimiento de las aplicaciones o de la seguridad en tránsito de su información, lo que les hace muy atractivos.

Las principales características del Cloud Computing [5] son:

- **El nivel de abstracción que hay detrás del servicio pasa desapercibido para el cliente:** el servicio final y el buen funcionamiento de este es lo más importante.
- **Accesibilidad y multiplataforma:** los servicios suelen estar disponibles para acceder a ellos desde distintos tipos de equipos: portátiles, dispositivos móviles, y desde distintos tipos de plataformas: Linux, Windows y MAC.
- **Multiusuario:** ofrecer distintos tipos de servicios de un mismo software dependiendo de las necesidades y exigencias de los clientes.
- **Auto-reparable y seguro:** en caso de fallo, el último back up de la aplicación pasa a ser automáticamente la copia primaria. Ofrece, además, un tratamiento seguro de la información mediante: *métodos de autenticación, transporte, cifrado de la información, entre otros.*
- **Escalable:** si el número de clientes de un servicio incrementa, la calidad en los servicios debe mantenerse. De esta manera, este tipo de sistemas son escalables para asegurar un buen del servicio.
- **Servicio virtualizado:** las aplicaciones son independientes del hardware en el que corren. Por ejemplo, varias aplicaciones pueden correr en una misma *máquina virtual* o una aplicación puede usar varias *máquinas virtuales* para realizar su propósito.
- **Multipropósito:** el sistema está creado de tal forma que permite a diferentes clientes compartir las infraestructuras sin preocuparse de ello y sin comprometer su seguridad y privacidad.
- **Supervisión de los recursos:** controlan y optimizan el uso de los recursos de manera automática. De esta forma, el uso de los recursos puede monitorizarse, controlarse y notificarse, aportando transparencia tanto al proveedor como al consumidor del servicio.
- **Cambio en la filosofía de trabajo mediante Internet:** utilizar Internet como un servicio que le permite al usuario prescindir de la necesidad de almacenar datos localmente o requerimientos físicos (hardware) para poder procesar la información. En consecuencia, el programa (software) pasa a ser un servicio.

Los principales proveedores de Cloud Computing son: *Amazon, Windows Azure, Blue Cloud de IBM o Google App.*

1.2.1. Breve historia de la aparición del Cloud Computing

La definición de computación en la nube comenzó a utilizarse sobre 2006 cuando Amazon Server ofreció su servicio *EC2 (Elastic Compute Cloud)* donde ofrecían a empresas e instituciones la posibilidad de alquilar espacios en servidores virtuales para almacenar sus datos y sus propias aplicaciones. De esta manera, las empresas que aceptaban este servicio no necesitaban tener servidores ni encargarse del mantenimiento de estos. Esto les suponía una reducción de costes y un aumento importante de la eficacia. De esta forma, fue como poco a poco se fue integrando lo que hoy se conoce como *Computación en la nube*.

1.2.2. Tipos de servicios que ofrece Cloud Computing

Los servicios ofrecidos por el Cloud Computing están orientados principalmente a empresas aunque también existen servicios que están orientados a todo tipo de usuarios.

Generalmente, el Cloud Computing ofrece tres tipos de servicios diferentes: *IaaS (Servicio como una Infraestructura)*, *SaaS (Software como un Servicio)* y *Paas (Plataforma como un servicio)*.

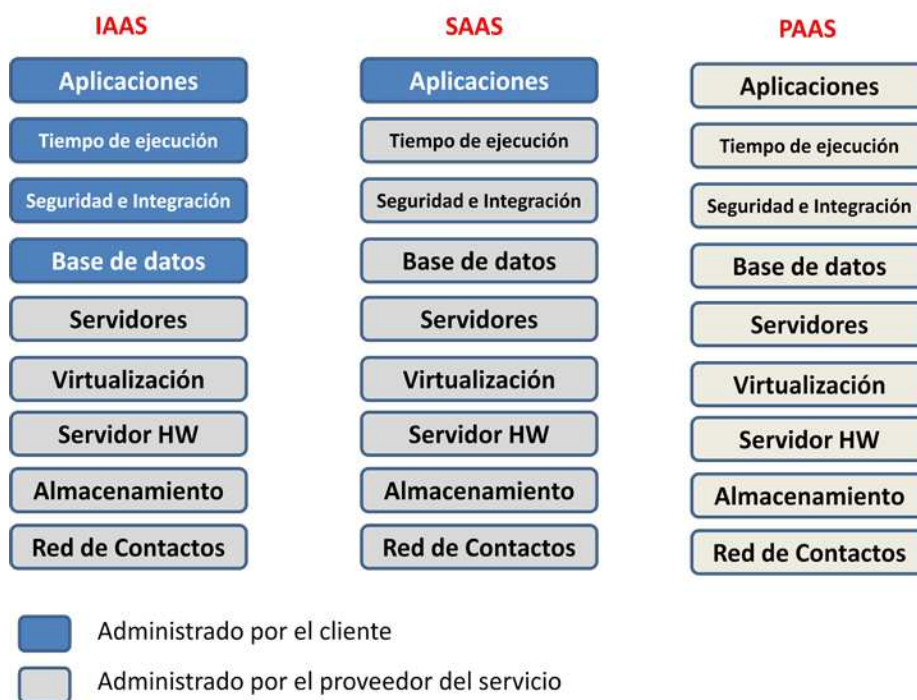


Figura 1: Esquema de tipos de Servicios ofrecidos por Cloud Computing.

Como se aprecia en la **Figura 1** un servicio, sea cual sea su nivel, se divide en varias partes (*recursos*) que son comunes a los diferentes tipos de servicios. Estos recursos son:

- Aplicaciones.
- Tiempos de ejecución.
- Seguridad e integración.
- Base de datos.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Servidores.
- Virtualización.
- Servidores físicos.
- Almacenamiento.
- Red.

Y en función de cuál sea el tipo de servicio demandado la gestión de algunos de estos recursos serán realizados por parte del cliente o del proveedor de estos servicios.

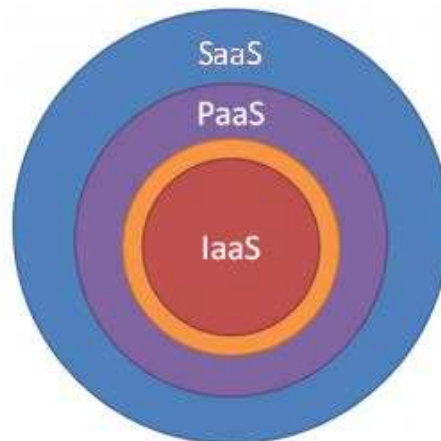


Figura 2: Esquema a nivel de capas de los distintos servicios ofrecidos por Cloud Computing.

1.2.2.1. Infraestructura como un servicio (IaaS)

IaaS se corresponde con el núcleo de los servicios ofrecidos en *Cloud Computing* [14]. En esta capa interior, los proveedores ofrecen un servicio de aprovisionamiento de infraestructuras tales como almacenamiento, hardware, servidores, etc. para evitar al cliente el gasto que supone la adquisición y mantenimiento de estos. De esta forma, los clientes realmente lo que contratan son capacidades como servicio y pagan en función de estas. Por ejemplo, capacidad de procesamiento, de almacenamiento o de ancho de banda. La técnica utilizada por los proveedores para ofrecer este servicio es la *virtualización de la plataforma*. Esta es una técnica donde se utilizan equipos suficientemente potentes o configurados para trabajar en paralelo, utilizando *máquinas virtuales* configuradas para soportar los servicios demandados por sus huéspedes [15].

Este tipo de servicio es útil cuando los servicios ofrecidos por *SaaS* no se ajustan correctamente a las necesidades del cliente o casos donde los costes asociados a la adquisición, instalación y gestión de estos mismos recursos son tan elevados que es el cliente prefiere pagar únicamente por el uso de los mismos y dejar esa responsabilidad al proveedor.

1.2.2.2. Plataforma como un servicio (PaaS)

Se encuentra en la capa intermedia del modelo de servicios de la **Figura 2**. Se trata de una plataforma de software donde se integran herramientas de desarrollo como por ejemplo, Eclipse, Php, Mysql o Visual .net, entre otras. Las aplicaciones desarrolladas por el cliente dependerán siempre de la plataforma en la que se haya contratado el servicio. Es decir, si el cliente trabaja sobre una

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

plataforma orientada a Windows, el *PaaS* probablemente ofrecerá **C#** o **Visual Basic** entre los lenguajes de programación disponibles. Las aplicaciones desarrolladas por el cliente serán de tipo Web y deberán ser orientadas para ofrecer algún tipo de servicio. Por ejemplo, un portal de venta online. Tanto el desarrollo, como las pruebas y la ejecución de la aplicación a desarrollar/desarrollada se ejecutarán dentro de la *cloud privada* ofertada al cliente. Puesto que las herramientas de desarrollo están hospedadas en la nube, se evita así que el cliente tenga que instalarlas en su equipo, ofreciendo más dependencia de Internet, pero menos uso de recursos propios. Además, es un servicio bastante amplio y diversificado puesto que ofrece una gran variedad de posibilidades en lo que respecta al área de desarrollo de proyectos: *ofrece diferentes herramientas para las distintas fases de desarrollo de un proyecto o herramientas para pruebas de software*. Resumiendo, la verdadera finalidad de este servicio es la de ejecutar una aplicación como servicio, ofreciéndole al cliente diferentes herramientas para desarrollarla, y cobrarle únicamente por el hospedaje en la mayoría de los casos.

Se trata de un servicio óptimo para desarrolladores Web o empresas que quieren ofrecer algún tipo de servicio vía Web mediante alguna aplicación online. Sin embargo existen las limitaciones propias de la plataforma en que se desea trabajar: sistema a utilizar, lenguajes de desarrollo, modelos de bases de datos. De esta forma, se debe tener muy en cuenta la plataforma en la que se quiera trabajar antes de escoger el servicio.

Ejemplos de empresas que ofrecen este servicio: *App Engine, Salesforce o Bungee Connect*.

1.2.2.3. Software como un servicio (SaaS)

Este tipo de servicio se encuentra en la capa más externa, **Figura 2**, de este modelo [19]. Se caracteriza por ser una aplicación remota ofrecida como un servicio por el proveedor a través de la red. Es el proveedor el que hospeda las aplicaciones en sus servidores y se encarga del mantenimiento de la misma. El cliente, por el contrario, se suscribe a este servicio y accede mediante un software instalado localmente o mediante el portal Web de dicho servicio. Es imprescindible el uso de Internet. De esta forma, el cliente se olvida de la administración y mantenimiento de este servicio, puesto que esa parte recae sobre el proveedor [20].

Realmente existen gran variedad de tipos de herramientas que ofrecen servicios bastante eficientes para: *redes, almacenamiento, sistemas operativos, bases de datos, servidores Web y servicios de restauración y de copia de seguridad*.

Este servicio está orientado para todo tipo de usuarios y empresas. Los demandantes de estos servicios deben comprobar si este software como servicio se ajusta a sus necesidades y a la calidad deseada.

Como desventaja, y como se aprecia en la **Figura 1**, se trata del servicio donde el cliente se tiene que encargar de la instalación, configuración y mantenimiento de la maquina virtual y de sus componentes físicos tales como bases de datos o servidores.

1.2.3. Ventajas y desventajas del Cloud Computing

A continuación se describen las ventajas y desventajas del Cloud Computing [7].

Ventajas

- **Integración:** probada de servicios Web. Por su naturaleza, la tecnología de *Cloud Computing* se puede integrar con facilidad y rapidez con las aplicaciones empresariales que usan los clientes.
- **Prestación de servicios a nivel mundial:** las infraestructuras de *Cloud Computing* proporcionan mayor capacidad de adaptación, recuperación de desastres y reducción al mínimo de los tiempos de inactividad.
- **Muchos tipos de servicio sólo necesitan que el cliente disponga únicamente de un navegador para conectarse a internet:** una infraestructura 100% *Cloud Computing* puede ofrecer una tecnología muy simple y eficaz.
- **Implementación más rápida y con menores riesgos para el cliente:** cualquier cliente podrá comenzar a trabajar en pocos días mediante el uso de los servicios ofrecidos por *Cloud Computing* (ver apartado 1.2.2.). Si un cliente contrata un determinado software como servicio (*SaaS*) evitará los riesgos de tener que hacer fuertes inversiones cuando una aplicación integrada quede obsoleta y haya que desarrollar una nueva solución, debido a que se le garantiza el mantenimiento y la actualización constante del software contratado.
- **Actualizaciones automáticas que no afectan negativamente a los recursos de TI:** si actualizamos la última versión de la aplicación, nos veremos obligados a dedicar tiempo y recursos para volver a crear nuestras personalizaciones e integraciones. La tecnología de *Cloud Computing* no obliga a decidir entre actualizar y conservar un trabajo, porque esas personalizaciones e integraciones se conservan automáticamente durante la actualización.

Desventajas

- **Privacidad de los datos:** el tráfico de los datos estará continuamente en manos de otros, en manos de las empresas que ofrecen el servicio. Estas deben ser una empresa de total confianza y con una gran solvencia pública.
- **Dependencia de los servicios en línea.**
- **Posibles fallos en la seguridad y privacidad de la información.**
- **Caídas del servicio:** Catástrofes naturales o errores humanos que dejen dicho servicio offline, con las malas repercusiones para los clientes.
- **Descontrol del manejo, almacenamiento y uso de esta información.**
- **Dependencia de la tecnología:** existirán tecnologías que no soporten el servicio y esto conlleve a que distintos tipos de dispositivos no puedan hacer uso de él.
- **Mayor dependencia de los proveedores de Internet y de la velocidad de ADSL, cable, fibra óptica u otras tecnologías.**
- **Ataques cibernéticos:** para romper la seguridad del servicio y robar los datos privados.

1.3. Herramientas actuales para almacenamiento virtual

Debido a la gran diversidad de herramientas de almacenamiento virtual existentes y puesto que todas tienen, en gran medida, ciertas similitudes en lo que a características, funcionalidades y servicios se refiere, se han escogido para estudio aquellas que difieren más entre sí en cuanto a servicios y que se han creído más interesantes para establecer los verdaderos problemas que han llevado a sus usuarios al uso de herramientas complementarias de cifrado.

1.3.1. Dropbox, Ubuntu One y SpiderOAK

Las herramientas seleccionadas para estudio son sumamente conocidas: *Dropbox*, *Ubuntu One* y *SpiderOAK*. En los siguientes apartados se describen sus características y principales servicios ofertados.

1.3.2. Servicios ofertados

En este apartado se describen de forma esquematizada los principales servicios ofertados y sus características para las diferentes herramientas a estudiar. La descripción de estos servicios y sus características tiene como objetivo intentar ofrecer una visión precisa de cada una de ellas y mostrar claramente sus puntos fuertes y débiles en cuanto a servicios y seguridad se refiere.

CARACTERÍSTICAS	DROPBOX	UBUNTU ONE	SPIDEROAK
HOSTING			
Espacio gratuito (GB)	2GB	5GB	2GB
SINCRONIZACIÓN (0)			
Directorio centralizado (1)	NO	NO	NO
Tipo de sincronización	AUTOMÁTICA	AUTOMÁTICA	AUTOMÁTICA
Control de versiones	SI	NO	SI
Sincronización selectiva	SI	SI	SI
Conflictos entre archivos	SI	SI	NO
SEGURIDAD (2)			
Archivos cifrados localmente	NO	NO	NO
Canal seguro	SI (SSL)	SI (SSL)	SI (SSL)
Archivos cifrados en el servidor	SI	NO	SI
Método de encriptación	AES 256	NINGUNO	RSA 2048 - AES 256
Validación de usuario mediante contraseña	NO	NO	SI
SERVICIO SHARING (3)			
Compartir archivos	SI	SI	SI
Técnica utilizada (4)	Link públicos	Link públicos	Link públicos
Compartir directorios	SI	SI	SI
Back-up local	NO	NO	SI
OTRAS CARACTERÍSTICAS			
Multiplataforma	SI	SI	SI
Acceso Web	SI	SI	SI

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Facilidad de uso	SI	SI	NO
Velocidad de sincronización (5)	RÁPIDA	LENTA	LENTA

Tabla 1. Características principales de las herramientas estudiadas.

(1) Indica si cabe la posibilidad de sincronizar diferentes directorios desde ubicaciones diferentes.

(2) Ver apartado 1.3.1.2.

(3) Ver apartado 1.3.1.3.

(4) Técnica utilizada para compartir archivos públicamente.

(5) Esta información es obtenida del uso personal de cada una de las herramientas.

1.3.2.1. Sincronización de archivos

Las principales características del servicio de sincronización de las diferentes herramientas estudiadas vienen descritas en la siguiente Tabla y van a ser brevemente explicadas para ofrecer una visión más precisa de cada una de ellas.

SINCRONIZACIÓN	DROPBOX	UBUNTU ONE	SPIDEROAK
Directorio centralizado	NO	NO	NO
Tipo de sincronización	AUTOMÁTICA	AUTOMÁTICA	AUTOMÁTICA
Sincronización selectiva	SI	SI	SI
Control de versiones	SI	NO	SI
Conflictos entre archivos	SI	SI	NO

Tabla 2: Servicios de sincronización en herramientas de almacenamiento virtual.

Dropbox

- Utiliza un método de sincronización que compara el archivo a sincronizar con la copia que hay almacenada en el servidor y envía únicamente las partes modificadas.
- Ofrece la sincronización de un único directorio. Para sincronizar directorios que se encuentren en ubicaciones externas la comunidad de usuarios ha desarrollado varias herramientas para plataformas Windows o MAC basándose en las técnicas de *enlaces entre archivos*. MacDropAny [25] y DropboxFolderSync [26] son dos aplicaciones asociadas a Dropbox que permiten enlazar diferentes carpetas en plataformas MAC y Windows, respectivamente. Para Linux no existe actualmente ninguna herramienta similar, pero se puede obtener el mismo resultado mediante el uso del comando *ln* desde la terminal. Esta técnica también se puede utilizar para Mac y Windows si no se desea hacer uso de las herramientas mencionadas anteriormente [22].

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- La sincronización de archivos es *automática*. Tras cada edición de un archivo o directorio, estos se sincronizarán automáticamente con el servidor siempre que así lo haya indicado el usuario.
- Permite *sincronización selectiva* mediante la opción:

Menú → Preferencias → Avanzado → Sincronización Selectiva.

Con esta opción el usuario puede elegir los directorios que desea sincronizar de manera automática con el servidor [16].

- Mantiene un histórico con copias de todas las ediciones de archivos y directorios durante 30 días en la versión gratuita. Gracias a esto el usuario puede recuperar copias de archivos o directorios anteriormente editados o eliminados antes de 30 días hasta la fecha.
- Aunque no se trate de una herramienta colaborativa, si dos usuarios están editando un mismo archivo a la vez y lo guardan al mismo tiempo, se genera un archivo de conflicto como el que se ve en la siguiente Figura.

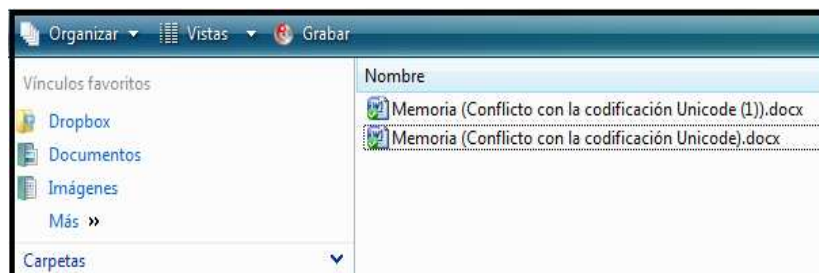


Figura 3: Conflictos por edición simultánea de archivos.

Ubuntu One

- Para sincronización de archivos y directorios existe un agente de sincronización (***u1sync-agent***) que se encarga de la sincronización y de la gestión de los cambios en los archivos. Además, los archivos que son modificados en el cliente son subidos íntegramente de nuevo. La técnica es descrita con más detalle en la sección de detalles técnicos de *Ubuntu One* [21].
- En Linux existe también la opción de *sincronizar directorios no centralizados*, es decir, que se encuentran fuera del directorio asociado a *Ubuntu One* [9]. En el caso de la versión beta de Windows se puede realizar mediante *la consola de Windows creando links simbólicos* [37].
- Sobre Linux la *sincronización de archivos* es automática, pero en la versión beta de *Ubuntu One* para Windows no lo es. Esta última tiene integrado un temporizador donde el usuario tiene que establecer el tiempo que debe transcurrir para que la información se sincronice.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

También, la sincronización se puede hacer de manera manual mediante la opción de *sincronizar ahora* [37].

- En cuanto a *sincronización selectiva*, solo está disponible para la versión de Ubuntu 11.04 Natty Narwhal [18]. Para la versión beta de Windows o para la aplicación Web no está disponible.
- *Ubuntu One* no utiliza ningún método de control de versiones, aunque está en proyecto [10].
- Al igual que en *Dropbox*, existen conflictos cuando se editan y se guardan dos archivos simultáneamente. El archivo que genera el conflicto toma el formato *.u1conflict[.NN]* [8]. Con la edición de este archivo se puede recuperar la copia conflictiva.

SpiderOAK

- Esta herramienta comprime la información en tránsito para acelerar el proceso de sincronización. Además, busca mediante métodos de redundancia la información que ha variado para así no tener que subir las partes del archivo que no han sido editadas.
- Por diseño no existe un directorio centralizado para esta herramienta. Por el contrario, permite la sincronización en todo el sistema de archivos de forma nativa [38].
- La sincronización es automática, aunque también puede ser establecida la frecuencia de sincronización por el usuario [40].
- Se puede realizar sincronización selectiva, pero de una forma diferente y no tan sencilla a la de las herramientas anteriores. Para ello hay que otorgarle un nombre a la sincronización, establecer una carpeta origen y seleccionar una o varias carpetas que se desean sincronizar [39].
- Utiliza un método de control de versiones. De esta manera ofrece la posibilidad, al igual que *Dropbox*, de poder recuperar antiguas ediciones de archivos o carpetas [4].
- Al contrario de las otras dos herramientas, la tolerancia a fallos de esta herramienta ante cualquier tipo de problema relacionado con la información es máxima.
- La sincronización en SpiderOAK es unidireccional, y cada equipo asociado a una cuenta posee un espacio de almacenamiento diferente en el servidor, lo que implicaría que la información fuera redundante. Sin embargo, un sistema anti duplicado que evita este tipo de problemas [12].
- No se tiene constancia de resolución de conflictos entre archivos.

1.3.2.2. Seguridad

Las principales características en cuanto a técnicas de seguridad de las diferentes herramientas estudiadas vienen descritas en la siguiente Tabla.

SEGURIDAD	DROPBOX	UBUNTU ONE	SPIDEROAK
1. Archivos cifrados localmente	NO	NO	NO
2. Canal seguro	SI (SSL)	SI (SSL)	SI (SSL)
3. Archivos en cifrados en el servidor	SI	NO	SI
4. Método de encriptación	AES 256	NINGUNO	RSA 2048 - AES 256
5. Validación de usuario mediante contraseña	NO	NO	SI

Tabla 3: *Técnicas y métodos de seguridad en las herramientas de almacenamiento virtual.*

A continuación, se van a describir brevemente estas características para tener un conocimiento más preciso de dichas técnicas.

Dropbox

- No mantiene sus archivos cifrados localmente. Lo que sí proporciona es el envío seguro de información mediante un protocolo de certificación *SSL*, un canal seguro y el envío de los datos de manera cifrada al servidor utilizando el algoritmo de clave simétrica *AES -256*.
- La información se mantiene cifrada con *AES -256* en el servidor.
- No utiliza ningún método de validación de contraseña al inicio de sesión. Cuando una cuenta de usuario es asociada a un equipo, se genera un identificador (*ID Cliente*) que identifica a la pareja máquina y usuario de manera única. A pesar de no pedir la contraseña al usuario al inicio de sesión, utiliza métodos de autenticación de usuario antes del envío de la información [28].

Ubuntu One

- No utiliza ninguna técnica para mantener los datos cifrados ni en el equipo del usuario ni en el servidor. Su seguridad se basa en utilizar un protocolo de comunicación cifrada (*SSL*) basado en certificados y un método de autenticación *Oauth* [30] que viene descrito en el apartado de seguridad de *Ubuntu One* [29].
- En cuanto a validación de contraseña al inicio de sesión, *Ubuntu One* no le pide al usuario introducirla al inicio de la misma. A diferencia de *Dropbox*, no se conoce qué información es la que se envía para autenticar al cliente con el servidor.

SpiderOAK

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Basa su seguridad en un sistema que llama “zero-knowledge” [31]. Este sistema se basa en que la clave es gestionada localmente por el usuario y solo es conocida por él y no por el servidor.
- El proceso de envío de datos utiliza un canal seguro, un protocolo de certificación SSL y el cifrado de los mismos mediante una combinación de métodos de cifrado RSA - 2048 y AES - 256 [32].
- Los datos se almacenarán cifrados en el servidor y nadie, salvo el cliente, podrá descifrarlos.
- Para iniciar la sesión de *SpiderOAK*, se puede establecer en las preferencias del software que el usuario tenga que validarse al inicio de la misma para poder tener acceso a la aplicación.

1.3.2.3. Servicio sharing

Las principales características en cuanto al servicio de sharing (compartir archivos y carpetas) de las diferentes herramientas estudiadas vienen descritas en la siguiente Tabla.

SERVICIO SHARING	DROPBOX	UBUNTU ONE	SPIDEROAK
1.Compartir archivos	SI	SI	SI
2.Técnica utilizada	Links públicos	Links públicos	Links públicos
3.Compartir directorios	SI	SI	SI
4.Back-up local	NO	NO	SI

Tabla 4: Servicios sharing en herramientas de almacenamiento virtual.

Dropbox

- Permite compartir archivos y carpetas. Los archivos sólo se pueden compartir si se encuentran dentro de la carpeta *Public* y los directorios sólo si se encuentran dentro de la carpeta *Photos*.
- La técnica utilizada para compartir archivos es mediante *links públicos*. Con esta técnica se permite a los usuarios de las herramientas de almacenamiento virtual compartir archivos públicamente mediante una URL: todos los usuarios que la conozcan podrán tener acceso al archivo desde un navegador. Un ejemplo de un link público es el siguiente: <http://dl.dropbox.com/u/6747916/How%20to%20use%20the%20Public%20folder.rtf>
- Las carpetas se pueden compartir únicamente desde el servicio web. La invitación se realiza mediante la cuenta de correo electrónico de la persona con la que se quiere compartir la carpeta. Una vez que el destinatario acepta la invitación, éste obtiene una copia sincronizada en su directorio local de *Dropbox*.

Ubuntu One

- Las funcionalidades sobre servicios sharing son muy similares a las de *Dropbox*. La única diferencia que existe es que en la versión Beta de *Ubuntu One* no se permite compartir archivos ni carpetas. La técnica para compartir archivos es la misma que la utilizada por *Dropbox* (*links públicos*). A continuación se muestra un ejemplo: <http://ubuntuone.com/1cmwpgM4AJwCkGIHDCRbbY>
- Con respecto a la opción de back up local, tampoco está contemplada.

SpiderOAK

- Permite compartir tanto archivos como carpetas, al igual que las herramientas anteriores.
- *SpiderOAK* sí ofrece la posibilidad al usuario de tener una copia cifrada de sus archivos en un directorio local o remoto elegido por él mismo. La información almacenada en el directorio back up es ilegible y la estructura de éste también [34].

1.4. Herramientas complementarias de seguridad

Como se aprecia en el **apartado 1.3.2.2**, la información almacenada en el directorio local no tiene ningún tratamiento especial por parte de la mayoría de las herramientas estudiadas. Con lo de tratamiento especial, nos referimos a que dichas herramientas no cifran la información en el directorio local del usuario. Además, en el caso *Ubuntu One*, la información tampoco es almacenada de forma cifrada en sus servidores.

Este aspecto ha ido poco a poco tomando importancia debido a diferentes motivos de seguridad como los descritos en el **apartado 2** y han llevado a los usuarios que utilizan los servicios estudiados a utilizar otras herramientas de seguridad complementarias para aplicar más seguridad a su información. Algunas de estas herramientas son recomendadas por los propios desarrolladores del software de almacenamiento virtual, como es el caso de *TrueCrypt* por parte *Dropbox* [35] o el script *Ubuntu One Encrypt/Decrypt* [36] por parte de *Ubuntu One*. También existen otras herramientas como *SecretSync* que no lo están.

En este apartado se van a describir y explicar las principales características de los tres servicios nombrados anteriormente y que son utilizados comúnmente junto a las herramientas de almacenamiento virtual estudiadas en el **apartado 1.3**.

En la **Tabla 5** se pueden ver las características más importantes de dichas herramientas:

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Software/ Características	SecretSync	TrueCrypt	Ubuntu One Encrypt/Decrypt
Dedicado a un determinado software de almacenamiento Virtual	SI (<i>Dropbox</i> – <i>Ubuntu One</i>)	NO	SI
Técnica de trabajo	Directorio – <i>Tunneling</i>	Unidad o Volumen cifrado	Cifrado individual de archivos
Tipo de cifrado	AES 256	Varios tipos (1)	Triple DES
Multiclave	SI	SI	SI
Gestión de cifrado para grupos (2)	NO	NO	NO
Interoperabilidad con el Software de almacenamiento virtual (3)	NO	NO	SI

Tabla 5. Descripción de características de las herramientas de encriptación.

(1) Utiliza los siguientes métodos de cifrado: **AES, Serpents, TwoFish** y la combinación de estos.

(2) Es una utilidad o funcionalidad añadida en el proyecto que permite a los distintos usuarios que forman parte de una carpeta compartida poder cifrar la información de tal manera que algunos miembros puedan tener acceso a la información y otros no (**ver apartado 3.4**).

(3) El software está fuertemente acoplado a la herramienta de almacenamiento virtual.

A continuación, se explicarán brevemente el funcionamiento y las características principales de las herramientas de encriptación descritas en la **Tabla 5**.

1.4.1. SecretSync

- Es una herramienta de encriptación diseñada en principio para *Dropbox*, pero que puede utilizarse por otras herramientas de almacenamiento virtual, como por ejemplo *Ubuntu One*.
- Utiliza un método de cifrado de clave simétrica **AES 256**, utilizando para el cifrado de la información la clave con la que se ha registrado el usuario al instalar la aplicación.
- Utiliza *tunnelling*, la técnica de encapsulación de protocolos, para el envío de la información al directorio remoto de forma segura. Para ello se emplea un directorio llamado SecretSync que se encuentra en el directorio de instalación de dicha herramienta y donde, todo lo introducido en él, será cifrado y sincronizado desde esta carpeta a otra con el nombre *SecretSync_tunnel_Root* que se encuentra dentro de la herramienta de almacenamiento virtual con la que se trabaja.
- No es multiclave, es decir, no puede haber varios usuarios en el mismo equipo que utilicen la aplicación con diferentes claves.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- No puede realizar sincronización selectiva. Todo lo que se edite y se introduzca dentro de la carpeta *SecretSync* se cifrará y sincronizará directamente.
- No permite la interoperabilidad con el software de almacenamiento virtual, puesto que se trata de un software bastante sencillo que trabaja de forma independiente de las herramientas de almacenamiento virtual.

1.4.2. TrueCrypt

- Es una herramienta de encriptación cuyo uso para el cifrado de información en herramientas de almacenamiento virtual como *Dropbox* es bien conocido [35].
- Utiliza una técnica de montaje de volúmenes para mantener la información cifrada. El usuario introducirá su password y seleccionará con qué tipo de cifrado (*AES*, *TwoFish*, *Serpents* o combinación de ellos) y con qué algoritmos de resumen (*RIPMD-160*, *SHA-512*, *WhirPool*) deseará cifrar la información.
- Puesto que se pueden montar varios volúmenes con diferentes claves se podría cifrar la información con distintas claves en función del volumen sobre el que se trabaje.
- No contempla el trabajo para grupos, la sincronización selectiva ni la interoperabilidad con el software de almacenamiento virtual puesto que el propósito de este software no es el de trabajar con este tipo de herramientas.

1.4.3. Ubuntu One Encrypt/Decrypt

- Es un script desarrollado únicamente para Linux que permite cifrar la información almacenada en *Ubuntu One*.
- La técnica de cifrado y descifrado es mediante la selección del archivo que se desea cifrar utilizando un cuadro de selección de archivos integrado en la herramienta. El método de cifrado utilizado por esta herramienta es *Triple DES*.
- Se puede utilizar una clave distinta para cada archivo.
- Las opciones de sincronización selectiva y el trabajo en grupo no están contempladas puesto que sus finalidades no son esas.
- Existe integración con *Ubuntu One* en cierta medida, puesto que es un script desarrollado para dicho servicio.

P.F.C: *Herramienta de encriptación adicional para almacenamientos virtuales.*

2. Descripción de los objetivos

Debido a la gran polémica acontecida con la modificación de las cláusulas de privacidad en *Dropbox* (ver apartado 2.1) y los muchos problemas de seguridad que mensualmente se ven reflejados en foros y portales Webs especializados acerca de esta herramienta, el desarrollo del proyecto se ha centrado en ofrecer un servicio más seguro para los clientes de *Dropbox* mediante el desarrollo de una herramienta complementaria de seguridad basada en el cifrado de la información, KonEncriptación. Además, puesto que *Dropbox* ofrece un servicio sharing que permite compartir carpetas, se ha querido ofrecer también la posibilidad de compartir los archivos cifrados y determinar qué usuarios van a tener acceso a determinada información compartida.

2.1. Problemas legales de Dropbox

En la primera mitad de 2011 los usuarios de *Dropbox* recibieron un correo electrónico donde se les informaba de los nuevos cambios en: *los términos de privacidad del servicio, la política de privacidad y las descripciones de seguridad*. A pesar del descontento de una gran parte de los usuarios estos cambios se hicieron válidos el pasado 15 de Julio de 2011.

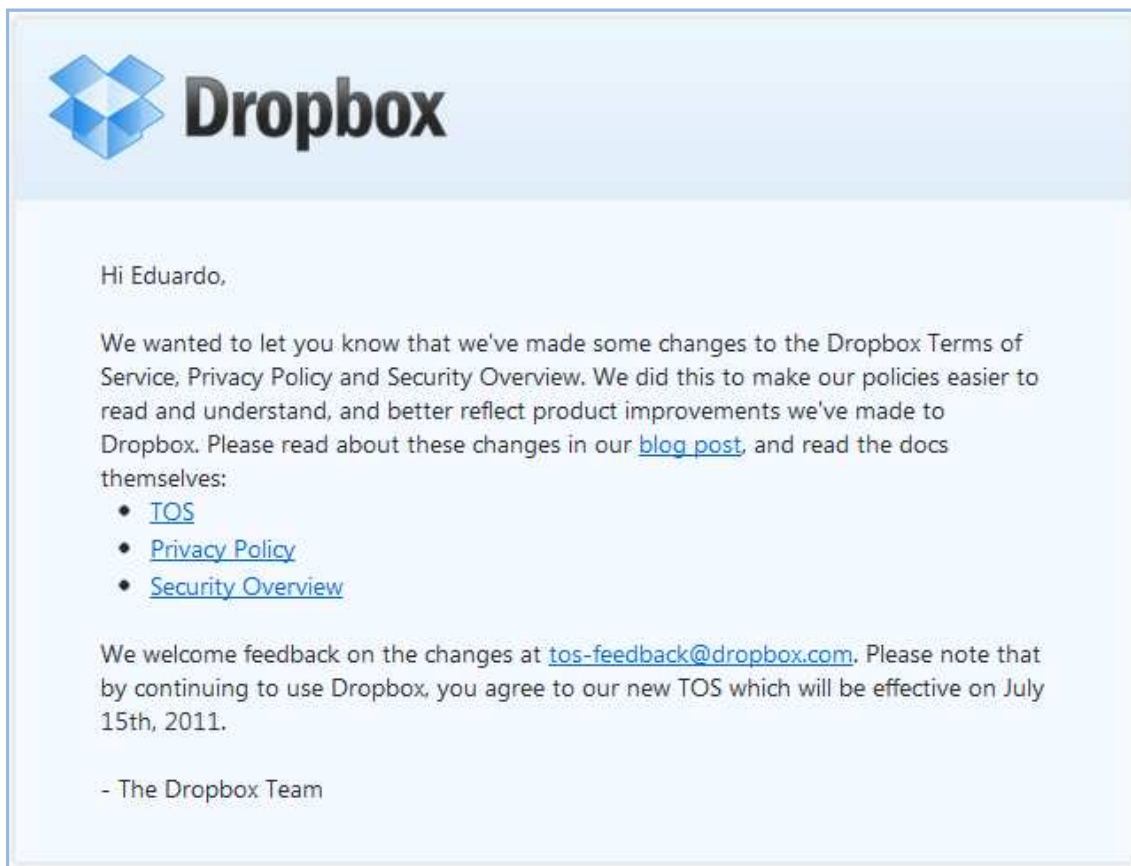


Figura 4: *Nuevos términos de seguridad.*

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Si accedemos a www.dropbox.com/privacy#terms podremos ver los términos de privacidad de Dropbox y las cláusulas que han suscitado tanta polémica. Estos se describen a continuación:

Privacy

A copy of our full privacy policy can be found at: <https://www.dropbox.com/privacy>. We guard your privacy to the best of our ability and work hard to protect your information from unauthorized access.

Dropbox employees are prohibited from viewing the content of files you store in your Dropbox account, and are only permitted to view file metadata (file names and locations). Like most online services, **we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so)**. But that's the rare exception, not the rule. **We have strict policy and technical access controls that prohibit employee access except in these rare circumstances**. In addition, we employ a number of physical and electronic security measures to protect user information from unauthorized access.

Compliance with Laws and Law Enforcement

As set forth in our privacy policy, and in compliance with United States law, Dropbox cooperates with United States law enforcement when **it receives valid legal process, which may require Dropbox to provide the contents of your private Dropbox. In these cases, Dropbox will remove Dropbox's encryption from the files before providing them to law enforcement**.

I think I've found a security exploit. Where do I report security concerns?

We take a number of measures to ensure that the data you store on Dropbox is safe and secure. While we're very confident in our technology, **we recognize that no system can guarantee data security with 100% certainty**. For that reason, we will continue to innovate to make sure that our security measures are state of the art, and we will investigate any and all reported security issues concerning Dropbox's services or software. For a direct line to our security experts, report security issues to security@dropbox.com.

De manera resumida, estas cláusulas indican:

- La información de registro de un usuario en la aplicación (datos personales al darse de alta en *Dropbox*), los datos del equipo del usuario y la información hospedada en los servidores de *Dropbox*, van a poder ser enviadas a las autoridades pertinentes de Estados Unidos si ellos lo requieren por colaboración con ellos.
- Sólo existen unos pocos empleados que tienen acceso a la información del usuario, y el resto, rara vez y por circunstancias excepcionales, podrán tener acceso también a ella.
- No pueden garantizar la seguridad al 100 % de la información del usuario con su servicio.

How to Add Your Own Layer of Encryption to Dropbox

Dropbox applies encryption to your files after they have been uploaded, and we manage the encryption keys. Users who wish to manage their own encryption keys can apply encryption before placing files in their Dropbox. **Please note that if you encrypt files before uploading them, some features will not be available, such as creating public links. Doing so will also make it impossible for us to recover your data if you lose your encryption key.**

Además, como se aprecia en la clausula “*How to Add your own layer of encryption to Dropbox*”, insta a los usuarios de *Dropbox* a que la información que alojan en sus servidores no esté previamente cifrada con una herramienta de encriptación alternativa para facilitarles el acceso a ella. Para ello alegan un mal funcionamiento de las funcionalidades ofrecidas por el servicio.

2.2. Problemas actuales de seguridad de Dropbox

Dropbox está sometido actualmente a diferentes tipos de problemas de seguridad como por ejemplo: *el robo del archivo de configuración o los ataques a los servidores de las herramientas de almacenamiento*. Por esta razón, es importante describir dichos problemas para que usuarios de este servicio o de servicios similares tengan conocimiento de ellos.

2.2.1. Problemas de suplantación de identidad

Como ocurre, por ejemplo, en el caso descrito en el **apartado 2.2.2**, cuando estamos trabajando con carpetas compartidas, podría existir la situación en que *otra persona suplante la identidad de un usuario* y tengan así acceso a la información de esta tercera persona. En este caso, el uso de login y password no garantiza que la información almacenada en los servidores este a salvo de terceras personas que no son quien dicen ser.

2.2.1.1. Robo del archivo de configuración de Dropbox

Un experto en seguridad, *Derek Newton*, reveló que los hackers pueden descargar fácilmente todos los archivos de la cuenta de *Dropbox* de un usuario si roban el archivo de configuración (*config.db*) de *Dropbox* de alguno de los equipos donde esté asociada la cuenta de dicho usuario [17].

Si un atacante puede obtener dicho archivo a través de malware, acceso físico o puerta trasera, entonces puede utilizarlo para hacerse pasar por el usuario legítimo y poder así descargar todos los archivos de la cuenta de la víctima.

En la **Figura 5**, se puede ver la estructura de la base de datos *config.db* donde se guardan los datos de configuración de *Dropbox* y el campo *Host_ID* con el que se identifica de manera única a cada equipo con el que tiene un usuario asociada su cuenta de *Dropbox*.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

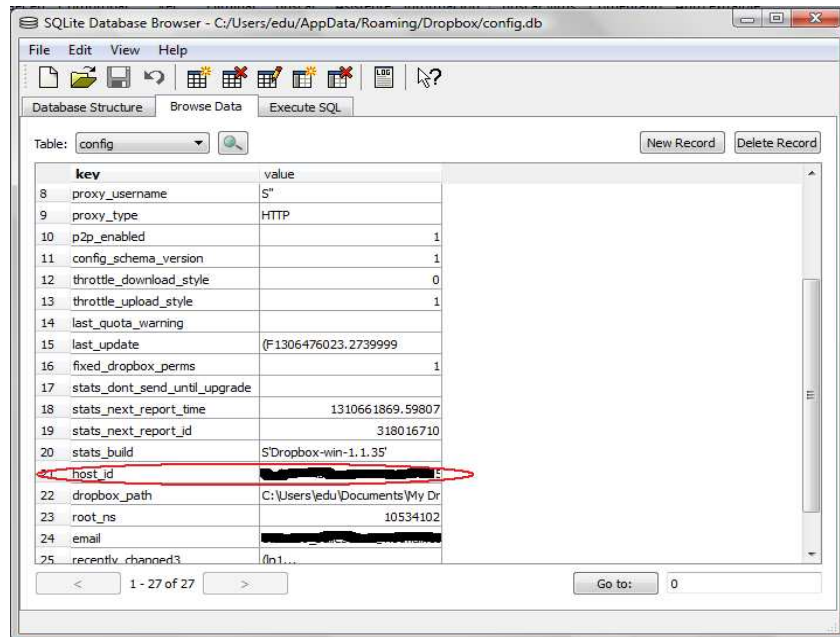


Figura 5: Vista de la estructura del archivo de configuración de Dropbox.

Ante este caso, *Dropbox* no se responsabiliza de la pérdida de información por este tipo de ataque, pues señala al usuario del equipo como culpable de ello, aunque trabaja en medidas para solucionarlas como se describe en el siguiente comunicado realizado por ellos: "estableceremos permisos más restrictivos en la carpeta que almacena el archivo de autenticación, y pronto le proporcionaremos una solución que hará que el archivo de autenticación sea inútil en un segundo equipo".

2.2.2. Confianza Transitiva

Dropbox, entre otras funcionalidades, ofrece la opción de compartir carpetas con otros usuarios mediante invitación previa.



Figura 6: Forma de compartir una carpeta mediante servicio Web.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

El sistema de invitación para pasar a formar parte de una carpeta compartida en *Dropbox* es *abierto*. Es decir, una vez que el creador de la carpeta compartida (*propietario*) haya invitado a otro usuario, y éste haya aceptado la invitación, el nuevo invitado podrá seguir invitando a otros usuarios para que formen parte de dicha carpeta compartida.

De esta manera, existen casos donde terceras personas, que son desconocidas entre sí y con las que solo existe un *nexo de confianza transitiva* (*los amigos de mis amigos son mis amigos*), comparten información sin conocerse siquiera. Para muchos usuarios, posiblemente este nexo de confianza no sea suficiente y rehúsen a tener cierta información expuesta con usuarios que no son de su confianza y con los que no quieren hacerlo.

Además, el sistema de gestión de usuarios para carpetas compartidas sólo ofrece la posibilidad al propietario de la carpeta de poder eliminar a miembros del grupo, mientras que a un usuario invitado no se la ofrecen.

En la **Figura 7** se aprecia la existencia de dos roles distintos cuando trabajamos con carpetas compartidas:

- Propietario(**Eduardo Ballesta Caparrós**)
- Usuario normal (**Pedro Ayala**).

En casos como éste, sólo **Eduardo** tiene privilegios para expulsar a todos los miembros con los que comparte esa carpeta mediante la opción de **No compartir esta carpeta** o expulsar selectivamente a cualquier miembro mediante la opción **Sacar**.

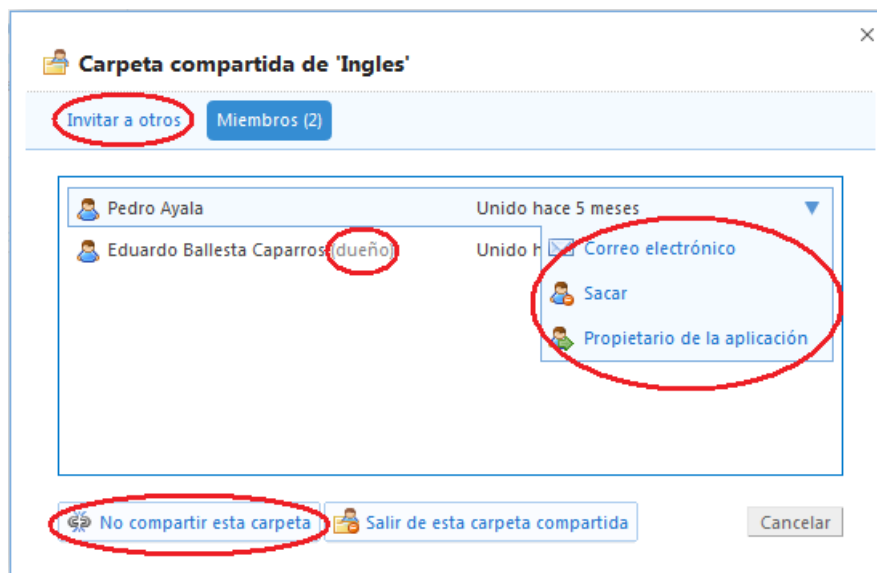


Figura 7: Gestión de usuarios de una carpeta compartida mediante servicio Web.

Cabe destacar que una vez que un miembro es desligado de una carpeta compartida o la propia carpeta deja de ser compartida, la información que había en dicha carpeta en el momento de ser desligado como miembro o al desligar la carpeta como compartida, se copia localmente en la máquina de cada usuario. De esta manera, un usuario poseería información de otros usuarios sin la posible aprobación de estos terceros.

2.2.3. Ausencia de cifrado

Como se puede ver en la **Tabla 1** del **apartado 1.3**, donde se describen las características principales de las herramientas de almacenamiento virtual estudiadas en este proyecto, ninguna de ellas integra técnica alguna para el cifrado de la información almacenada localmente. Además, no tener cifrada la información localmente con otro método alternativo al que usa la herramienta de almacenamiento virtual, no es suficiente para garantizar problemas como los de los **apartados 2.2.1** y **2.2.2**. Para la mayoría de los problemas descritos en este apartado no tener la información cifrada localmente es igual a una vulnerabilidad real de seguridad a la que expone la información del usuario.

2.2.3.1. Vulnerabilidad en el servicio Web de Dropbox

A finales del mes de Junio de 2011, se pudo acceder durante 4 horas mediante el servicio Web a cualquier cuenta de usuario ingresando una contraseña errónea [13]. Según describen las funcionalidades de *Dropbox*, el cifrado y descifrado de los archivos se realiza en los servidores de la empresa y no en las computadoras de cada usuario. De esta manera, el usuario sobreentiende que sus archivos se encuentran almacenados de forma cifrada y segura en los servidores de estos.

Como se ha demostrado con éste tipo de ataque, puede que no exista ninguna relación entre la autenticación del usuario para acceder al servicio Web de *Dropbox* y la información que se presenta descifrada al acceder al servicio una vez identificado el usuario.

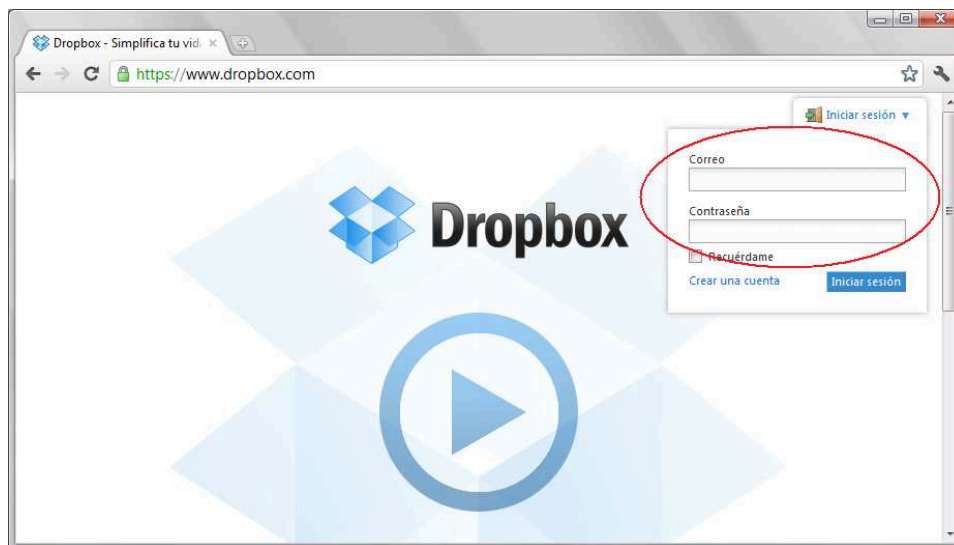


Figura 8: Acceso al servicio Web de Dropbox.

2.2.3.2. Ataques a los servidores de las herramientas de almacenamiento virtual

La universidad de California realizó un estudio [1], junto a otras universidades colaboradoras, donde se demostró que se podía acceder a la información de los usuarios utilizando herramientas de monitorización capaces de determinar la parte de la memoria compartida que usaba la *máquina virtual* de los servidores *EC2* para ejecutar las aplicaciones.

Esto supone que la información almacenada en los servidores de proveedores *SaaS* no es totalmente inaccesible y es vulnerable a posibles ataques con el fin del robo de la información.

2.2.4. Falta de funcionalidad de las herramientas complementarias de seguridad

Si observamos la **Tabla 5** donde se describen las principales características de las herramientas de encriptación utilizadas por los software de almacenamiento virtual del **apartado 1.4**, se aprecia que funcionalidades como: *la orientación de estas herramientas para la gestión de trabajo en grupo en carpetas compartidas, la sincronización selectiva o la interoperabilidad con el software de almacenamiento virtual*, no están contempladas en ninguna de ellas. Esto nos hace ver que dichas herramientas solo tienen el único fin de cifrar y no complementan, con más funcionalidades, ciertos aspectos que durante el desarrollo de *KonEncriptación* han sido relevantes y se han tenido muy en cuenta.

2.3. Solución de Problemas

A continuación se describirán las distintas soluciones desarrolladas para los problemas descritos en el apartado anterior (**ver apartado 2.2**).

2.3.1. Establecer contraseña de *KonEncriptación* diferente a la de *Dropbox*

Como es bien sabido, *Dropbox* solo utiliza la contraseña para validar al usuario en su servicio Web o cuando un usuario asocia el equipo donde trabaja con su cuenta de usuario (**correo electrónico**) en *Dropbox*.

Puesto que se intenta evitar el problema derivado del acceso a la información por parte del personal de *Dropbox* (**ver apartado 2.1**) o los problemas descritos en el **apartado 2.2**, es conveniente utilizar *una clave de acceso para KonEncriptación diferente* a la utilizada en la herramienta de almacenamiento virtual para, de esta manera, dificultar aún más el acceso a la información a personas no autorizadas a hacerlo.

Así, si un *usuario A* se adueñara de la cuenta de *Dropbox* de otro *usuario B*, temporal o definitivamente, y tuviera acceso continuo a la información de éste, y de otros usuarios en los casos de carpetas compartidas, necesitaría conocer la clave de acceso de *KonEncriptación* para poder así

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

descifrar la información cifrada. De esta manera, se evitaría además el problema de suplantación de identidad descrito en el [apartado 2.2.1](#).

2.3.2. Sistema de cifrado local

En primer lugar, cuando se trabaja con una carpeta compartida en *Dropbox*, los archivos y subdirectorios allí guardados son visibles por el resto de usuarios que son miembros de esa carpeta.

Si simplemente cada usuario se encargara de cifrar la información dentro de una carpeta compartida, el resto de usuarios no podrían tener nunca acceso a dicha información a no ser que el usuario tomara alguna medida externa como enviar las claves por correo electrónico o teléfono a los usuarios.

Cómo se describió en la [Tabla 5](#) del [apartado 1.4](#), ninguna de las herramientas de encriptación estudiadas está diseñada para la gestión de trabajo en grupo. Con lo de trabajo en grupo, nos referimos al servicio sharing que permite la compartición de carpetas. Por esta razón, cuando se cifra un archivo con alguna de estas herramientas estudiadas no se ofrece ninguna estrategia para que el resto de usuarios miembros de una carpeta compartida puedan descifrar dicho archivo.

En KonEncriptación, en cambio, sí se ha desarrollado una estrategia de cifrado donde se permite el trabajo en grupo. Para ello se almacena una cabecera en los archivos cifrados ([ver apartado 3.2.1](#)) guardando información que indica qué usuarios pueden editar los archivos cifrados y qué usuarios adicionales lo han solicitado. De esta forma, se evita el problema descrito en el [apartado 2.2.2](#).

Por otra parte, *al cifrar la información con un sistema de cifrado basado en contraseña se evita también el problema descrito en el [apartado 2.1](#) sobre el acceso a la información por parte del personal de Dropbox*. Al cifrar la información con KonEncriptación estamos haciendo ilegible e inservible la información para personas no autorizadas que puedan tener acceso a ella en algún momento. Con el cifrado de la información no se resuelve únicamente este problema, sino también todos los descritos en el [apartado 2.2.1](#).

Además, se le ofrece al usuario una forma más segura y aislada de trabajar con la información en claro (*sin cifrar*). KonEncriptación posee un directorio local que funciona como back up del directorio remoto. El diseño de KonEncriptación ha centrado su esfuerzo en que el usuario aprenda a trabajar en dicho directorio local donde el usuario puede tener su información en claro sin que ningún usuario ligado con *Dropbox*, ya sea empleado, hacker o amigo, pueda tener conocimiento directo del contenido de la información que un usuario maneja. Si el usuario aprendiera ese hábito, se evitarían los problemas de los [apartados 2.1](#), [2.2.1](#) y [2.2.3](#).

A pesar de ello, en el diseño de la herramienta se ha dado flexibilidad a la hora de trabajar con información en claro en el directorio asociado a *Dropbox*, considerando que no toda la información almacenada tiene por qué ser de la máxima importancia para el usuario.

2.3.3. Validación de confianza transitiva

Es imposible para *KonEncriptación* conocer qué usuarios forman parte de una carpeta compartida y cuándo un usuario se ha desligado de dicha carpeta, puesto que una vez desligado no existe ningún tipo de notificación que pueda capturarse en Dropbox.

De esta manera, cuando un usuario está interesado en tener acceso a un archivo que está dentro de una carpeta compartida, enviará una petición de acceso que será introducida dentro de la cabecera, para que otros usuarios ya validados puedan otorgarle el permiso para que pueda editarlo.

Así pues, aunque se sigue manteniendo un nexo de confianza transitiva, puesto que un usuario no creador ya validado puede aceptar la petición de otro usuario que lo solicite, el usuario que creó el archivo puede eliminar dicho archivo y no darle acceso de nuevo a ese usuario.

2.3.4. Integración con Dropbox

Con el desarrollo de *KonEncriptación*, se pretende ofrecer una herramienta más versátil que las que actualmente existen y se utilizan. Si utilizamos como patrón la **Tabla 5** del **apartado 1.4** y construimos esta misma con las funcionalidades de *KonEncriptación*, se pueden apreciar las diferencias existentes entre las herramientas de encriptación anteriormente estudiadas en el **apartado 1.4** y la herramienta desarrollada.

Software/ Características	<i>SecretSync</i>	<i>TrueCrypt</i>	<i>Ubuntu One Encrypt/Decrypt</i>	<i>KonEncriptación</i>
Dedicado a un determinado software de almacenamiento virtual	NO	NO	SI	SI (1)
Técnica de trabajo	Directorio – <i>Tunneling</i>	Volumen cifrado	Cifrado individual de archivos	Directorio espejo para trabajo seguro
Tipo de cifrado	<i>AES 256</i>	Varios tipos	<i>Triple DES</i>	<i>RSA 1024 + AES 128</i>
Multiclave	SI	SI	SI	SI
Gestión de cifrado para grupos	NO	NO	NO	SI
Interoperabilidad con el Software de almacenamiento virtual	NO	NO	SI	SI

Tabla 6: Descripción de características de herramientas de encriptación.

(1). Actualmente, la herramienta está desarrollada para trabajar sobre Dropbox debido a que es la herramienta más comercial, extendida y quizás con más problemas de seguridad en el mercado. En versiones futuras, y siempre que se pudiera tener acceso a cualquier archivo de configuración del software de almacenamiento virtual para extraer determinada información necesaria, se podría perfectamente desarrollar otras versiones que se adaptaran a otros software distintos a Dropbox con alguna facilidad.

Como se puede apreciar en la **Tabla 6**, *KonEncriptación* ofrece gestión de cifrado para grupos y sincronización selectiva, puesto que trabaja con un directorio espejo de forma segura. Además, la

integración con *Dropbox* es máxima como se verá en el **apartado 4.1**. De esta manera, se pueden ver todas las mejoras que ofrece KonEncriptación con respecto a las herramientas estudiadas.

2.4. Herramientas de desarrollo

Una vez finalizadas las tres primeras fases del proyecto: *estudio de requisitos, revisión bibliográfica y webs de contenidos y análisis y diseño*, la idea fundamental para la selección de la herramienta de desarrollo fue que ésta fuera totalmente independiente respecto al sistema operativo en el que se trabajara. De esta manera, se podría ofrecer al usuario final una herramienta multiplataforma que cubriera mejor sus necesidades.

Además, conocidas las necesidad de diseño y teniendo una idea general de cómo iba a ser la estructura de la herramienta, el primer paso que se dio fue la búsqueda de recursos. Se comprobaron los componentes y APIs para las distintas herramientas de desarrollo que iban a ser necesarias para la implementación de la misma. Tras una búsqueda web exhaustiva se determinó que la herramienta para el desarrollo del proyecto que mejor se ajustaba a estas necesidades era **java**.

2.4.1. Herramientas criptográficas empleadas

Para el desarrollo de KonEncriptación se han utilizado dos APIs de seguridad destinadas principalmente a la generación y tratamiento de distintos tipos de claves así como al cifrado y descifrado tanto de claves como de información.

java.security

Esta librería ofrece interfaces y clases relacionadas con la seguridad de la información ofreciendo diferentes métodos para generar y almacenar claves, resúmenes y números aleatorios. También ofrece métodos para la generación permisos de acceso.

- **java.security.KeyPair**: almacena una pareja de claves pública – privada generada.
- **java.security.PublicKey**: interfaz que sirve para ofrecer el transporte seguro de la clave pública.
- **java.security.MessageDigest**: genera resúmenes de mensaje. Para ello hay que indicarle qué tipo de resumen va a ser generado, utilizando los ofrecidos por los distintos proveedores que existen actualmente o los permitidos por el propio lenguaje de programación.
- **java.security.SecureRandom**: generador seguro de números pseudoaleatorios. Se trata de un generador criptográficamente fuerte ampliamente utilizado en el mundo de la seguridad java.

Web Oficial: <http://download.oracle.com/javase/6/docs/api/java/security/package-summary.html>

javax.crypto

Esta librería ofrece clases e interfaces para las operaciones de cifrado, generación de claves, autenticación de los mensajes mediante el uso de resúmenes de los mismos o intercambio seguro de claves. Las clases e interfaces utilizadas de esta librería en KonEncriptación son:

- **javax.crypto.SecretKey**: interfaz que asegura el transporte seguro de la clave simétrica.
- **javax.crypto.KeyGenerator**: generador de claves simétricas. Se puede inicializar o no, con el tipo de método de clave simétrica que se desea generar.
- **javax.crypto.IVParameterSpec**: generador del vector de inicialización necesario para poder cifrar en el modo retroalimentación. En KonEncriptación el modo cifrado es CBC.
- **javax.crypto.Cipher**: clase utilizada para cifrar y descifrar información y claves. Contiene los métodos necesarios para ello.

El proceso de cifrado o descifrado con Cipher se inicia instanciando:

- El método a utilizar para cifrar o descifrar.
- El modo de cifrado (*ECB, CBC*, ninguno).
- El tipo de padding utilizado.

Posteriormente, se tiene que especificar el tipo de operación a realizar, comúnmente cifrar o descifrar, y la clave a utilizar para ello.

Cabe destacar los modos utilizados en la implementación de KonEncriptación para cifrar y descifrar la clave simétrica.

- **WRAP_MODE (modo de envoltura)**: tipo de operación donde se envuelve (*cifra*) una clave utilizando un método de cifrado. El resultado es un array de bytes del mismo tamaño que la clave cifrada.
- **UNWRAP_MODE (modo de desenvoltura)**: tipo de operación donde se desenvuelve (*descifra*) una clave cifrada utilizando el mismo método de cifrado utilizado para cifrarla.

Web Oficial: <http://download.oracle.com/javase/6/docs/api/javax/crypto/package-summary.html>

2.4.2. Otro tipo de herramientas utilizadas

Eclipse

Entorno de desarrollo integrado de código abierto multiplataforma para el desarrollo de aplicaciones cliente. Este software ha sido utilizado, bajo lenguaje de programación java, para el desarrollo de KonEncriptación.

Photoshop

Software de edición de imágenes que se permite el diseño y retoque de cualquier tipo de imagen de manera profesional. La mayoría de gráficos e iconos de la aplicación han sido diseñados o retocados con esta herramienta.

Dreamweaver

Software para diseño, construcción y edición de portales Web. La ayuda de KonEncriptación ha sido desarrollada íntegramente con esta herramienta.

NSIS (*Nulsoftl Scriptable Install System*)

Software bajo licencia libre para crear scripts de instalación en plataformas Windows desarrollado por NullSoft. Posee un script que puede integrarse en Eclipse y facilita, mediante un asistente, la creación de instaladores para cualquier aplicación desarrollada en esta herramienta. Ese script ha sido el que se ha utilizado para desarrollar el instalador de KonEncriptación.

VirtualBox

Software de virtualización de plataformas desarrollado por Oracle y que permite instalar máquinas virtuales con diferentes características software y hardware en el equipo donde esté instalado. Este software ha sido utilizado para instalar los sistemas operativos Ubuntu y Kubuntu para el que se han desarrollado versiones Linux de KonEncriptación.

Otras herramientas

Las herramientas estudiadas en los **apartados 1.3 y 1.4** han sido instaladas y utilizadas durante el desarrollo del proyecto para tener un conocimiento directo de las mismas. Esto nos ha ayudado a tener una imagen más objetiva de sus características principales que ha sido fundamental en las etapas iniciales del proyecto.

3. Gestión de archivos cifrados

En este apartado se describe todo lo referente a las estrategias, toma de decisiones y diseño relacionadas e implementadas en la herramienta *KonEncriptación*.

3.1. Estrategias de cifrado

A continuación se describen detalladamente todas las estrategias utilizadas e implementadas en *KonEncriptación* para ofrecer la máxima seguridad a la información del usuario.

3.1.1. Validación de parámetros de inicio de sesión

La herramienta desarrollada en el proyecto cuenta con un archivo de configuración con la siguiente estructura:

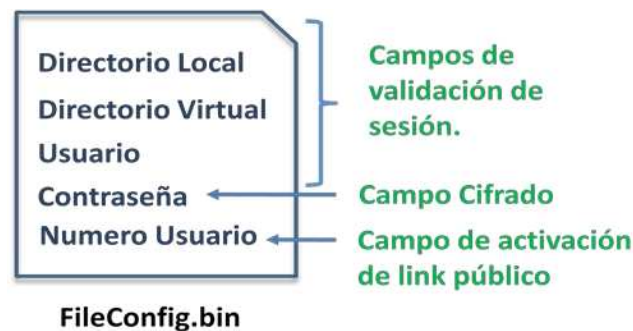


Figura 9: Estructura del Archivo de configuración.

La estructura del archivo, como se puede ver en la **Figura 9**, se divide en tres grupos diferentes cuyas finalidades son distintas. Indicar que este archivo es imprescindible para el buen funcionamiento de la herramienta y, sin él, el funcionamiento de *KonEncriptación* no sería posible.

El primer grupo de campos está destinado a la **validación de parámetros** antes del inicio de sesión. Se trata de *datos sin cifrar* y son necesarios para asegurar que los parámetros de configuración de la herramienta antes del inicio de sesión son totalmente correctos. La descripción de estos campos es la siguiente:

- **Directorio Local:** ruta donde se encuentra el directorio seguro de trabajo del usuario.
- **Directorio Virtual:** ruta donde se encontraba el directorio asociado a *Dropbox* en la última sesión y que debe coincidir con la ruta donde se encuentra el directorio asociado a *Dropbox* al inicio de una nueva sesión de *KonEncriptación*.
- **Usuario:** *email del usuario* de la última sesión, que también debe coincidir con la cuenta asociada a *Dropbox* al inicio de la sesión de *KonEncriptación*.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Todos estos datos pueden ser validados gracias a que la herramienta tiene acceso al archivo de configuración de *Dropbox* (*config.db*).



Figura 10: Campos utilizados del archivo de configuración de *Dropbox* para validación de la sesión.

Como se ve en la **Figura 10**, los campos necesarios de la base de datos *config.db* de *Dropbox* para validar los parámetros antes del inicio de sesión de KonEncriptación son:

- **Dropbox_Path:** directorio asociado a la cuenta de *Dropbox* en el equipo.
- **Email:** cuenta asociada a *Dropbox*.

Una vez que la herramienta contrasta la información de ambos archivos y se asegura que los campos de los directorios, local y virtual, existen, y que los usuarios de KonEncriptación y *Dropbox* son los mismos, se puede asegurar el correcto inicio de sesión una vez validada la clave de KonEncriptación.

Por otra parte, el campo **contraseña** es necesario para la *autenticación del usuario*. A diferencia de los campos descritos anteriormente, el campo contraseña se encuentra cifrado con el login y password del usuario. Indicar que el password del usuario *no es almacenado* en ningún momento en el archivo de configuración sino que se utiliza una cadena con el texto **“OK”**, que es cifrada y almacenada en el campo contraseña previamente, la que es guardada en el archivo de configuración. Si el usuario introduce su password y login correctamente, esta cadena se podrá descifrar con la clave privada generada y el usuario se habrá autenticado y, por tanto, podrá tener acceso a KonEncriptación.

Para el cifrado del campo contraseña, se ha utilizado en primer lugar un sistema de clave *simétrica AES 128*, aplicándole posteriormente a la contraseña cifrada el método de envoltura de claves descrito en el **apartado 3.1.4**.

Por el contrario, el resto de campos del archivo de configuración no están cifrados puesto que si se cifrara toda la información del archivo con la clave del usuario no se podrían hacer las validaciones pertinentes del inicio de sesión hasta que el usuario no introdujera su password correctamente.

Por último, el campo **número usuario**, está relacionado con la activación de la función de enlace público descrita en el **apartado 5.7.6**.

3.1.2. Generación de claves asimétricas basadas en contraseña

Cada vez que un usuario es validado por el sistema al inicio de sesión, el sistema generará una pareja de claves (**pública y privada**) que serán indispensables para realizar cualquier operación relacionada con el cifrado o descifrado.

Para generar la pareja de claves, KonEncriptación utiliza la combinación del login y el password del usuario. Es necesario utilizar la combinación de estos dos campos para poder obtener así una pareja de claves distintas para cada uno de los usuarios de KonEncriptación.



Figura 11: *Proceso de generación de parejas de claves.*

La **Figura 11** muestra esquemáticamente cómo es el proceso de generación de la pareja de claves pública - privada en KonEncriptación. El proceso de generación es el siguiente:

- Se utiliza una **clave pública RSA** para la generación de las mismas.
- Cada vez que se genera el par de claves al inicio de sesión se utiliza **una semilla**.
- El tamaño de las claves resultantes es de **1024 bytes** cada una.
- **Las claves no se almacenan físicamente**. Se crean y destruyen al inicio y final de la sesión.
- La **clave pública** será utilizada en los proceso de cifrado (**apartado 3.2.1.1**) y envío de peticiones (**apartado 3.4.1**).
- La **clave privada** será utilizada en los proceso de descifrado (**apartado 3.2.2**).

3.1.3. Generación de claves simétricas

Para el cifrado de información, KonEncriptación está diseñado para generar claves simétricas aleatoriamente mediante un algoritmo de clave simétrica **AES**. La longitud de la clave es de **128 bits**. Esta clave será almacena de forma cifrada (**apartado 3.2.1.1**) en cada una de las entradas de la cabecera correspondientes a los usuarios que ya estén validados.



Figura 12: Creación de clave simétrica.

3.1.4. Envoltura de la clave simétrica con clave pública

Se utiliza este método de cifrado para almacenar de forma segura la clave simétrica con la que ha sido cifrada la información de un archivo y evitar que usuarios no validados puedan tener acceso a dicha clave, y por tanto a la información que contiene el archivo.

Este método de cifrado crea una envoltura alrededor de una clave simétrica mediante una clave pública, convirtiendo así la información en algo ilegible para los atacantes.



Figura 13: Proceso de envoltura de clave simétrica.

Como se puede ver en la **Figura 13**, el proceso de envolver de clave (**WRAP**) sería el siguiente:

- Poseemos una clave simétrica que es la que queremos hacer ilegible y una clave pública que es la que vamos a utilizar para el proceso de envoltura.
- El contenedor (envoltura) es donde viajará la clave de manera ilegible.
- La acción de envoltura consiste en guardar esa clave en un contenedor ilegible, haciendo uso de la clave pública para el cifrado de dicha información.
- El método de envoltura solo permite cifrar claves, no otro tipo de información.

La única forma de poder desenvolver esa clave es utilizando la clave privada del usuario que la cifró y saber con qué método fue generada la clave pública. De otra manera, no se podrá obtener dicha clave.

Este proceso se suele usar cuando se crea una cabecera nueva o cuando se valida una petición de usuario.

3.1.5. Desenvoltura de clave simétrica con clave privada

Es el proceso inverso al de envoltura de clave simétrica. Se trata de extraer la clave simétrica que está envuelta y cifrada con la clave pública de un usuario.

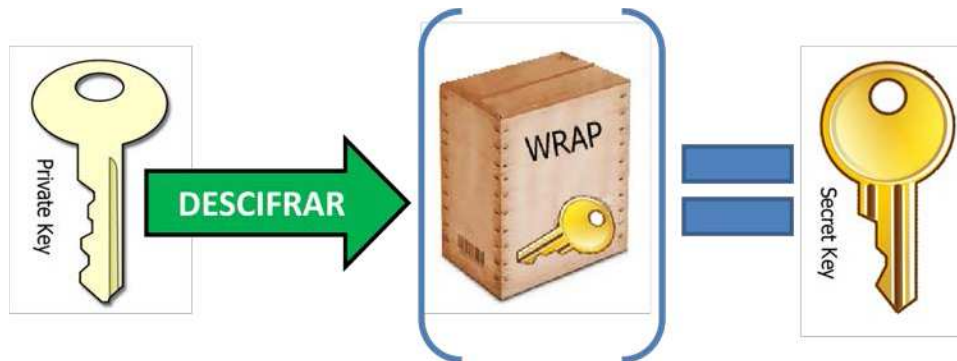


Figura 14: Proceso de desenvoltura de clave simétrica.

Como se puede ver en la **Figura 14**, el proceso de desenvolver de clave (**UNWRAP**) sería el siguiente:

- Poseemos la **clave privada** del usuario y conocemos el método con el que fue generada la clave simétrica.
- La clave privada es utilizada para desenvolver la información cifrada con la clave pública del usuario en el proceso de envoltura.
- Una vez tengamos la información desenvuelta que es la clave secreta podremos utilizarla utilizando los algoritmos de cifrado que se especificaron en la cabecera para esa clave secreta.

Este método está ligado directamente con las operaciones de descifrado.

3.1.6. Cifrado de la información con clave simétrica

Para cifrar la información del archivo en claro se utiliza un método de cifrado con clave simétrica, es decir, se utiliza la misma clave para cifrar y descifrar.

Como se describe en el **apartado 3.2.1**, referente a las cabeceras, la clave simétrica, con la que se cifra y descifra un archivo, se transporta cifrada en las entradas de cabecera de los usuarios que han sido validados para tener acceso a la información. Esta clave simétrica es diferente para cada archivo puesto que se genera aleatoriamente cada vez que se va a cifrar un archivo por primera vez.

Las características del cifrado de la información son las siguientes:

- El método de clave simétrico utilizado es **AES**.
- La longitud de la clave es de **128 bits**.
- Se utiliza un **modo de cifrado por bloques CBC** (*Cipher Block Chaining*).
- El padding utilizado es el estándar **PKCS5**.

3.2. Cifrado y descifrado de archivos

En este apartado se describen paso a paso y esquemáticamente los procesos de cifrado y descifrado de un archivo, así como la gestión de peticiones de acceso.

3.2.1. Estructura de un archivo cifrado

La estructura de un archivo cifrado consta de dos áreas bien diferenciadas; el área destinada a guardar metainformación acerca de los usuarios, sus estados y contraseñas, y la parte destinada a la información en sí.

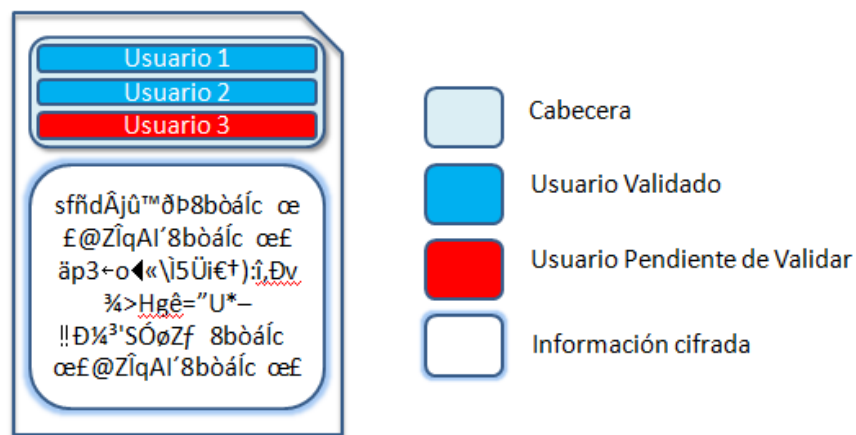


Figura 15: Estructura de un archivo cifrado.

La **Figura 15** muestra la estructura de un archivo cifrado generado con *KonEncriptación*. En el inicio del archivo, parte superior, se almacena la cabecera, que consiste en un número variable de entradas asociadas a los usuarios que tengan acceso a la información o lo hayan solicitado (**apartado 3.5**), mientras que la parte inferior almacena la información cifrada.

La **cabecera de un archivo cifrado** se podría definir como la parte destinada a guardar información asociada con los usuarios que tienen acceso a la información o que lo han solicitado. Dicha cabecera es dinámica en función del **número de entradas** y del estado de la información que contenga.

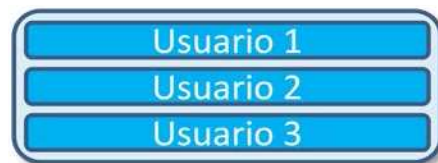


Figura 16: Cabecera de un archivo cifrado con tres entradas.

Una **entrada de una cabecera** podría definirse como un registro donde se guarda información que identifica de manera única a un usuario y determina si éste puede o no acceder a la información que hay cifrada en el archivo donde se encuentra almacenada dicha cabecera.

Cada **entrada de la cabecera** almacena los siguientes campos:

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- **Usuario:** se corresponde con el **correo electrónico** asociado a la cuenta de *Dropbox*. Además, debe coincidir con el de la cuenta usada por KonEncriptación. Este campo identificará de manera única a cada usuario en la cabecera.
- **Algoritmo de Cifrado:** algoritmo utilizado para cifrar la información del archivo original.
- **Clave Pública:** almacena la clave pública del usuario generada al inicio de sesión y que se utilizará para cifrar la clave simétrica en el proceso de envoltura de la clave simétrica (**apartado 3.1.4**).
- **Petición:** indica si la entrada de la cabecera es una petición hecha por un usuario que quiere tener acceso al archivo cifrado o es una entrada de un usuario ya validado (**apartado 3.4**).
- **Clave simétrica:** almacena la clave simétrica cifrada con la clave pública del usuario mediante el método de envoltura de claves (**apartado 3.1.4**). De esta manera, se asegura que sólo el usuario autorizado de esa entrada pueda descifrarla y tener acceso a ella.
- **IV:** almacena el vector de inicialización que fue utilizado para cifrar la información del archivo cifrado con la clave pública del usuario. Este valor es necesario para poder descifrar el archivo. El tamaño del vector de inicialización es 16.

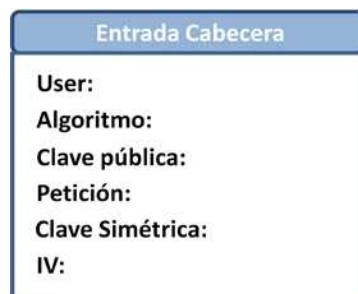


Figura 17: Estructura de una entrada de la cabecera.

3.2.2. Proceso de cifrado de archivos

Para realizar el cifrado de un archivo se siguen los siguientes pasos:

1. Generar la clave simétrica con **AES - 128** y el vector de inicialización para cifrar la información.
2. Envolver la clave simétrica y el vector de inicialización con la clave pública **RSA - 1024**.
3. Insertar los datos en la cabecera.
4. Insertar la cabecera en el nuevo archivo que contendrá los datos cifrados.
5. Leer bloques de tamaño **1MB** del archivo en claro y cifrarlo con la clave simétrica.
6. Insertar los bloques cifrados de tamaño **1MB** en el archivo cifrado a partir de la cabecera.

7. Añadir el padding en el último bloque.

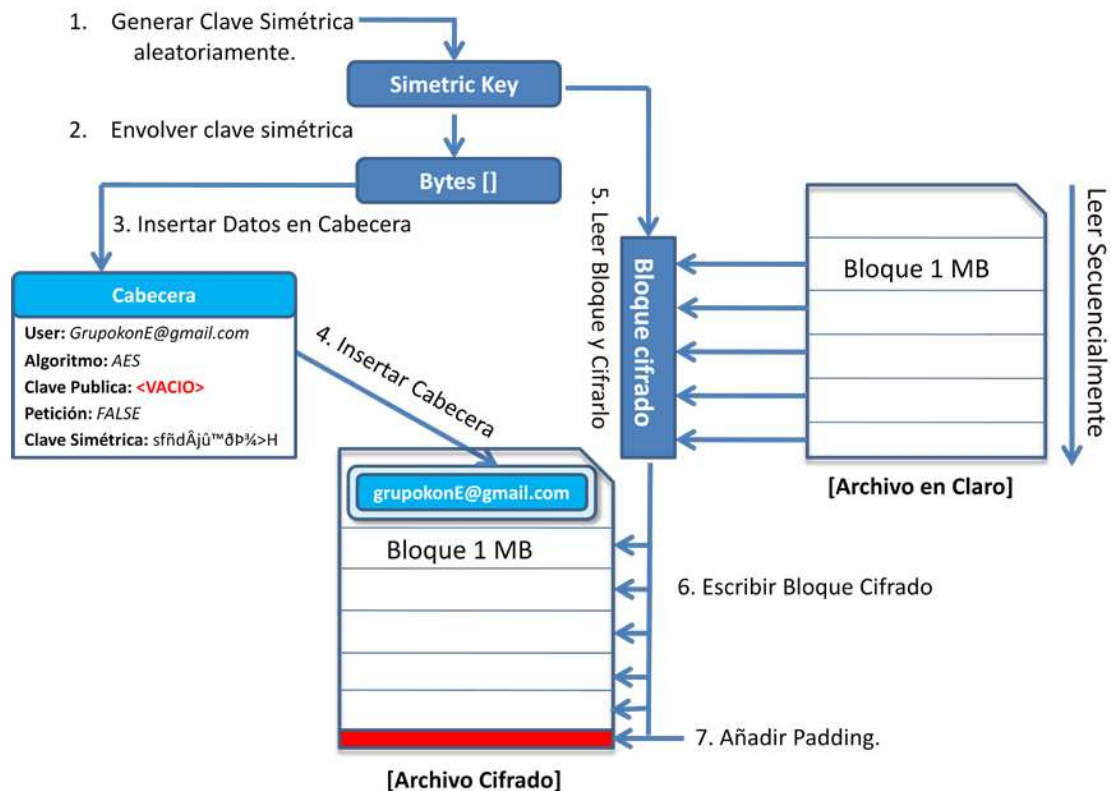


Figura 18: Proceso de cifrado de un archivo.

3.2.3. Proceso de descifrado de archivos

Para realizar el descifrado de un archivo hay que seguir los siguientes pasos:

1. Leer la cabecera del archivo cifrado.
2. Comprobar si el usuario está en estado **validado**.
3. Extraer la clave simétrica cifrada para ese usuario y descifrar el vector de inicialización con la clave privada del usuario.
4. Desenvolver la clave simétrica cifrada con la clave privada del usuario.
5. Descifrar los bloques de tamaño **1MB** del archivo cifrado con la clave simétrica y el vector de inicialización obtenidos.
6. Escribir los bloques de tamaño **1MB** descifrados en el nuevo archivo en claro.

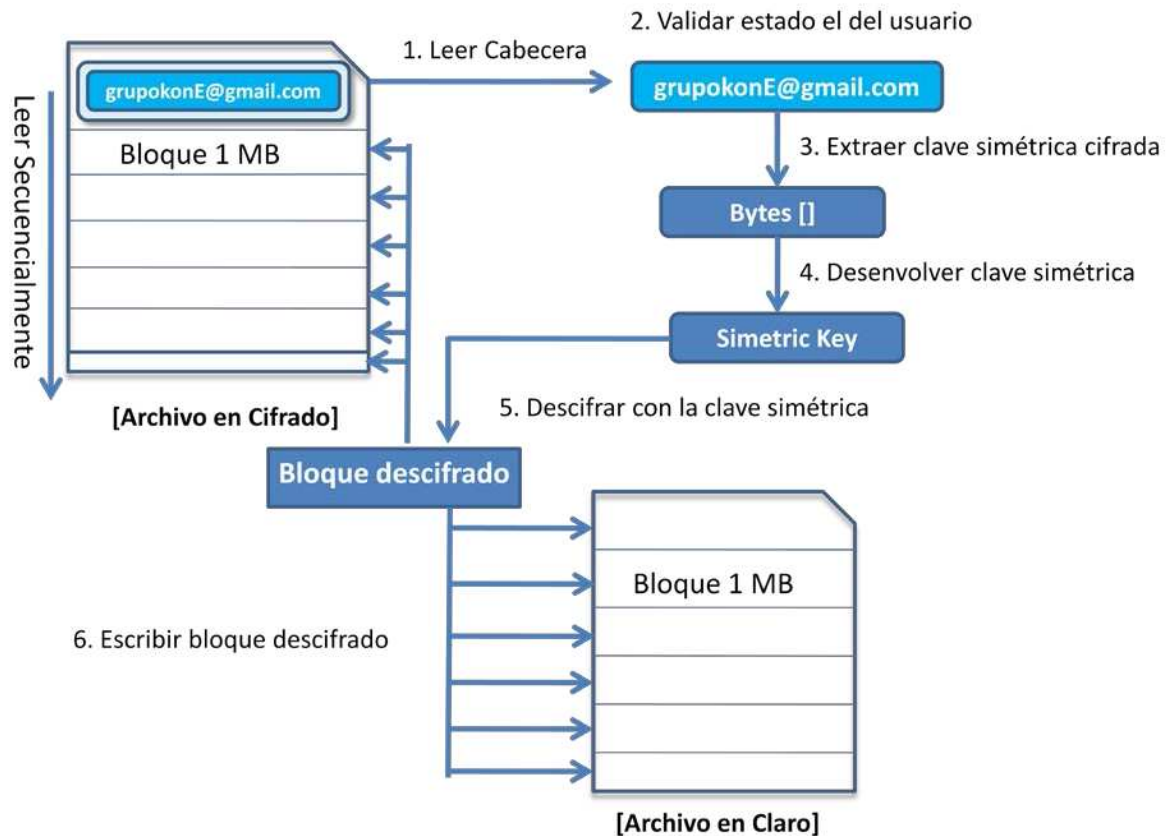


Figura 19: Proceso de descifrado de un archivo.

3.3. Políticas de acceso

Se han establecido las siguientes políticas de acceso para establecer qué usuarios tienen permiso de modificación de los archivos cifrados y además puedan permitir el acceso de otros usuarios a dichos archivos. Esto evita el uso indebido de los archivos cifrados por parte de usuarios que no tengan permiso para hacerlo.

El apartado 2.2.2 describe el problema sobre confianza transitiva que existe cuando terceras personas acceden a la información que otros usuarios depositan en carpetas compartidas.

En una primera instancia, se barajó la posibilidad de establecer una política rígida donde solo el primer creador del archivo cifrado, **dueño**, fuera el único que pudiera aceptar las peticiones de acceso de los usuarios que quisieran tener acceso a la información. Esta idea fue descartada debido a las siguientes consideraciones:

- Evitar, que por largas ausencias del usuario dueño, el resto de personas no pudieran tener acceso a dicha información.
- Evitar la centralización del usuario dueño para aceptar las peticiones de acceso.
- Entender que el resto de usuarios actúan de buena fe, hasta cierto punto, puesto que es una herramienta colaborativa y la información compartida tiene intereses comunes.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

En contraposición, se han establecido algunas leves restricciones para que un usuario propietario o con permiso de acceso siempre pueda tener acceso a la información. A continuación se tratarán las restricciones de acceso de terceras personas a la información en carpetas compartidas donde haya como mínimo dos usuarios:

- **Ningún usuario validado puede ser eliminado de una cabecera.** Todos los usuarios tienen siempre acceso a la información, independientemente de quién la edite.
- **Un usuario sin permiso de acceso a un archivo cifrado no podrá realizar ninguna operación con el mismo.** Por ejemplo, no podrá eliminar, renombrar o reemplazar dicho archivo.

Sin embargo, el sistema presenta la siguiente debilidad. Un usuario sin permiso de acceso podría coger un archivo donde sí tuviera una cabecera con permiso, renombrarlo con el nombre del archivo al que quiere tener acceso, reemplazando éste, con lo que aparecerá como un usuario con permisos en su cabecera. De esta forma, si el propietario del archivo original no se da cuenta del cambio en la cabecera y en los contenidos, de la versión en Dropbox, al actualizar su copia en Dropbox, permitiría al usuario sin permisos acceder a dicha información.

- **Se le permitirá a un usuario con permisos eliminar el archivo cifrado,** para de esta manera comenzar de nuevo proceso de otorgar permisos a sus usuarios de confianza. Así tendrá la posibilidad, en cierta medida, de volver a negarle el acceso a aquellos usuarios con los que no quiere compartir esa información.

3.4. Gestión de peticiones de acceso

En este apartado se describen todas las operaciones y estrategias de diseño que giran alrededor del acceso a los archivos cifrados por parte de los usuarios de KonEncriptación. Como se ha visto en el [apartado 3.2.1](#), cada cabecera de un archivo cifrado contiene una o varias entradas y cada una de estas entradas ofrecen principalmente información acerca de los permisos de acceso de los usuarios a dicho archivo.

Entrada Cabecera
User:
Algoritmo:
Clave pública:
Petición:
Clave Simétrica:
IV:

Figura 20: Entrada de una cabecera. Campo petición.

El **campo petición** de la entrada de una cabecera permite a la herramienta conocer si un usuario puede o no tener acceso a la información cifrada en el archivo. Una petición de acceso tiene **dos estados** diferentes:

- **Validado:** indica que el usuario de esa entrada tiene acceso a la información.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- **Petición:** indica que el usuario está esperando que otro usuario le otorgue permiso de acceso a su entrada para que pueda tener acceso a la información.

El campo petición y algunos de los campos de las entradas de las cabeceras serán utilizados y/o editados en las operaciones que se describen en los siguientes apartados.

3.4.1. Envío de petición de acceso

Cuando KonEncriptación lee una cabecera de un archivo cifrado y no encuentra al usuario de sesión en ninguna de las entradas de dicha cabecera es indicador de que el usuario no tiene acceso al archivo y tampoco ha realizado anteriormente ninguna petición de acceso para tenerlo.

Si un usuario desea tener acceso a un archivo cifrado debe enviar una petición de acceso y esperar a que sea aceptada por alguno de los usuarios con los que comparte este archivo y que ya están validados. Como método alternativo, un usuario utilice la agenda de usuarios para otorgarle dicho permiso (**ver apartado 4.2**).

Para el envío de una petición de acceso a un archivo cifrado, o lo que es igual, introducir una nueva entrada en estado de petición en la cabecera de un archivo cifrado, KonEncriptación realiza el siguiente proceso:

1. Leer la cabecera del archivo cifrado y comprobar que no existe entrada para el usuario de sesión.
2. Generar y rellenar una nueva entrada para el usuario de la sesión en estado de petición.
3. Agregar la nueva entrada en la cabecera leída.
4. Escribir la nueva cabecera en el archivo cifrado y volcar de nuevo la información cifrada.

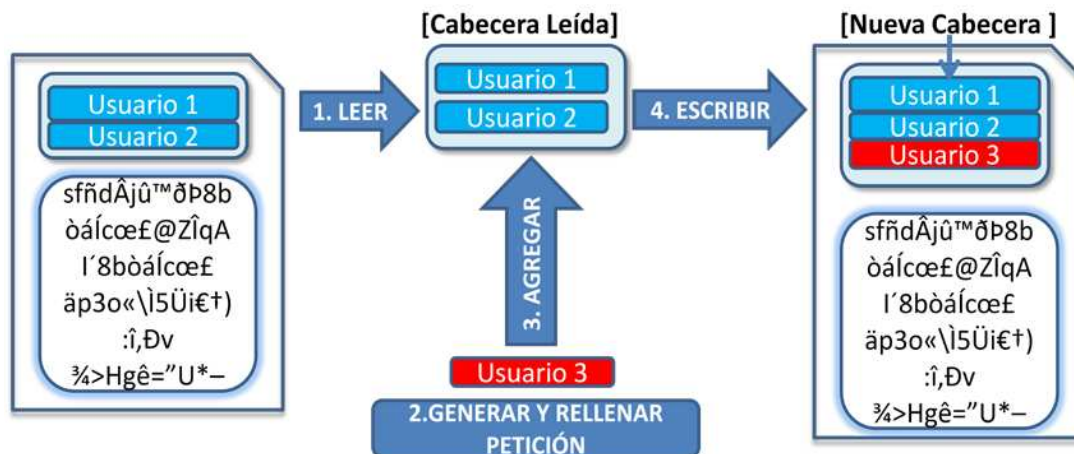


Figura 21: Proceso de generación de una petición de acceso.

El **paso 2**, donde se genera y se rellena una nueva entrada en estado de petición, sigue el siguiente patrón:

- Introducir el nombre del usuario (**correo electrónico**).

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Introducir el campo algoritmo como **vacío**, puesto que este campo está ligado con la clave simétrica.
- Introducir la clave pública del usuario que será utilizada por el usuario que acepte la petición para cifrar la clave simétrica.
- Establecer el campo petición a **TRUE**.
- Introducir la **clave simétrica como vacía**, puesto que no se conoce aún.
- Introducir el **vector de inicialización como vacío**, puesto que no se conoce.

La siguiente figura muestra una entrada de la cabecera en estado de petición:

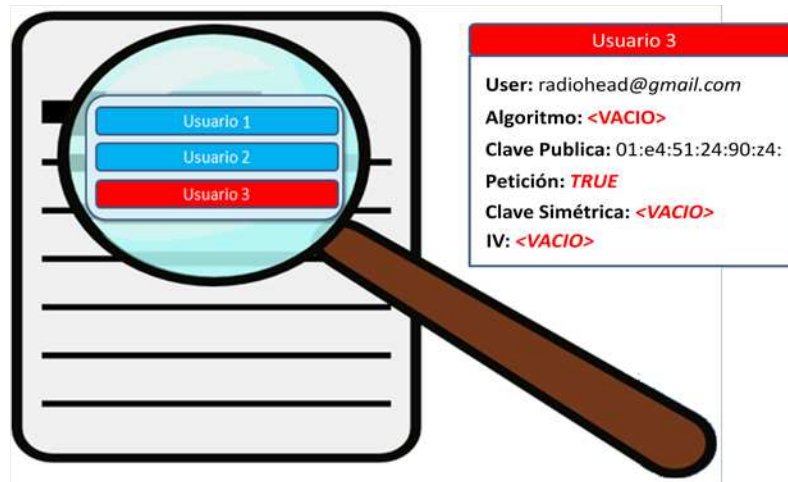


Figura 22: Entrada de la cabecera en estado de petición

Para el **envío de peticiones de acceso** se aprovecha la sincronización del archivo cifrado por parte de *Dropbox* para que sea enviado al resto de usuarios.

3.4.2. Aceptar petición de acceso

Cuando la herramienta lee una cabecera de un archivo cifrado y encuentra alguna entrada diferente a la del usuario de sesión en estado de petición, ofrece la posibilidad al usuario de sesión de aceptarla.

Previamente, la herramienta comprobará que el usuario de la sesión tiene permiso de acceso al archivo validando la entrada de la cabecera asociado a este. En caso de no encontrarse su entrada en la cabecera o tenerla en estado de petición, pendiente de ser validada, el usuario no podrá realizar esta acción.

Si un usuario legítimo desea dar permiso de acceso a otros usuarios que han enviado peticiones a un archivo cifrado simplemente deberá aceptarlas. Para dar permiso a otros usuarios hay que cifrar la clave secreta (utilizada para cifrar el archivo) con la clave pública del usuario que ha solicitado la petición de acceso y añadir esta información a la cabecera. Además, también se introducirá el vector de inicialización en la cabecera del archivo cifrado con la clave pública del usuario al que pertenece la petición.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

El proceso donde una nueva petición de acceso es aceptada e introducida en la cabecera de un archivo cifrado en *estado validado* sigue los siguientes pasos:

1. Leer la cabecera del archivo cifrado.
2. Comprobar y extraer la petición que va a ser aceptada.
3. Procesar la entrada en *estado de petición*, generando las claves necesarias y establecer el nuevo estado como **validado**.
4. Agregar la entrada procesada a la cabecera leída.
5. Escribir la nueva cabecera en el archivo y volcar la información de nuevo en el archivo cifrado.

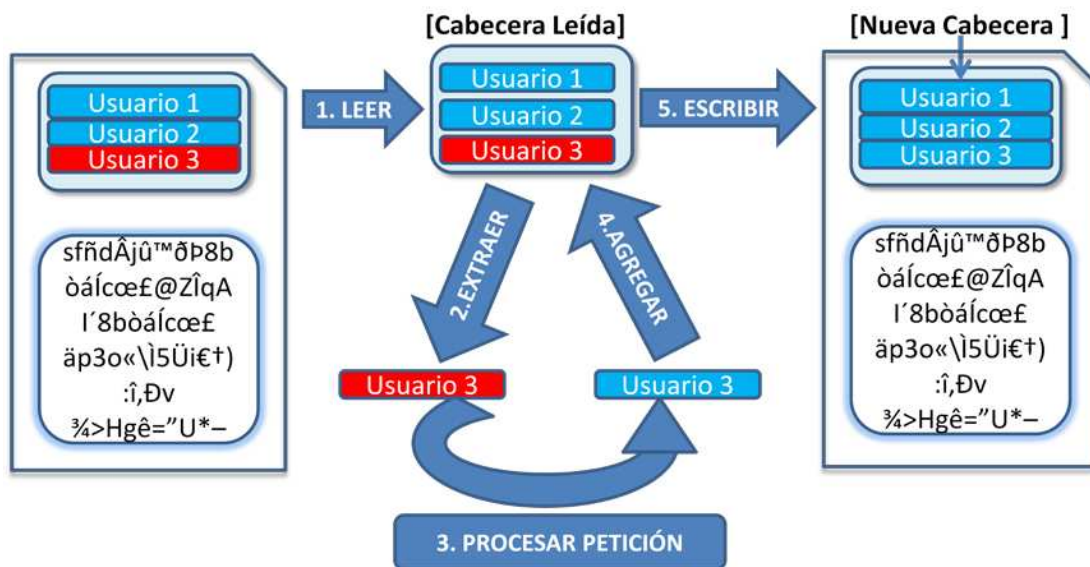


Figura 23: Proceso de aceptar una petición de acceso.

El **paso 3**, donde *se procesa la entrada en estado de petición*, sigue el siguiente patrón:

- Mantener el nombre del usuario (**correo electrónico**).
- Introducir el nombre del algoritmo con el que se ha generado la clave simétrica en el correspondiente campo de la entrada.
- Eliminar la clave pública puesto que ya no es necesaria.
- Establecer el campo petición como *validado* (**FALSE**).
- Introducir la clave simétrica cifrada con la pública para que el usuario correspondiente pueda descifrarla con su privada.
- Introducir el vector de inicialización cifrado con la clave pública del usuario de la petición.

La **Figura 24** muestra el estado de una entrada de la cabecera en estado validado.

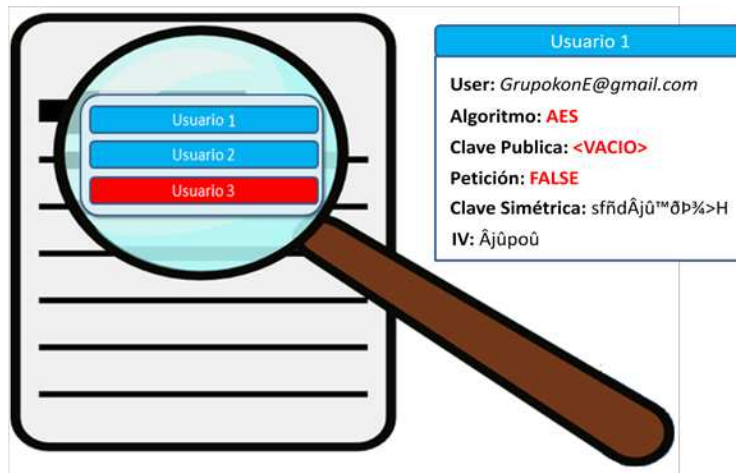


Figura 24: *Entrada de la cabecera en estado validado*

En este proceso, al igual que en el de envío de peticiones de acceso, se aprovecha la sincronización del archivo por parte de *Dropbox* una vez que se han guardado la nueva cabecera con las peticiones validadas.

3.4.3. Búsqueda de peticiones de acceso

KonEncriptación realiza dos operaciones distintas para buscar peticiones de acceso en archivos cifrados. La primera de ellas se centra en la búsqueda de peticiones de acceso en un archivo cifrado y la segunda, que integra a la primera, tiene como ámbito de búsqueda todas las peticiones de acceso de los archivos cifrados que se encuentran dentro de un directorio y sus subdirectorios.

Para almacenar los resultados de las búsquedas KonEncriptación utiliza un *array de datos* de tipo **DefaultMutableTreeNode** (nodos de una estructura árbol) que va a ser utilizado posteriormente como modelo para los árboles que muestran el resultado de las búsquedas después de realizar las operaciones en KonEncriptación de:

- Ver peticiones de acceso pendientes ([ver apartado 5.6.6.3](#)).
- Buscar peticiones de acceso en directorios ([ver apartado 5.6.6.4](#)).
- Fusionar dos cabeceras al reemplazar un archivo cifrado ([ver apartado 5.8.4](#)).

La estructura **DefaultMutableTreeNode** tiene la siguiente forma:

- **Objeto:** puede ser:
 - Nombre del archivo cifrado.
 - Nombre del usuario.
 - Nombre del directorio de búsqueda.
- **Nodo Hoja:** opción para indicar si es un nodo o una hoja del árbol. Por ejemplo, de un archivo cifrado, pueden colgar los usuarios que tienen peticiones pendientes.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- **Seleccionado:** si la casilla de selección asociada al nodo está seleccionada o no. Por ejemplo, de esta manera la aplicación puede saber si ese elemento (usuario, directorio o archivo cifrado) está seleccionado para ser procesado.

CheckNode		
Object	boolean	boolean
Objeto	Nodo Hoja	Seleccionado

Figura 25: Estructura CheckNode: tipos y nombre de los campos.

CheckNode		
C:\User\Dropbox\Prueba.txt.cif	true	false

Figura 26: Entrada de un CheckNode.

3.4.3.1. Búsqueda de peticiones de acceso en un archivo cifrado

La búsqueda de peticiones de acceso en archivos cifrados por parte de la herramienta es un proceso bastante sencillo. Este proceso de búsqueda sigue el siguiente patrón:

1. Leer la cabecera del archivo cifrado.
2. Leer secuencialmente las entradas de la cabecera y extraer las entradas en estado de petición almacenándolas en una **lista de peticiones de acceso**.
3. A partir de la lista de peticiones y del nombre del archivo cifrado se construye el árbol resultado de la búsqueda de la siguiente manera:
 1. *Raíz del árbol* con el nombre del archivo donde se buscan las peticiones.
 2. A continuación, se añaden el nombre de los usuarios que tienen peticiones pendientes en el archivo.

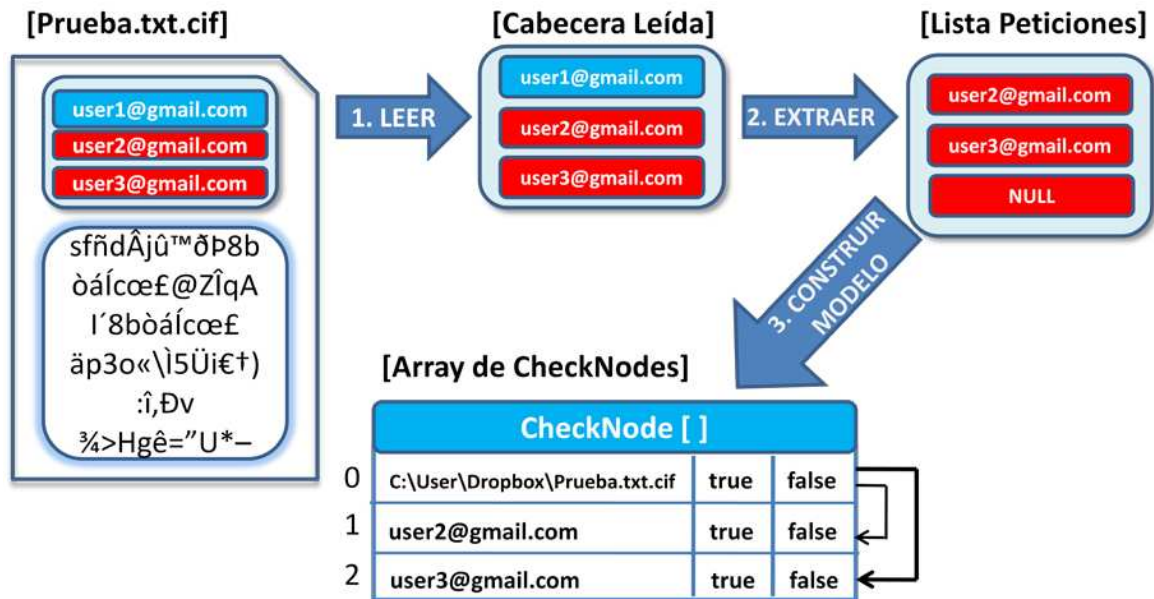


Figura 27: Proceso de búsqueda de peticiones de acceso en un archivo cifrado.

3.4.3.2. Búsqueda de peticiones de acceso en directorios

El proceso de búsqueda de peticiones de acceso en directorios es prácticamente igual al de la búsqueda en archivos. La diferencia está en la **estrategia de búsqueda de las peticiones de acceso** y en la construcción y el modelo de datos resultante.

El proceso de búsqueda de peticiones de acceso en un directorio es el siguiente:

1. Se realiza un descenso por el árbol de directorios en *inorden* buscando archivos cifrados.
2. Si se encuentra un archivo cifrado se lee la cabecera para determinar si hay peticiones de acceso.
3. Si existen peticiones de acceso pendientes se introducen en la lista de peticiones.
4. Posteriormente, las peticiones de acceso encontradas se agregan al árbol de resultados de búsqueda para su presentación en pantalla.

El modelo de datos se va construyendo de la siguiente manera:

- *La raíz del árbol*: coincide con el *nombre del directorio*.
- De la raíz cuelgan: *los usuarios*.
- Y cada usuario tendrá una lista con las **rutas parciales** de los archivos donde el usuario tiene las peticiones pendientes de ser aceptadas. La ruta parcial de un archivo es la ruta que comienza a partir del directorio raíz del directorio local o remoto y termina en dicho archivo.

Por ejemplo: la ruta parcial de C:\user\Dropbox\Fotos\102.jpg sería **Fotos\102.jpg**.

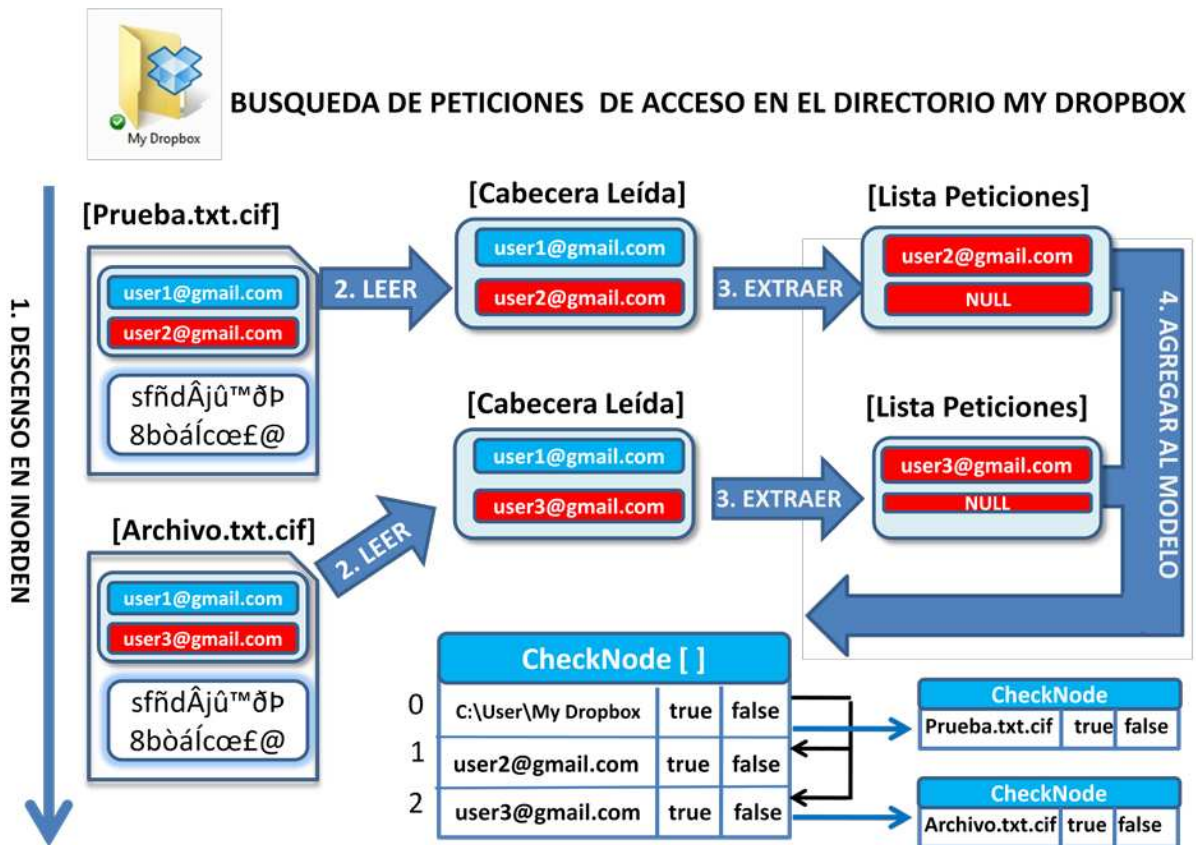


Figura 28: Proceso de búsqueda en un directorio.

KonEncriptación utiliza una estrategia de **recorrido en inorden de árboles** para la búsqueda de peticiones de acceso en los archivos cifrados que se encuentran dentro de un directorio. Para implementar dicho recorrido, se ha tenido que utilizar un método recursivo que es llamado cada vez que en el recorrido de descenso del árbol de archivos se encuentra un directorio.

La parte derecha de la **Figura 29** muestra la secuencia en la que los archivos y directorios serán visitados en el proceso de búsqueda de peticiones de acceso en el directorio *Compárteme*. Conforme se vayan encontrando archivos cifrados que contengan peticiones pendientes, la información se irá guardando de la misma forma que muestra la **Figura 28**.

El valor **(4*)** de *Nivel 1* de la **Figura 29**, indica que se ha llamado a un nuevo procedimiento recursivo para que se evalúen los hijos de dicho directorio.

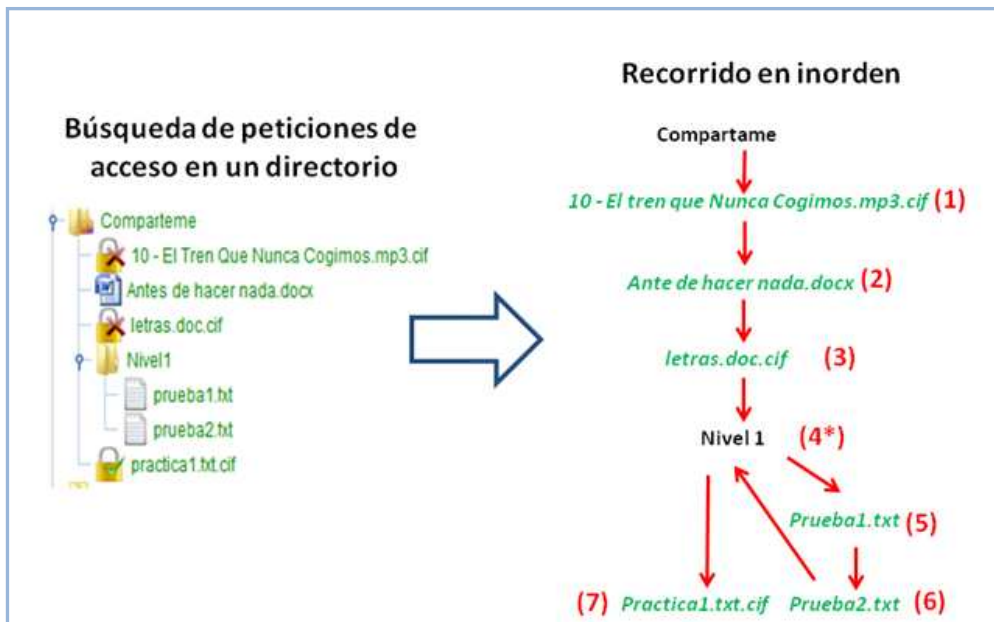


Figura 29: Estrategia de recorrido del árbol de archivos en inorden.

3.4.4. Fusión de permisos de acceso al reemplazar un archivo cifrado

Existen operaciones en las que el usuario puede tener que decidir si reemplaza o no un archivo cifrado ya existente. Estas operaciones son:

- Renombrar
- Cifrar
- Cifrar Aquí
- Mover
- Enviar archivos cifrados entre los directorios local y remoto.
- Pegar

Cuando se va a reemplazar un archivo cifrado por otro, la herramienta seguirá una estrategia de fusión para unir los permisos de acceso de ambos archivos cifrados.

Si un archivo cifrado va a ser reemplazado por otro es imprescindible que el usuario de la sesión tenga permisos de acceso en ambos archivos. Si es así, la herramienta comenzará a realizar esta estrategia de criba de usuarios entre ambas cabeceras con el fin de ir construyendo un modelo de datos similar al del apartado 3.4.3 y que será utilizado para mostrar al usuario el posible estado final, pero no definitivo, de los permisos de acceso del archivo cifrado.

Para almacenar los datos en el modelo, la herramienta tendrá que hacer uso de una nueva estructura de datos **CheckNodeReemplazo** y que tiene la siguiente forma:

- **Objeto:** puede ser:
 - El nombre del archivo cifrado.
 - El nombre del usuario.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- El nombre del directorio de búsqueda.
- **Nodo Hoja:** opción para indicar si es un nodo o una hoja del árbol. Por ejemplo, de un archivo cifrado, pueden colgar los usuarios que tienen peticiones pendientes.
- **Seleccionado:** si la casilla de selección asociada al nodo está seleccionada o no. Por ejemplo, de esta manera la aplicación puede saber si ese elemento (usuario, directorio o archivo cifrado) está seleccionado para ser procesado.
- **Modificable:** si el usuario puede ser o no seleccionado para evitar que se edite. Por ejemplo, para evitar que no se puedan eliminar usuarios con permiso en un proceso de fusión.

La única diferencia entre esta estructura y *CheckNode* (Figura 25) es que se añade un campo **Modificable**. Este campo es esencial, puesto que es la única forma de que el modelo de datos sepa que ese campo no puede ser modificado. Así, los usuarios que tengan el acceso validado a alguno de los archivos cifrados siempre formarán parte de la nueva cabecera en ese estado y no podrán ser eliminados puesto que están bloqueados y no pueden serlo por las restricciones descritas en el *proceso de criba*.

CheckNodeReemplazo			
Object	boolean	boolean	boolean
Objeto	Nodo Hoja	Seleccionado	Modificable

Figura 30: Estructura *CheckNodeReemplazo*: tipos y campos.

CheckNodeReemplazo			
C:\User\Dropbox\Prueba.txt.cif	true	false	true

Figura 31: Entrada de un *CheckNodeReemplazo*.

Una vez definida la estructura donde se va a almacenar el modelo de datos podemos pasar a explicar el **proceso de criba** de las cabeceras cuando se reemplaza un archivo cifrado. Este proceso es el siguiente:

1. Leer la cabecera del archivo que va a ser reemplazado.
2. Leer la cabecera del archivo que va a sustituir al reemplazado.
3. Realizar el proceso de criba de los permisos de usuario de ambas cabeceras para construir el modelo de datos. El *proceso de criba* tendrá en cuenta:

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Los usuarios distintos al de sesión que tengan acceso a la información en alguno de los dos archivos, es decir, que estén validados, formarán parte de la nueva cabecera y tendrán acceso a la información del nuevo archivo.
- Los usuarios distintos al de sesión que tengan alguna petición de acceso en alguno de los dos archivos, se mantendrán en este estado a espera de que el usuario de la sesión las acepte y pasen a ser parte de la nueva cabecera como validados.

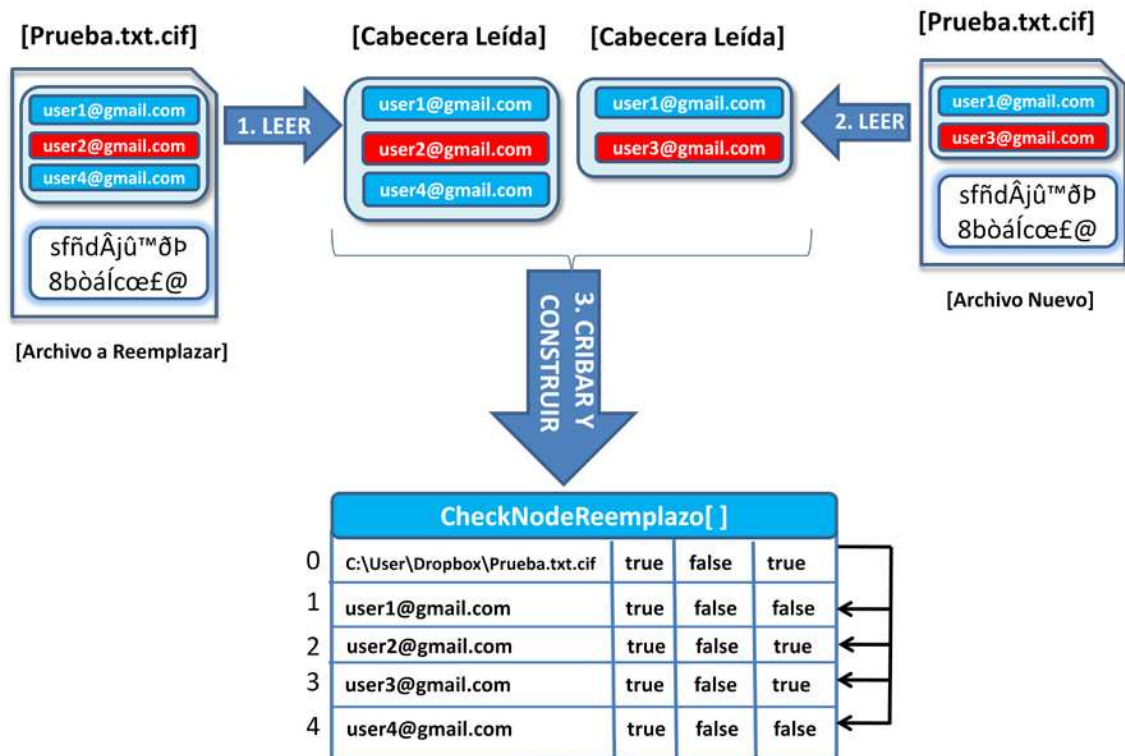


Figura 32: Proceso de criba de cabeceras.

3.5.5. Validación de peticiones de acceso

Una vez representados los resultados obtenidos de las búsquedas de peticiones de acceso o de la fusión de ambas cabeceras al reemplazar un archivo cifrado, el usuario de sesión podrá *validar*, es decir, otorgarle o no permiso de acceso a los usuarios que se encuentran en **estado de petición**.

Si se van a validar usuarios tras el proceso de fusión de cabeceras, serán representados tanto los usuarios que tienen ya acceso como los que no lo tienen, al contrario de las otras dos opciones anteriores dónde sólo se representan los usuarios que no tienen acceso. Los usuarios con acceso para este proceso, como indicamos en el **apartado 3.4.4**, no podrán ser eliminados ni editados y formarán parte de la nueva cabecera.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Una vez que el usuario de sesión haya escogido a los usuarios a los que desea otorgarle permiso de acceso en cada uno de los archivos donde corresponde cada una de las peticiones se realizará el proceso para aceptar peticiones de acceso descrito en el **apartado 3.4.2**.

En la siguiente Figura se muestra cómo quedaría un archivo cifrado tras fusionar dos cabeceras al reemplazar un archivo cifrado utilizando KonEncriptación.

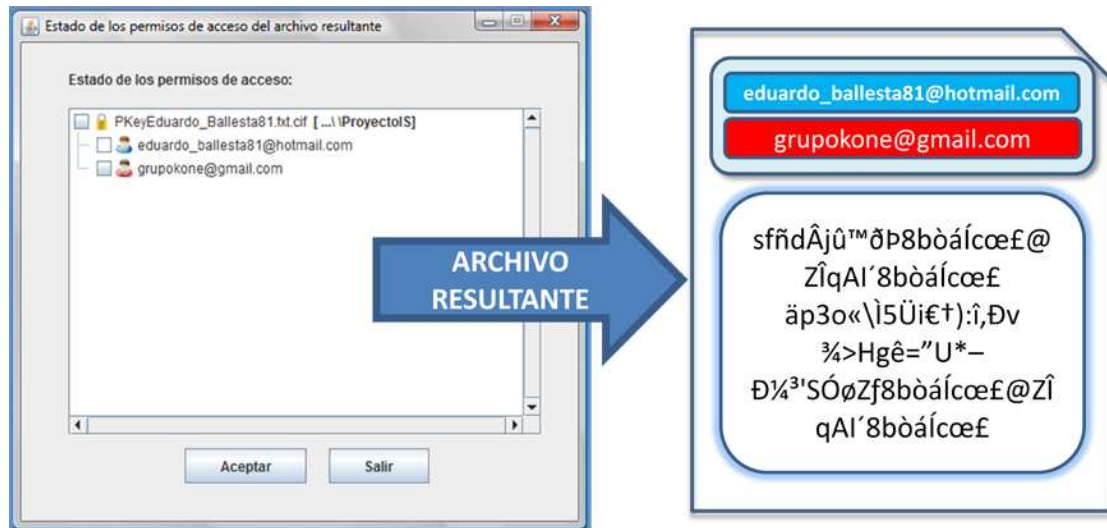


Figura 33: Estado del archivo tras el proceso de validación de peticiones de acceso de los usuarios.

Indicar que la herramienta va a necesitar de una estructura de datos donde almacenar las peticiones validadas para cada archivo para la operación de búsqueda de peticiones de acceso en un directorio.

Esta necesidad surge debido a que el modelo de datos organiza la información como muestra la **Figura 25**: cada usuario aparece con la lista de archivos donde el usuario tiene peticiones de acceso pendientes. Sin embargo sería más cómodo al contrario: cada archivo con la lista de usuarios que van a ser validados. Además, si se tuviera que leer y escribir un archivo tantas veces como peticiones validadas hubiera para ese archivo, el coste de procesamiento sería elevado.

Para ello la herramienta hace uso de una estructura de datos llamada **ListaUsuarioArchivo** que consta de dos campos:

- **Nombre del archivo:** nombre del archivo cifrado donde se va a procesar una petición de acceso.
- **Lista de usuarios:** lista con los nombres de todos los usuarios cuyas peticiones pendientes han sido validadas por el usuario de sesión para ese archivo.

En **Lista de Usuarios** se almacena la ruta del archivo donde el usuario de la sesión ha validado las peticiones de acceso y los usuarios a los que pertenecen esas peticiones validadas. De esta manera, sólo se hace una lectura y escritura de la cabecera por archivo.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.



Figura 34: Estado de una entrada de la ListaUsuarioArchivo después de haberse realizado una búsqueda.

4. Diseño e implementación de la herramienta KonEncriptación

En este apartado se van a describir detalladamente todas las funcionalidades diseñadas e integradas en KonEncriptación tales como el diseño del menú contextual de Dropbox, la agenda de usuario o la verificación de correspondencia de datos en KonEncriptación y *Dropbox*.

4.1. Diseño del menú contextual de Dropbox

El menú contextual de *Dropbox*, con el que se pueden realizar diferentes tipos de operaciones propias de esa herramienta, ha sido desarrollado e integrado en KonEncriptación para que los usuarios de la herramienta puedan hacer uso de él sin tener que recurrir a *Dropbox*.

Para el desarrollo e implementación de este menú ha sido necesario estudiar el patrón de las URLs que se generan en cada una de las operaciones permitidas con archivos y carpetas. Cabe indicar que el funcionamiento del menú en KonEncriptación es el mismo que el integrado en *Dropbox* salvo en algunos detalles que se describirán a lo largo de este apartado.

En los siguientes apartados se describen todos los detalles acerca de las distintas operaciones de este menú.

4.1.1. Ir al Navegador

Operación que permite a un usuario de *Dropbox* explorar un archivo o carpeta en el portal Web de *Dropbox* en la ubicación donde dicho archivo o carpeta se encuentra.

Existen dos patrones diferentes para generar una dirección web dependiendo de si lo que se quiere explorar es un archivo o un directorio.

Si lo que se desea **explorar es un archivo**, el portal web de *Dropbox* se abrirá por el directorio donde se encuentra dicho archivo y, la barra de opciones de este, estará desplegada como se muestra en la siguiente figura.

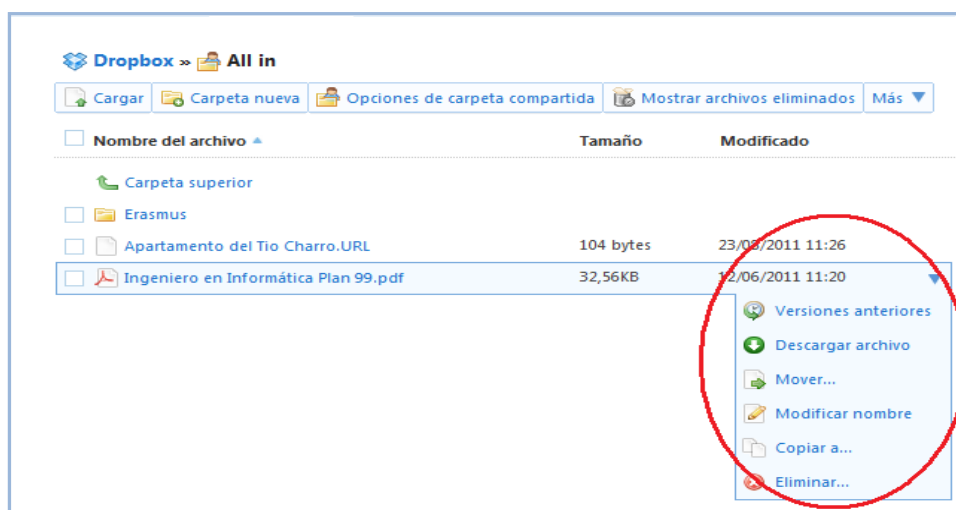


Figura 35: Opción ir al navegador de un archivo. Ventana de opciones del archivo expandida.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

El patrón para **explorar un archivo** en el portal web de Dropbox es:

<https://www.dropbox.com/homeDirectorio?select=Archivo#Directorio:::>

- **Archivo:** nombre del archivo que vamos a consultar formateado.
- **Directorio:** directorio donde se encuentra el archivo comenzado por el carácter /.

Ejemplo de dirección generada para visualizar un documento en *Dropbox* vía web:

<https://www.dropbox.com/home?select=metodo.txt>

En el caso de **visualizar el contenido de un directorio**, el patrón para visualizar dicho directorio en el portal Web de Dropbox es:

<https://www.dropbox.com/homeDirectorio#Directorio:::>

- **Directorio:** directorio que vamos a explorar.

Ejemplo de dirección generada para visualizar un directorio en *Dropbox* vía Web:

<https://www.dropbox.com/home/hola#/hola:::>

4.1.2. Crear enlace público

Operación con la que un usuario de *Dropbox* puede compartir cualquier archivo que se encuentre dentro del directorio *Public* o en *subdirectorios de éste* utilizando una dirección URL (*enlace público*) que es generada automáticamente por la aplicación. Si un usuario desea descargarse el archivo mediante el enlace público sólo tiene que introducirlo en el navegador y descargárselo (**ver menú usuario 5.8.2**).

Para esta operación existe un único patrón y es el siguiente:

http://dl.dropbox.com/u/Número_usuario/Ruta

- **Número usuario:** es el número que cada cuenta de usuario tiene asociado a *Dropbox*. Este número únicamente se puede obtener generando un *link público*.
- **Ruta:** ruta del archivo comenzando desde el directorio *Public*.

La creación de links o enlaces públicos puede realizarse desde la aplicación web de *Dropbox* o con la aplicación cliente de *Dropbox* pegándolo posteriormente en un archivo de texto para visualizarlo.

En la siguiente Figura se aprecia cómo se puede generar un enlace público desde la aplicación web. El rectángulo en rojo delimita el número de usuario que corresponde al usuario de la sesión y que es un elemento esencial para poder utilizar esta opción en KonEncriptación.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

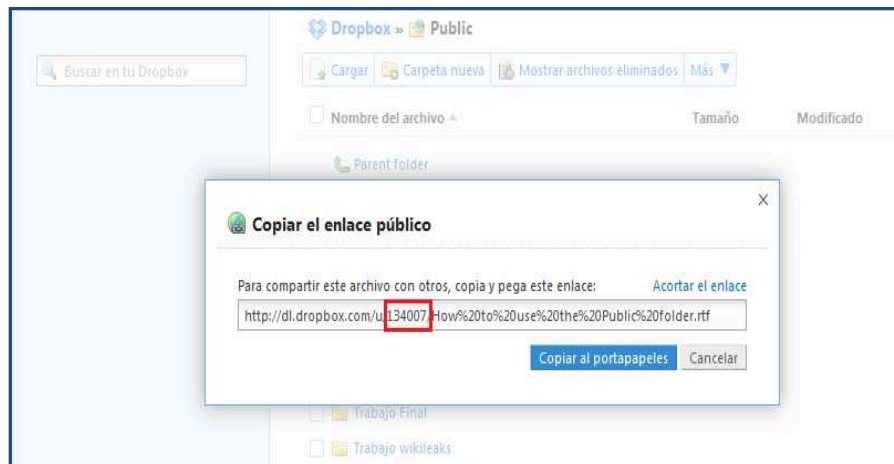


Figura 36: Cómo extraer el número de usuario desde la aplicación Web de Dropbox.

Ejemplo de URL de un enlace público:

<http://dl.dropbox.com/u/134007/Foto1.txt>

4.1.3. Ir a versiones anteriores

Esta opción permite al usuario de *Dropbox* visualizar y restaurar desde el portal Web de *Dropbox* alguna de las últimas modificaciones del archivo que esté consultando. Esta opción solo contempla las modificaciones de los últimos 30 días hasta la fecha y es sólo aplicable para archivos y no para directorios.

Existe únicamente un patrón para generar una URL para esta opción:

<https://www.dropbox.com/revisionsRuta>

- La primera parte es invariable y siempre es la misma.
- **Ruta:** ruta del archivo comenzando desde el siguiente directorio al home (sin incluir el directorio *Dropbox*). Cuando hay más de un nivel la ruta comienza con */*.

Ejemplo de URL para ir a versiones anteriores:

<https://www.dropbox.com/revisions/Photos/SampleAlbum/Boston.jpg>

4.1.4. Compartir esta carpeta

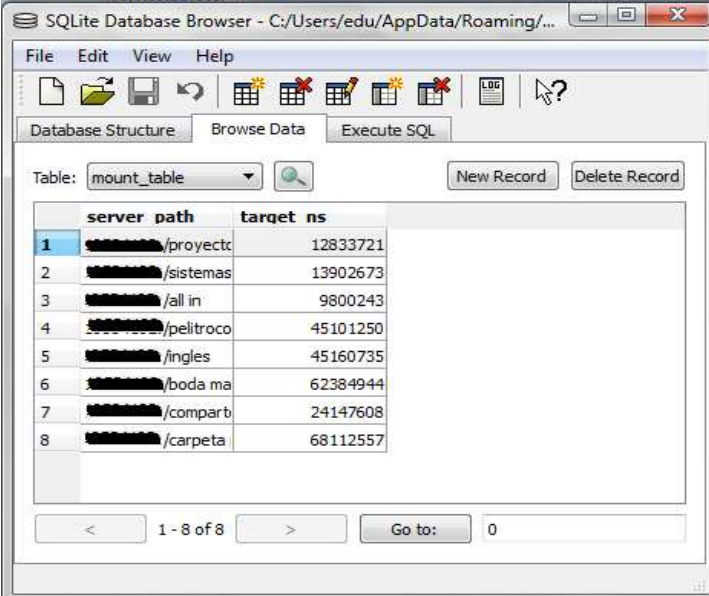
Opción donde un usuario de *Dropbox* puede compartir una carpeta con otros usuarios mediante el envío de invitaciones.

En esta opción existen varias restricciones importantes y que van a influir a la hora de generar la dirección URL correspondiente a la carpeta que se va a compartir. Estas restricciones son:

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Los directorios *Public* y *Photos* no pueden ser compartidos, pero si sus subdirectorios.
- El directorio *Dropbox* no puede ser compartido.
- Se puede compartir cualquier directorio siempre que un directorio a nivel superior o inferior no esté compartido.

KonEncriptación tendrá que hacer uso de la base de datos **FileConfig.db** de *Dropbox* donde vienen almacenados los nombres de las carpetas que están siendo compartidas actualmente por el usuario. En la siguiente Figura se puede ver la estructura de este archivo.



	server_path	target ns
1	[REDACTED]/proyecto	12833721
2	[REDACTED]/sistemas	13902673
3	[REDACTED]/all in	9800243
4	[REDACTED]/pelitroco	45101250
5	[REDACTED]/ingles	45160735
6	[REDACTED]/boda ma	62384944
7	[REDACTED]/compart	24147608
8	[REDACTED]/carpeta	68112557

Figura 37: Estructura de la Tabla *mount_table* de la base de datos *FileCache.db*

Los campos más importantes de esta base de datos son:

- **mount_table**: nombre de Tabla en *filecache.db* donde se encuentra el campo que almacena el nombre de las carpetas que están siendo compartidas.
- **server_path**: nombre de la carpeta compartida en Formato [*ID Usuario* (viene tachado por seguridad) / **Nombre de Directorio**]) como muestra la **Figura 37**.

Para esta opción existen dos patrones diferentes dependiendo de si el directorio es compartido o no.

El patrón para un **directorio compartido** es el siguiente:

<https://www.dropbox.com/home/Ruta?shareoptions=1#:::>

- **Ruta**: ruta del archivo comenzando desde el siguiente directorio al home (sin incluir el directorio *Dropbox*). Cuando hay más de un nivel de directorios con respecto al directorio home, se comienza con */*.

Ejemplo de URL para compartir directorio para una carpeta compartida:

<https://www.dropbox.com/home/Comparteme?shareoptions=1#::>

El patrón para un *directorio sin compartir* es:

<https://www.dropbox.com/Ruta?share=1#/Ruta::>

- **Ruta:** ruta del archivo comenzando desde el siguiente directorio al home (sin incluir el directorio *Dropbox*). Nunca comenzará por / porque ya va incluido en el patrón.

Ejemplo de URL para compartir directorio para una carpeta que no está compartida:

<https://www.dropbox.com/home/hola?share=1#/hola::>

Nota: el funcionamiento de esta opción en las versiones de KonEncriptación desarrolladas para la plataforma Linux no es totalmente estable debido a que *Dropbox* almacena las rutas de las carpetas compartidas en minúscula en la base de datos *FileConfig.db* y Linux, por ser un sistema Unix, es sensible al uso de mayúsculas y minúsculas a la hora de nombrar archivos y directorios.

4.1.5. Compartir galería de fotos

Dropbox permite compartir galerías de fotos, carpetas que se encuentran dentro del directorio *Photos*, mediante enlaces públicos de manera similar a la opción de compartir archivos vista en el apartado 4.1.2.

El patrón real de esta opción, pero no utilizado, sería el siguiente:

[https://www.dropbox.com/gallery/ Número usuario /1/Ruta?h=Resumen](https://www.dropbox.com/gallery/Número_usuario/1/Ruta?h=Resumen)

- **Número usuario:** número de usuario asociado a la cuenta de *Dropbox*. Este número se extrae generando un *link público para la galería*.
- **Ruta:** ruta del archivo comenzando desde el directorio *Photos*.
- **Resumen:** código generado por *Dropbox* para cada directorio compartido como galería.

Un link público para una galería puede ser generado, bien desde la aplicación Web de *Dropbox*, **Figura 38**, bien con la aplicación local de *Dropbox* y después pegándolo en un archivo de texto, pero siempre se debe estar dentro de un directorio o subdirectorio de *Photos*.

Actualmente, ***Dropbox* no ha hecho pública la función para generar el campo resumen de la URL** ni tampoco ninguna API con ningún tipo de función para generar dicha URL. Durante la realización del presente proyecto se han realizado pruebas para encontrar estimar función pero lo único determinado ha sido que el resumen obtenido para un directorio con el mismo nombre y la misma ubicación es diferente para dos usuarios distintos. Por esta razón, se cree que el código resumen generado está en función del nombre del directorio y del número de usuario. Esta misma función

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

para crear el resumen es también utilizada para generar un enlace público seguro desde el portal Web de Dropbox y tampoco ha podido ser contemplada en KonEncriptación.

Sin embargo, y para ofrecer una alternativa, se ha implementado la opción donde se genera una URL que abre el portal Web por la página donde aparece la URL generada para compartir la galería. Esta sigue el siguiente patrón:

<https://www.dropbox.com/Ruta>

- **Ruta:** ruta del archivo comenzando desde el directorio *Photos*.

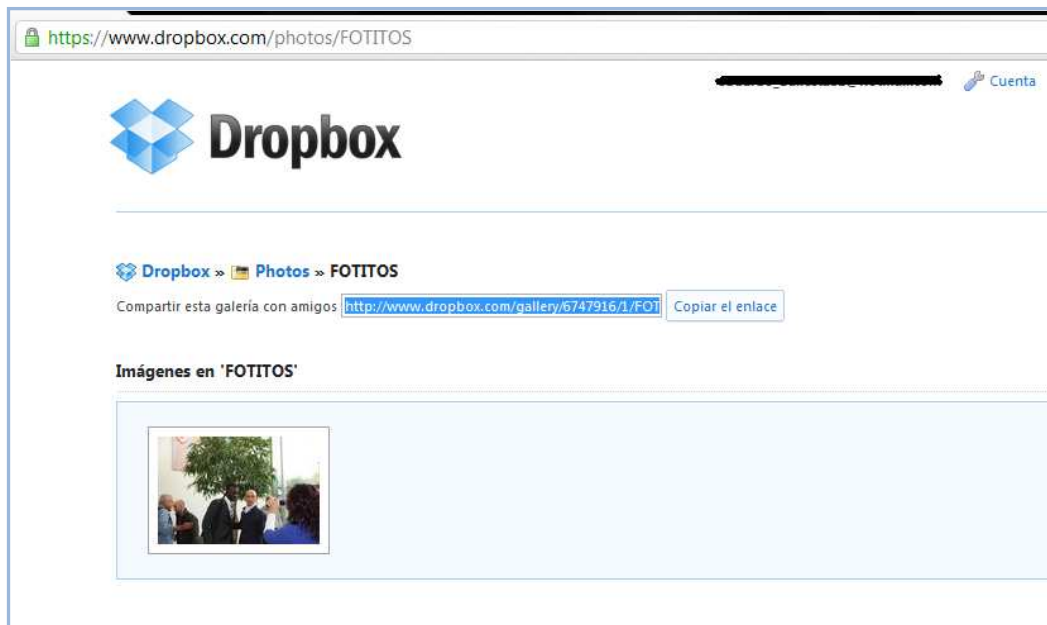


Figura 38: Forma de crear un enlace para la galería de fotos mediante el portal Web de Dropbox.

De esta manera, si un usuario desea compartir como galería, por ejemplo, la carpeta *FOTITOS* que se encuentra dentro del directorio *Photos*, la dirección generada sería la siguiente:

<https://www.dropbox.com/home/Photos/FOTITOS>

4.2. Concesión de permisos mediante la agenda de usuarios

Para añadir mayor funcionalidad a KonEncriptación y agilizar el proceso de asignación de permisos de acceso se ha integrado un sistema de agenda de usuarios donde se almacena localmente información útil sobre estos.

4.2.1. Estructura de una entrada de la agenda

Cuando un usuario envía una petición de acceso a un archivo cifrado, en ella envía información con la que se identifica y verifica a este usuario. Si esa información es almacenada localmente se podrá

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

utilizar posteriormente sin tener que esperar a que el usuario envíe en repetidas ocasiones otras peticiones de acceso para poder utilizarla. La información que contiene una entrada de la agenda es la siguiente:

- **Nombre del usuario:** login del usuario (**cuenta de correo electrónico**).
- **Alias:** nombre asociado al usuario para identificarlo de forma sencilla.
- **Clave pública:** del usuario y que se utilizará para cifrar la clave simétrica para ese usuario.
- **Lista de carpetas compartidas:** carpetas compartidas con las que el usuario está asociado.



Figura 39: Entrada de un usuario de la agenda.

La lista de carpetas compartidas, de la que son miembros algunos de los usuarios de la agenda, es utilizada para sugerirle al usuario de la sesión que estos usuarios deberían ser agregados como miembros del archivo cifrado si éste se encuentra dentro de alguna de esas carpetas compartidas (**ver apartado 4.2.3**).

Cada entrada de la agenda está asociada a un usuario y la información de la agenda de usuarios es almacenada en un archivo llamado **agenda.bin**.

Cabe indicar que pueden existir usuarios sin estar asociados a ninguna carpeta y que solamente podrán ser añadidos a la agenda cuando el usuario se encuentre en estado de petición, puesto que es el único momento donde el usuario envía su clave pública.

4.2.2. Mantenimiento de la Agenda de usuarios

El usuario es el encargado de ir insertando o eliminando a los usuarios de la agenda o de asociar o desasociar las carpetas compartidas con los mismos. La agenda de usuarios es leída al inicio de sesión, almacenada al final de la misma y validada cada cierto tiempo. El único proceso de mantenimiento que realiza KonEncriptación es el de ir eliminando las asociaciones de los usuarios con las carpetas compartidas cuando estas últimas dejan de serlo.

Las operaciones de mantenimiento que un usuario puede realizar son las siguientes:

- Añadir un usuario a la agenda.
- Eliminar usuario de la agenda.
- Editar el alias de un usuario.
- Quitarle el alias a un usuario.
- Asociar un usuario a una carpeta compartida.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Desasociar un usuario de una carpeta compartida.
- Buscar nuevos usuarios en carpetas compartidas.
- Agregar usuarios de la agenda a la cabecera de un archivo cifrado para ser validados.

Existen también operaciones de consulta de datos como:

- Ver las carpetas asociadas con los usuarios de la agenda.
- Ver los usuarios de la agenda.

La operación de búsqueda integrada es similar a la utilizada en el [apartado 3.4.3.2](#) y puede realizarse únicamente dentro de las carpetas compartidas.

4.2.3. Agregar usuarios desde la agenda a un archivo cifrado.

Como se indica al comienzo de este apartado, la agenda de usuarios es utilizada principalmente para validar usuarios directamente y que tengan así acceso a los archivos cifrados sin tener que esperar a que dichos usuarios tengan que enviar las peticiones de acceso previamente. Para que esto se pueda llevar a cabo, es necesario que dicha información esté almacenada anteriormente en la agenda de usuarios.

Se pueden agregar usuarios desde la agenda a la cabecera de un archivo cifrado en estado validado o con el fin de serlo mediante dos procesos diferentes:

- En los procesos de búsqueda de peticiones de acceso en archivos.
- De forma directa. Seleccionando un usuario de la agenda e insertándolo validado.

Según la ubicación del archivo cifrado sobre el que se esté trabajando, si se encuentra dentro de una carpeta compartida o fuera de ella, la información se representará de la siguiente manera.

- **Sugerencias:** indica que los usuarios no están aún validados en el archivo cifrado consultado y que dicho archivo se encuentra dentro de la carpeta compartida donde son miembros estos usuarios.
- **Otros usuarios:** son el resto de usuarios que no están asociados a la carpeta compartida donde se encuentra el archivo. Si la carpeta no está compartida son todos los usuarios dados de alta en la agenda y que no están validados en ese archivo cifrado.

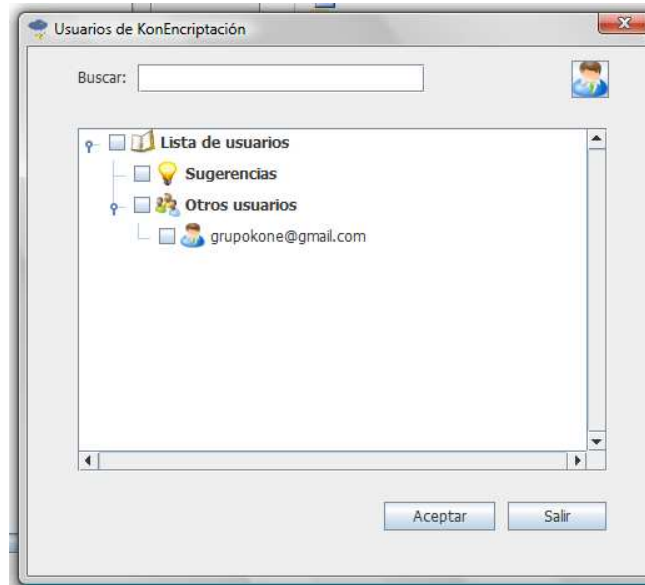


Figura 40: Ventana de KonEncriptación para agregar usuarios a los archivos cifrados desde la agenda de usuarios.

4.3. Verificación de la correcta correspondencia entre Dropbox y KonEncriptación

KonEncriptación necesita verificar, al inicio y durante la ejecución de la sesión, que las cuentas de usuario asociadas a *Dropbox* y a KonEncriptación son las mismas. Además, KonEncriptación debe asegurar también, en todo momento, que los directorios local y remoto existen y que el directorio asociado a la cuenta de Dropbox coincide con el directorio remoto de KonEncriptación. Como se vio en el apartado 3.3.1, KonEncriptación trabaja con dos archivos de configuración que le permiten realizar estas acciones, asegurando así el buen funcionamiento de la aplicación. Estos archivos son: el archivo *config.db* de *Dropbox* y el archivo *FileConfig.bin* de KonEncriptación.

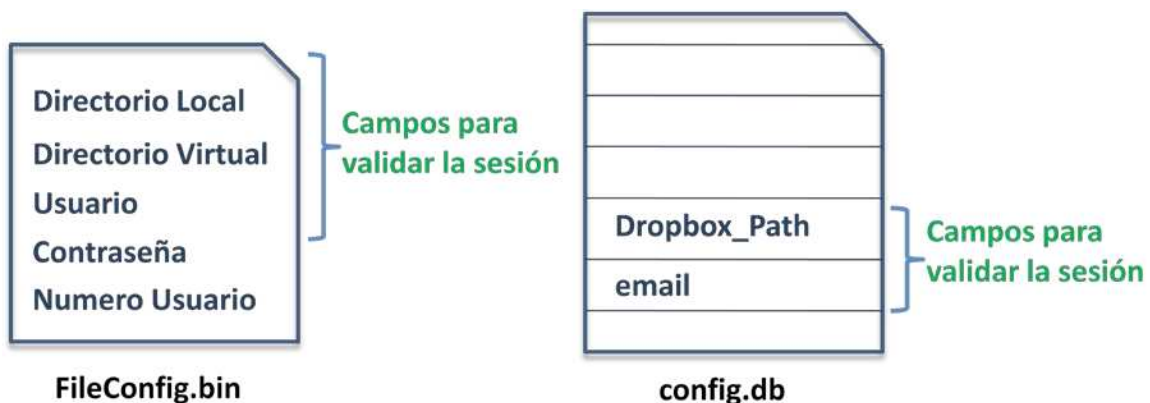


Figura 41: Archivos de configuración de las herramientas KonEncriptación y Dropbox

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Como se puede ver en la **Figura 41**, los campos utilizados por KonEncriptación para verificar una correcta integración son: *Directorio Local*, *Directorio Virtual* y *Usuario* en el archivo **FileConfig.bin** y los campos *Dropbox_Path* y *email* en la base de datos **config.db** de *Dropbox*.

En los siguientes apartados se explicará detalladamente cómo consigue KonEncriptación lograr dicho objetivo utilizando estos campos.

4.3.1. Cambio de usuario asociado a Dropbox

Puede suceder que mientras **KonEncriptación no esté ejecutándose** un nuevo usuario asocie su cuenta a la instancia de *Dropbox* instalada en el equipo, desligando así de la cuenta de *Dropbox* al usuario que había anteriormente. Si el anterior usuario había hecho uso de KonEncriptación, sus datos estarán almacenados en el archivo de configuración de este. De esta manera, si este nuevo usuario quisiera hacer uso de KonEncriptación, al iniciarse la herramienta le indicaría a este usuario que se tiene que registrar, puesto que el login asociado a la cuenta de *Dropbox* y el login del usuario asociado a KonEncriptación no coinciden.

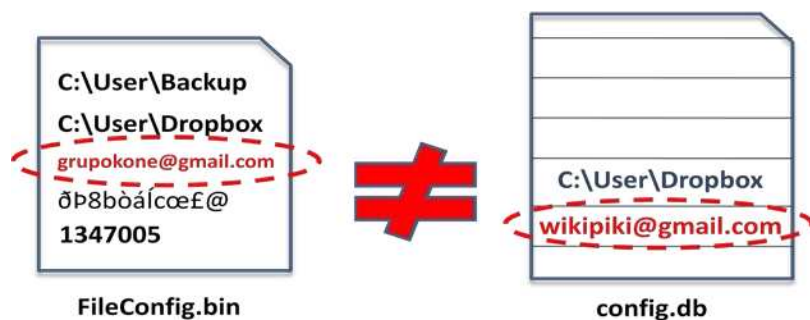


Figura 42: Inicio de sesión de KonEncriptación con usuarios diferentes en ambas cuentas.

Por otra parte, es posible también que mientras **KonEncriptación se esté ejecutando** un nuevo usuario asocie su cuenta a la instancia de *Dropbox* instalada en el equipo, desligando así de la cuenta de *Dropbox* al usuario anterior. Puesto que la sesión del anterior usuario se encuentra abierta, el nuevo usuario tendría la oportunidad de poder descifrar los archivos de éste aprovechando esta circunstancia. Para evitar este tipo de situaciones se ha utilizado un **timer (cronómetro)** para comprobar que los directorios asociados a ambas cuentas coinciden. Si el cambio fuera detectado por la aplicación, la aplicación se cerraría inmediatamente. La frecuencia de comprobación es de una vez por segundo.



Figura 43: Supervisión de cambio de usuario

4.3.2. Comprobación de los directorios local y remoto

De forma similar al apartado anterior, KonEncriptación verifica los directorios local y remoto asociados a la aplicación para asegurar su correcto funcionamiento. Esta comprobación se realiza tanto al inicio como durante la ejecución de la aplicación.

Puede ocurrir que durante el tiempo que **mientras KonEncriptación no se ejecuta** el usuario de *Dropbox* cambie la ubicación del directorio asociado a esa herramienta. KonEncriptación detectará esta circunstancia al iniciarse, avisará al usuario de que el directorio ha cambiado con respecto a la última sesión y almacenará *automáticamente* la nueva ubicación en el campo directorio Virtual en el archivo de configuración **FileConfig.bin**.

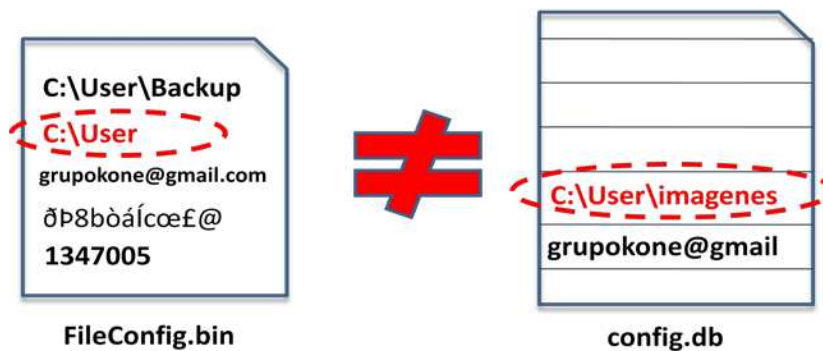


Figura 44: Inicio de sesión de KonEncriptación con rutas a directorios de Dropbox diferentes.

Además de esto, KonEncriptación también comprueba al iniciarse si los directorios local y remoto (*directorio asociado a Dropbox*) existen. En caso de que el **directorio local no exista**, se le exigirá al usuario que va a iniciar la sesión que seleccione un nuevo directorio local y la nueva ruta será almacenada en el campo *directorio local* en el archivo de configuración (**FileConfig.bin**). Ver apartado del manual de usuario 5.4.1.4.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

En caso de que sea el directorio asociado a la cuenta de *Dropbox*, **directorio remoto**, el que **no exista**, hasta que el usuario no escoja otra ubicación en *Dropbox* no se podrá iniciar ninguna sesión en KonEncriptación.

Es importante indicar que en ninguna de las dos opciones descritas anteriormente KonEncriptación permitirá que estos dos directorios estén contenidos uno dentro del otro en el ordenador del usuario.

Por otra parte, debido a que los directorios local y remoto pueden ser editados desde el explorador de archivos del sistema operativo (Windows o Linux) con el que se esté trabajando mientras **KonEncriptación está ejecutándose**, la herramienta debe estar continuamente comprobando que dichos directorios existen. Para asegurar esto y que no pueda generarse un mal funcionamiento en la herramienta se utiliza también un **timer (cronómetro)**, como el apartado anterior, para comprobar cada segundo que estos directorios existen. En caso de que alguno de los directorios sea eliminado o renombrado externamente, la aplicación se cerrará inmediatamente.



Figura 45: Estrategia basada en timer para comprobar si los directorios local y remoto existen.

4.4. Consideraciones sobre la edición, eliminación y renombrado de archivos y directorios

KonEncriptación, para asegurar el buen funcionamiento de la aplicación y cumplir con las pautas definidas sobre confianza transitiva en el [apartado 2.3.3](#), lleva a cabo una serie de consideraciones acerca de la edición, eliminación y renombrado de archivos y directorios que se describen en los siguientes párrafos.

En primer lugar, KonEncriptación **no permite a los usuarios de la sesión eliminar o renombrar los directorios local y remoto** para evitar así que se produzca cualquier tipo de problema de funcionamiento.

Tampoco **permite a ningún usuario que no tenga permiso de acceso a un archivo cifrado realizar las operaciones:**

- Eliminar.
- Renombrar.
- Descifrar.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Pegar.

De esta manera se pueden cumplir las pautas de confianza transitiva descritas en el **apartado 2.3.3**.

Por último, KonEncriptación **no permite a ningún usuario realizar ningún tipo de operación sobre un archivo cifrado mientras está siendo sincronizado y el tamaño de éste sea de 0 bytes**. Algunas veces, mientras *Dropbox* sincroniza un archivo creado por otro usuario miembro genera un archivo de 0 bytes en la carpeta compartida de los usuarios de esta y no cambia el tamaño hasta que se sincroniza el archivo completamente. Esto puede conllevar a un mal funcionamiento de la herramienta y a un mal uso por parte del usuario de la misma puesto que KonEncriptación necesita leer la cabecera del archivo cifrado para saber en qué estado de acceso se encuentra el usuario de la sesión y, conociendo este estado, establecer el icono que le indica al usuario dicha información. Para evitar esta situación la herramienta nunca leerá la cabecera de los archivos cifrados cuyo tamaño sea menor a 400 bytes que es aproximadamente el menor tamaño posible de una entrada de la cabecera. Para evitar que el usuario de sesión pueda consultar erróneamente el estado de las peticiones de dicho archivo mientras está siendo sincronizado, las opciones relacionadas con estas estarán deshabilitadas. También, el icono de la **Figura 46** será utilizado para indicar al usuario de la sesión que el archivo cifrado está siendo sincronizado y no puede tener acceso a él hasta que no cambie éste.



Figura 46: Icono de un archivo cifrado en estado de sincronización.

4.5. Uso de threads en la ejecución de operaciones.

Para evitar secuencialidad en la ejecución de diferentes operaciones y permitir así paralelismo en la ejecución de las mismas, todos los métodos asociados a las operaciones que permite realizar KonEncriptación se han implementado como threads. Esto permite al usuario seguir trabajando con la aplicación durante la realización de las tareas iniciadas.

4.6. Uso de Daemons

KonEncriptación utiliza daemons para supervisar los cambios que se producen en los directorios local y remoto por ediciones externas. De esta manera, KonEncriptación puede mantener la información presentada en los dos árboles de directorios (local y remoto) actualizada y en concordancia con la información que hay en cada momento en dichos directorios.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Para poder implementar estos daemons se ha hecho uso de la librería **JNotify**, descrita en el apartado 4.8.2. Gracias a ella KonEncriptación puede controlar las ediciones que se producen en el directorio o subdirectorios de este, ya sean realizadas por la aplicación o por edición externa a la aplicación. Las ediciones detectadas por este daemon son:

- Eliminación de archivos y directorios.
- Renombrado de archivos y directorios.
- Creación de nuevos archivos y directorios.

Cada vez que alguna de estas ediciones suceda en el directorio supervisado o en sus subdirectorios, el propio daemon llamará al método adecuado para que se encargue de la actualización de la información del árbol de archivos local o remoto de KonEncriptación según corresponda.



Figura 47: Funcionamiento de la supervisión de directorios de un Daemon

Los daemons utilizados por la herramienta son para:

- Supervisión del directorio local.
- Supervisión del directorio remoto.

4.7. Idiomas en KonEncriptación

Se ha dotado a KonEncriptación con la posibilidad de ser utilizado tanto en *español* como en *inglés*. Partiendo de la base de que el lenguaje seleccionado para la instalación de KonEncriptación va a ser el mismo que el utilizado por el usuario que va a hacer uso de la aplicación, se ha utilizado la siguiente técnica para que el idioma seleccionado durante el proceso de instalación y el de KonEncriptación coincidan.

Todos los idiomas para las herramientas de desarrollo de instaladores de software tienen asociados un valor numérico estándar en base hexadecimal y decimal. En el caso de KonEncriptación dichos valores son:

- **1033:** inglés.

- **3082:** español.

Así pues, cuando se instala KonEncriptación se generará un directorio “Idioma” que contendrá un archivo, sin extensión, con alguno de estos dos valores según haya sido el idioma seleccionado durante el proceso de instalación. Si por alguna razón estos valores no existen la herramienta tomará por defecto el idioma español y generará un archivo con el valor correspondiente, **3082**. Además, puesto que el usuario tendrá la oportunidad de cambiar el idioma en KonEncriptación, la herramienta se encargará de gestionar el valor del idioma en el archivo.

4.8. Implementación

En este apartado se describen brevemente las principales clases implementadas así como todas las APIs externas utilizadas para el desarrollo de KonEncriptación. Para más información el lector puede recurrir al código de la aplicación adjunto en este Proyecto Final de Carrera.

4.8.1. Clases

En este apartado se describen las clases que se han implementado para desarrollar KonEncriptación. Estas clases son las siguientes:

Cabecera.java

Es la clase encargada de la gestión de las cabeceras almacenadas en los archivos cifrados y que contiene los permisos de acceso de los usuarios a dicho archivos. En ella se integran principalmente métodos que se encargan de:

- Lectura de la cabecera con los permisos de acceso del archivo cifrado.
- Escritura en el archivo cifrado de las cabeceras con los permisos de acceso.
- Gestión de peticiones de acceso.
 - Añadir una nueva petición de acceso.
 - Eliminar una petición de acceso.
 - Aceptar una petición de acceso.
 - Búsquedas de usuarios en las cabeceras.
 - Validaciones de acceso de usuarios.

Cifrado.java

Clase que realiza todas las operaciones relacionadas con el cifrado y descifrado de información, así como la generación y manejo de claves simétricas y asimétricas.

Los principales métodos desarrollados en esta clase se encargan de:

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Cifrado y descifrado de archivos.
- Crear la pareja de claves pública – privada.
- Crear la clave simétrica para cifrar un archivo.
- Envoltura y desenvoltura de clave simétrica (**ver apartado 3.1.4**).
- Cifrar y descifrar la contraseña almacenada en el archivo de configuración de la herramienta.

ControlArchivosTemporales.java

Se encarga de eliminar los archivos descifrados que han sido abiertos por el usuario para consultar su contenido y que han sido guardados en la carpeta Temporal dentro del directorio usuario.

DaemonDirectorios.java

Clase en la que se crea un demonio que se encarga de escuchar todos los eventos de edición que suceden dentro del directorio local o remoto. Dichos eventos de edición son: creación, modificación, eliminación o renombrar de directorios y archivos dentro del directorio que vigila. Los eventos son configurables. **Ver ejemplo JNOTIFY en el apartado 4.8.2.**

Esta clase está ligada directamente a la clase ListenerCambios.java que es la que indica cuándo se produce alguno de los eventos anteriores.

DragAndDrop.java

Es la clase encargada de controlar la acción de arrastrar y soltar. Además, se controlan las posibles operaciones que se pueden realizar dependiendo de:

- Los tipos de archivos que se están arrastrando.
- El inicio y fin de la operación de arrastre.

Dropbox.java

Es una clase desarrollada principalmente para:

- Extraer los parámetros necesarios de los archivos de configuración de *Dropbox*: nombre de usuario, ruta del directorio de *Dropbox* o qué carpetas son compartidas, para asegurar, mediante la validación de estos, el buen funcionamiento de la herramienta KonEncriptación.
- Integrar las operaciones del menú contextual de *Dropbox* en la herramienta (**ver apartado 4.1**).

En esta clase trabaja con los archivos de *Dropbox*: **config.db y filecache.db (ver apartado 3.1.1)**.

Portapapeles.java

Clase encargada de enviar o extraer los archivos y/o directorios del portapapeles del sistema. Además, se encarga de enviar al portapapeles del sistema los links públicos generados por la aplicación en la opción crear enlace público (**ver apartado 4.1.2**).

ListenerCambios.java

Es una clase que avisa de los eventos que se producen en el directorio que está siendo escuchado por el daemon creado en la clase **DaemonDirectorios.java**. Cada vez que la clase notifica una edición de un archivo (crear, renombrar o eliminar), valida en cuál de los directorios (local o remoto) se ha producido y llama al evento indicado para que se encargue de actualizar en tiempo real los directorios local y remoto que aparecen en la ventana principal de la aplicación.

ListinUsuarios.java

Se trata de una clase donde se gestiona totalmente la agenda de usuarios y donde se integran métodos que principalmente realizan:

- Búsqueda de usuarios.
- Búsqueda de carpetas compartidas.
- Insertar usuarios a la agenda.
- Eliminar usuarios de la agenda.
- Asociar usuarios con la agenda a carpetas compartidas.
- Desasociar usuarios de la agenda a carpetas compartidas.
- Insertar o eliminar alias.
- Validar usuarios.

OperacionesArchivosyDirectorios.java

En esta clase se desarrollan todas las operaciones relacionadas con la edición de archivos y directorios. Los métodos que se implementan realizan principalmente las siguientes operaciones:

- Opciones de Edición.
 - Crear un archivo o directorio.
 - Eliminar un archivo o directorio.
 - Renombrar un archivo o directorio.
- Abrir archivos con herramientas externas.
- Tratamiento de rutas de archivos.
- Extraer el icono según el tipo de archivo.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Validar archivos y directorios para asegurar la correcta realización de las operaciones que ofrece la herramienta.
- Extraer parámetros informativos como fecha, tamaño o extensión de un archivo.

Las clases **TreeRendered.java**, **AbstractTreeModel.java** y **FileSystemModel.java** se encargan principalmente de:

- Apariencia de los árboles (directorio local y remoto).
- Gestión de modelo de datos con el que se cargan los datos en los árboles.
- Actualización de los datos presentados en pantalla.

4.8.2. APIS externas utilizadas

En este apartado se describen brevemente las principales características y funcionalidades de las APIs externas al proyecto utilizadas.

JNotify

Se trata de una librería open source que permite a un desarrollador de aplicaciones java establecer un evento listener que se encargue de escuchar un directorio o archivo y avise a una clase principal de los eventos que suceden en ese directorio o archivo. Dichos eventos son los siguientes:

- Crear un fichero (**File created**).
- Modificar un fichero (**File modified**).
- Renombrar un fichero (**File renamed**).
- Eliminar un fichero (**File deleted**).
- Todos los anteriores (**File any**).

Cualquiera de estos eventos puede ser elegido selectivamente por el desarrollador del software. Una forma sencilla de escogerlos todos es mediante la opción de seleccionar todos (**File any**).

Cada vez que alguno de los eventos indicados suceda el método asociado a él se disparará y se llevarán a cabo las acciones preestablecidas por el desarrollador.

Su página web ofrece un ejemplo de uso donde podemos ver las variables y métodos que ofrece esta Librería.

```
public void sample() throws Exception {
    // Directorio o Archivo que se va a escuchar
    String path = System.getProperty("user.home");

    // Mascara de escucha. Especificamos los eventos que queremos escuchar
    // or JNotify.FILE_ANY si escogemos todos los eventos.
    int mask = JNotify.FILE_CREATED |
              JNotify.FILE_DELETED |
              JNotify.FILE_MODIFIED |
```

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

```
        JNotify.FILE_RENAMED;

// Si queremos escuchar también los subdirectorios
boolean watchSubtree = true;

// LLamamos al metodo de escucha
int watchID = JNotify.addWatch(path, mask, watchSubtree, new Listener());

// sleep a little, the application will exit if you
// don't (watching is asynchronous), depending on your
// application, this may not be required
Thread.sleep(1000000);

// Eliminar el listener
boolean res = JNotify.removeWatch(watchID);
if (!res)
{
    // invalid watch ID specified.
}
}

//Clase con los métodos que se dispararán cuando suceda alguno de los
//eventos
class Listener implements JNotifyListener
{
    //Cuando renombramos un fichero dentro del directorio que escuchamos
    public void fileRenamed(int wd, String rootPath, String oldName,
        String newName) {
        print("renamed " + rootPath + " : " + oldName + " -> " + newName);
    }

    //Cuando modicamos un fichero dentro del directorio que escuchamos
    public void fileModified(int wd, String rootPath, String name)
    {
        print("modified " + rootPath + " : " + name);
    }

    //Cuando eliminamos un fichero dentro del directorio que escuchamos
    public void fileDeleted(int wd, String rootPath, String name) {
        print("deleted " + rootPath + " : " + name);
    }

    //Cuando creamos un fichero dentro del directorio que escuchamos
    public void fileCreated(int wd, String rootPath, String name) {
        print("created " + rootPath + " : " + name);
    }

    //Metodo para mostra el texto por pantalla
    void print(String msg) {
        System.err.println(msg);
    }
}
}
```

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Para compilar una aplicación donde se usa JNotify hay que enlazar de manera manual la librería externa estableciendo la ruta donde se encuentra el .jar.

```
java -Djava.library.path=. -jar jnotify-VER.jar [dir]
```

Debido a que la ruta donde se encuentra la librería JNotify, y por tanto su .jar va a estar siempre dentro del directorio donde se instala KonEcriptación, la forma de enlazar la ruta de ejecución de Jnotify se realiza de forma manual mediante el siguiente método.

```
public static void EnlazarPathLibreria()
{
    if (System.getProperty("suppress-natives-injection", null) == null)
    {
        try
        {
            Field sys_paths = ClassLoader.class.getDeclaredField("sys_paths");
            sys_paths.setAccessible(true);
            sys_paths.set(ClassLoader.class, null);
            String path = "..\\jnotify-lib-0.93\\";
            System.setProperty("java.library.path", path);
        }
        catch (Exception e)
        {
            e.printStackTrace();
            System.exit(1);
        }
    }
}
```

Debido a que esta clase tiene que estar ejecutándose en paralelo, la clase Jnotify ha sido embebida en otra clase superior que hereda de la interfaz thread.

Por último indicar, que esta librería soporta Windows 2000 y posteriores, Linux y Mac.

Web Oficial: <http://jnotify.sourceforge.net/>

Sqlitejdbc.jar

Es una librería opensource que implementa un motor de base de datos SQL transaccional autónomo, sin servidor y sin ninguna configuración. SQLite es el más extenso motor de bases de datos SQL en el mundo.

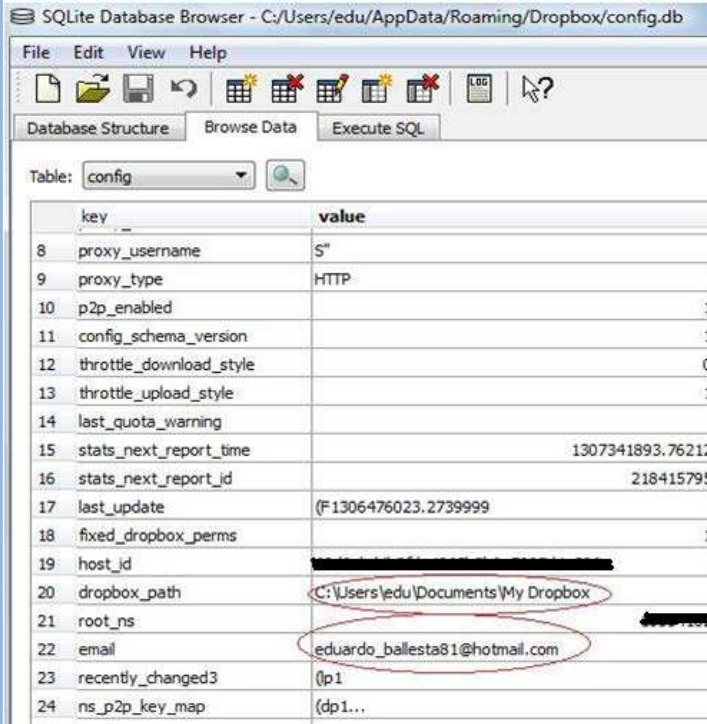
Algunas de sus funciones principales son:

- Las transacciones son automáticas, consistentes, aisladas y permanentes
- No necesita ninguna configuración.
- Implementa la mayoría de los estándares SQL92.
- Soporta bases de datos de terabytes y cadenas de GB.
- Más rápida que los motores de base de datos cliente / servidor para la mayoría de las operaciones comunes.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Debido a que *Dropbox* utiliza una base de datos SQLite para almacenar los parámetros de configuración tales como la cuenta usuario asociada a *Dropbox* o el directorio remoto a esta cuenta que se va a sincronizar con el servidor de *Dropbox*, se ha tenido que hacer uso de esta librería para tener acceso a dicha información.

En la siguiente Figura se muestra algunos de los campos que almacena el archivo de configuración de *Dropbox*.



key	value
8 proxy_username	S"
9 proxy_type	HTTP
10 p2p_enabled	1
11 config_schema_version	1
12 throttle_download_style	0
13 throttle_upload_style	1
14 last_quota_warning	
15 stats_next_report_time	1307341893.76212
16 stats_next_report_id	218415795
17 last_update	(F1306476023.2739999
18 fixed_dropbox_perms	1
19 host_id	[REDACTED]
20 dropbox_path	C:\Users\edu\Documents\My Dropbox
21 root_ns	[REDACTED]
22 email	eduardo_ballesta81@hotmail.com
23 recently_changed3	{p1
24 ns_p2p_key_map	{dp1...

Figura 48: Campos de la archivo de configuración de *Dropbox*.

Para leer estos datos se ha desarrollado un método para obtener los siguientes campos:

- Dropbox_path
- Email

```
import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.sql.Statement;

public static void LeerArchivoConFiguracionDropBox(String Ruta) throws
ClassNotFoundException, SQLException
{
    Class.forName("org.sqlite.JDBC");
    Connection conn = DriverManager.getConnection("jdbc:sqlite:"+Ruta);
    Statement stat = conn.createStatement();
    ResultSet rs = stat.executeQuery("select * from config;");
```

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

```
int i = 0;
while (rs.next())
{
    if((i == 20) || (i== 18))
    {
        //Extraer los datos para validar cuenta
        //Extraer los datos para enlazar el Directorio
    }
    i++;
}
rs.close();
conn.close();
}
```

Web oficial: <http://www.sqlite.org/>

5. Manual de usuario

En este apartado se van a describir todas las características, operaciones y funcionalidades de KonEncriptación desde el punto de vista del usuario.

5.1. Requisitos

Para poder hacer uso de KonEncriptación es necesario tener instalada la versión de Java 1.6 JDK para Windows versión 32 bits o la versión 1.7 JDK en Windows versión 64 bits.

Además, es también imprescindible que Dropbox esté instalado en el equipo. En caso contrario KonEncriptación no funcionará. Las versiones de Dropbox utilizadas en este proyecto han sido la 1.1.45 en Windows y la 1.1.35 en Linux.

KonEncriptación hace uso de varios archivos de configuración de Dropbox. Futuros cambios en dichos archivos por parte del equipo de desarrolladores de Dropbox podrían resultar en un mal funcionamiento, o no funcionamiento, de KonEncriptación.

5.2. Instalación

La herramienta soporta distintos sistemas operativos. En plataformas Windows puede ser instalado para XP, Vista o 7. En plataformas Linux ha sido testeado en Kubuntu.

El primer paso para instalar KonEncriptación en Windows es ejecutar el archivo de instalación *setup.exe*.

Una vez iniciada la instalación aparecerá una ventana de selección del idioma con el que se realizará el proceso de instalación. El usuario deberá elegir entre los idiomas ofrecidos: español e inglés.



Figura 49: *Ventana de selección de idioma del proceso de instalación.*

Una vez escogido el idioma aparecerá una ventana de bienvenida para el asistente de instalación. El usuario deberá escoger la opción siguiente para poder continuar con la instalación de KonEncriptación. Por el contrario, si el usuario no desea continuar con la instalación de

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

KonEncriptación, deberá pulsar la opción cancelar. Cabe indicar también que el idioma seleccionado en el proceso de instalación será el mismo que el que aparezca por defecto en KonEncriptación. Es decir, si en el proceso de instalación se selecciona como idioma el inglés, el idioma de KonEncriptación será el mismo.

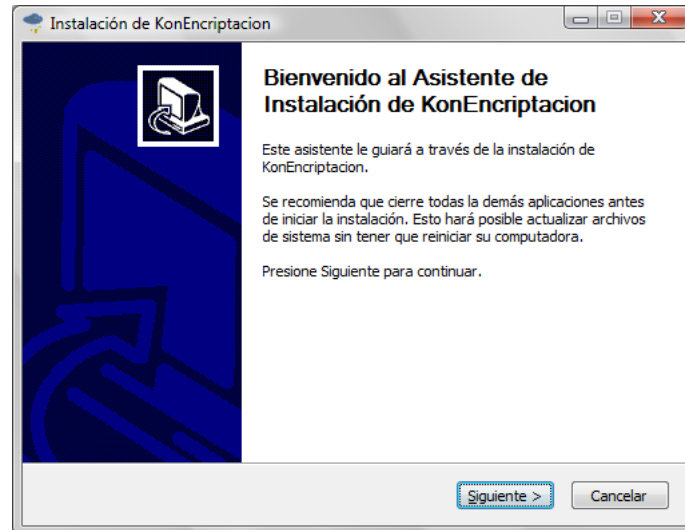


Figura 50: Ventana de bienvenida al asistente de instalación de KonEncriptación.

Si el usuario pulsa el botón siguiente, la siguiente ventana que aparecerá será la de selección del directorio destino donde se instalará KonEncriptación. La ruta que aparece por defecto es *Unidad:\Archivos de programa\KonEncriptación*, pero el usuario podrá seleccionar el directorio que desee mediante la opción examinar.

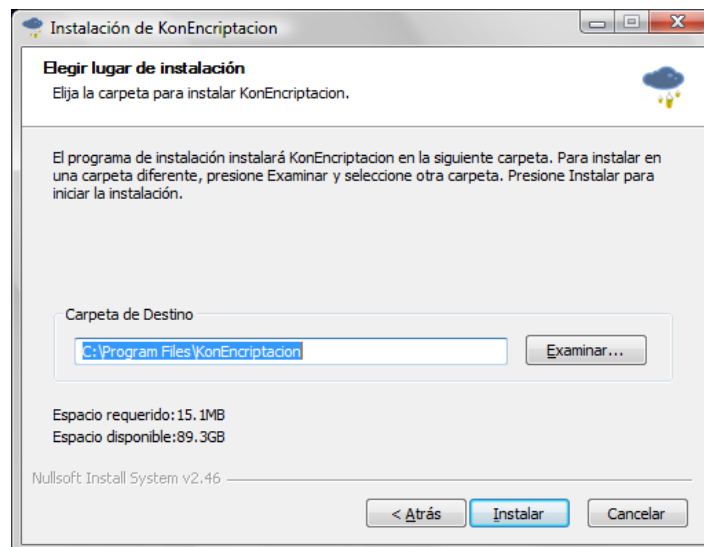


Figura 51: Ventana de selección de carpeta destino donde instalar KonEncriptación

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Una vez escogido el directorio destino, el usuario deberá seleccionar la *opción instalar* para que la KonEncriptación puede ser instalado en la ubicación escogida. Si el usuario pulsa esta opción, KonEncriptación se instalará en dicho directorio.

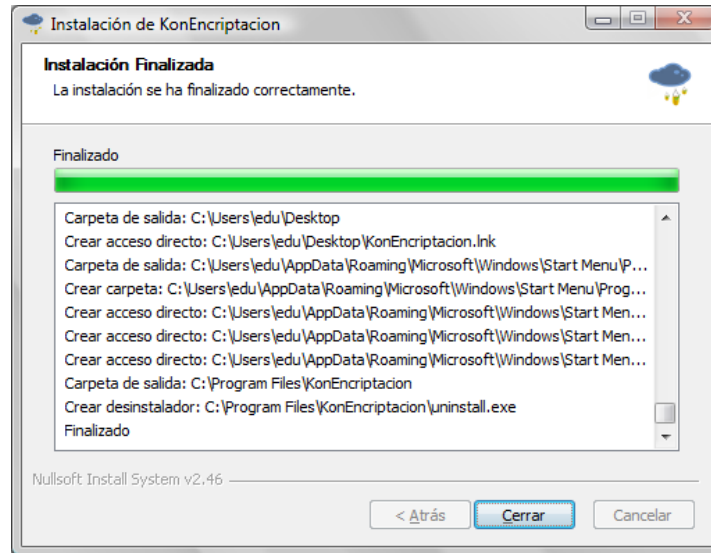


Figura 52: Ventana de instalación de KonEncriptación en el directorio destino seleccionado.

Una vez instalada la aplicación en el directorio se abrirá una ventana indicándole al usuario que el proceso de instalación de KonEncriptación en el equipo ha finalizado. En este último paso y antes de cerrarse el asistente de instalación, el usuario tendrá la opción de ejecutar la aplicación por primera vez y/o leer el archivo Leeme.txt donde se indican las características de la aplicación.

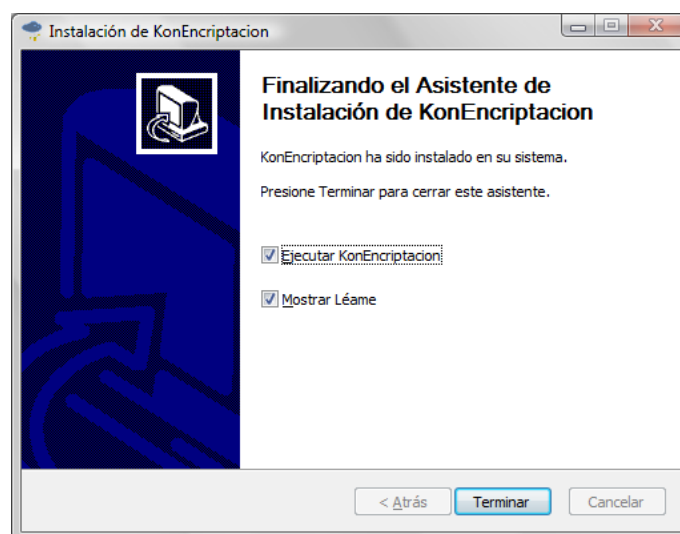


Figura 53: Ventana de finalización de instalación de KonEncriptación.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Durante el proceso de instalación se crean un acceso directo a KonEncriptación en el escritorio



y una entrada en el menú inicio de KonEncriptación como muestra la siguiente Figura.

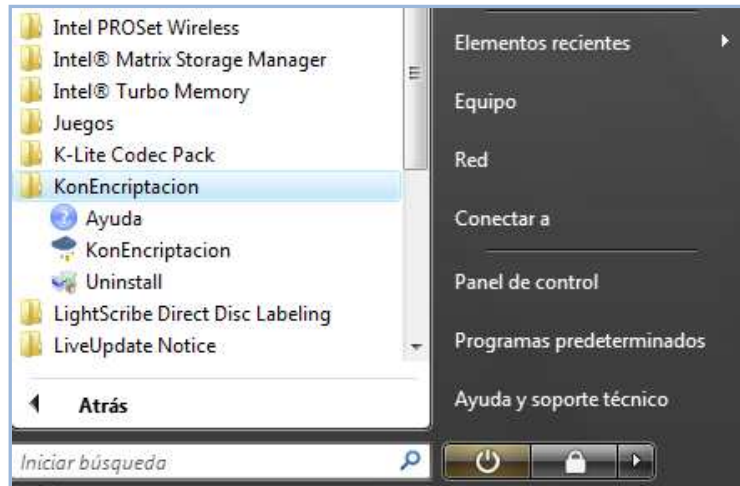


Figura 54: Entrada de KonEncriptación generada por el instalador en el menú inicio.

5.3. Registro en la aplicación

Cuando se ejecuta por primera vez KonEncriptación o cuando se inicia una sesión y el usuario asociado a la cuenta de *Dropbox* ha cambiado (**ver apartado 5.4.1.1**) se le exigirá al nuevo usuario que se registre en KonEncriptación para poder hacer uso de la herramienta. En caso de no hacerlo, el usuario no podrá tener acceso a KonEncriptación.

En cualquiera de los dos casos mencionados en el párrafo anterior, después del aviso pertinente, una ventana con un mensaje de bienvenida aparecerá indicándole al nuevo usuario cuál es la cuenta de usuario (*correo electrónico*) que está asociada en ese momento a *Dropbox*. En ese instante comenzará el proceso de registro en KonEncriptación para este nuevo usuario.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.



Figura 55: Inicio de registro de un usuario.

Cuando el usuario **pulse el botón siguiente** pasará al paso 1: *ventana de selección del directorio local*. En esta ventana, el usuario tendrá que seleccionar el directorio local donde desea trabajar de forma segura. La siguiente Figura muestra la apariencia de la *ventana de selección del directorio local*.



Figura 56: Paso 1 del registro de usuarios. Ventana de selección del directorio local.

Para seleccionar el directorio local el usuario dispone de dos posibilidades:

- Pulsar el botón de exploración (*icono con una casa*) y seleccionar el directorio deseado desde el explorador de archivos que aparecerá.
- Introducir manualmente la ruta del directorio.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

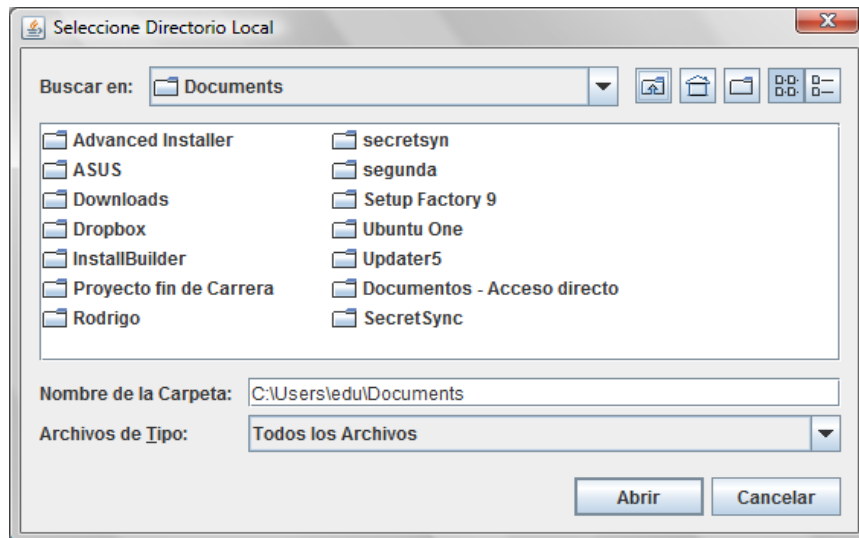


Figura 57: Explorador de archivos para seleccionar el directorio local.

Sea cual sea la opción elegida por el usuario, la ruta del directorio seleccionado tiene que ser correcta para poder avanzar al siguiente paso: *Introducir la clave de la aplicación.*

En este último paso de registro, el nuevo usuario tendrá que introducir el password.

Existen las siguientes restricciones:

- Existe **longitud mínima (8 caracteres)** pero no máxima.
- No se están permitidos los **caracteres no válidos** [*, ?, ,>, <, \, /, |].

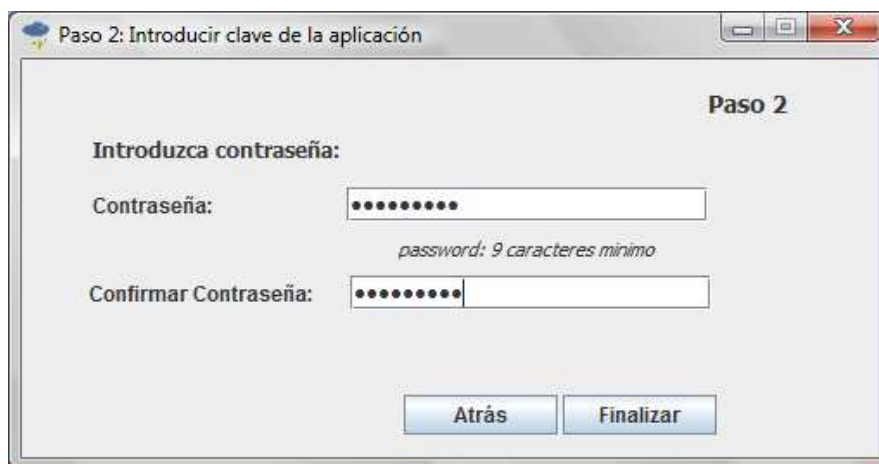


Figura 58: Paso 2 del registro de usuarios. Ventana para introducir el password de la aplicación.

Si el password introducido es correcto y coincide en ambas casillas, el usuario quedará registrado en la aplicación y podrá comenzar a utilizar KonEncriptación.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Una vez que el usuario se ha registrado, KonEncriptación ofrece la posibilidad de exportar la clave a un archivo de texto.



Figura 59: Aviso para exportar la clave de usuario.

Únicamente existe esta oportunidad de hacerlo. Es recomendable que se haga, pero no obligatorio.

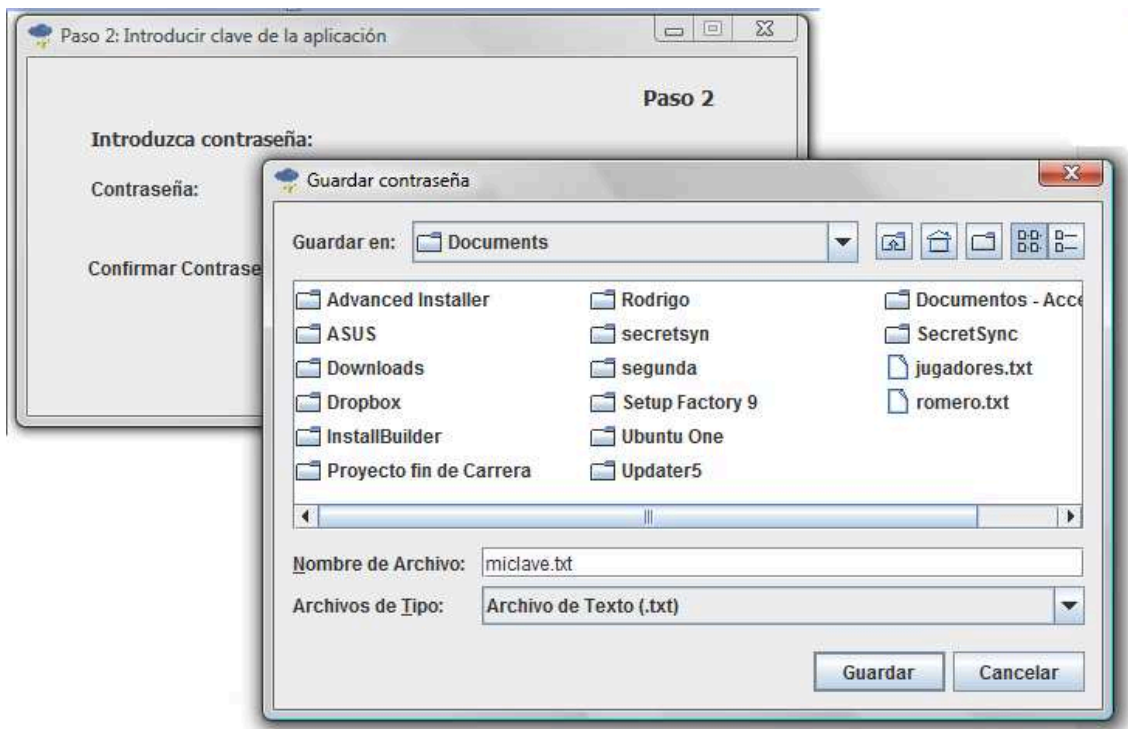


Figura 60: Explorador de archivos para exportar la clave.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

La responsabilidad de guardar posteriormente estos datos es del usuario. Se aconseja que se guarde en lugares que no estén al acceso de otras personas.

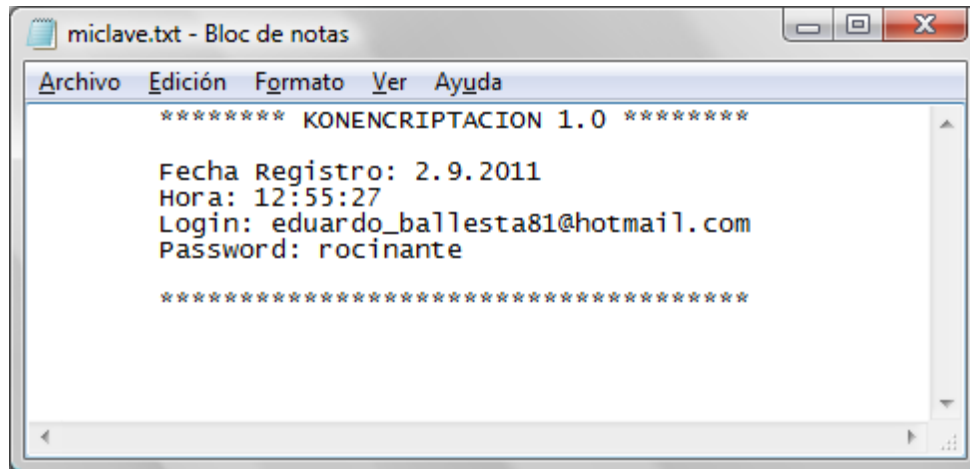


Figura 61: Archivo generado al exportar la clave.

Antes de que se cierre la aplicación tras el registro, el usuario tendrá también la oportunidad de activar la opción de crear links públicos de la barra de herramientas integrada de *Dropbox* (**ver apartado 5.8.2**).

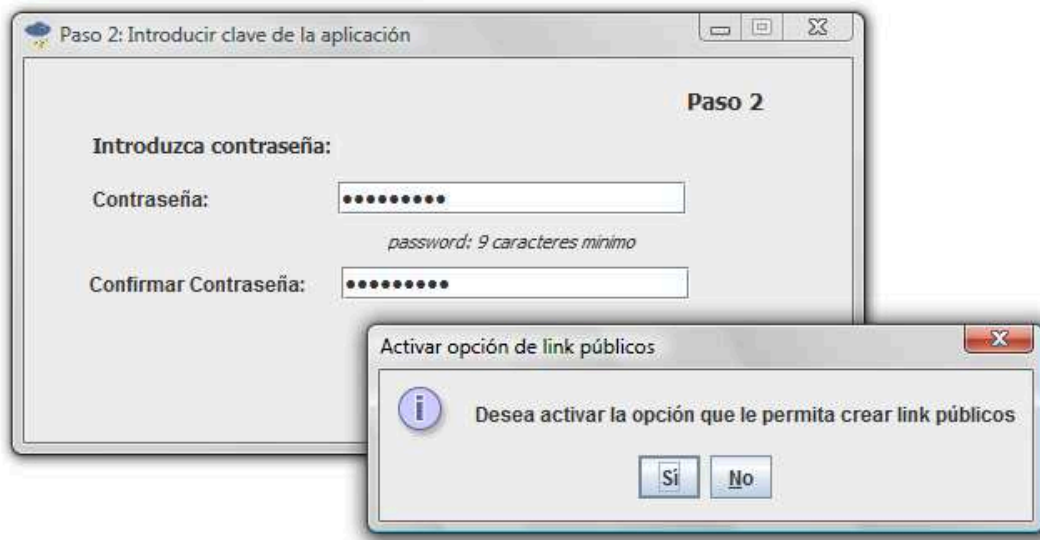


Figura 62: Ventana de opción de activación de links públicos del registro de usuario.

Esta acción es opcional puede activarse posteriormente desde el menú principal de la aplicación (**ver apartado 5.7.6**). Si el usuario desea activarla en ese momento, la ventana de activación del link público del **apartado 5.8.2** se mostrará y podrá hacerlo.

Una vez completados estos pasos, se mostrará de nuevo la ventana de acceso a KonEncriptación y el usuario podrá comenzar la sesión.

5.4. Acceso a la aplicación

Para acceder a la aplicación hay que hacer doble clic sobre el icono de acceso directo a KonEncriptación que hay en el escritorio. En ese momento aparecerá la ventana de acceso a KonEncriptación donde el usuario de la sesión deberá introducir su login y password para identificarse. Si el usuario está registrado y todo es correcto, el usuario podrá comenzar una nueva sesión en KonEncriptación. Además, KonEncriptación se iniciará en inglés, si el idioma preestablecido es ese.

Al iniciarse KonEncriptación, en la barra de tareas de la plataforma aparecerá el icono de la herramienta indicándole al usuario que la aplicación está ejecutándose. Una vez que KonEncriptación termine su ejecución este icono desaparecerá de la barra de tareas.



Figura 63: *Icono en la barra de tareas de KonEncriptación indicando que la herramienta se está ejecutando.*



Figura 64: *Formulario de identificación de usuario.*

5.4.1. Posibles problemas al inicio de sesión

KonEncriptación, valida antes del inicio de sesión ciertos parámetros para determinar que el inicio de sesión va a ser correcto. Si alguno de estos parámetros no es correcto KonEncriptación no podrá iniciarse. Las validaciones realizadas por Encriptación se pueden ver en los siguientes apartados.

5.4.1.1. Validación de usuario

El usuario registrado en KonEncriptación y el de *Dropbox* tienen que ser el mismo. Si algún usuario cambia la cuenta de usuario asociada a *Dropbox* mientras que KonEncriptación no está siendo

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

utilizado, KonEncriptación detectará dicho cambio cuando compruebe las cuentas de ambas herramientas al inicio de sesión.

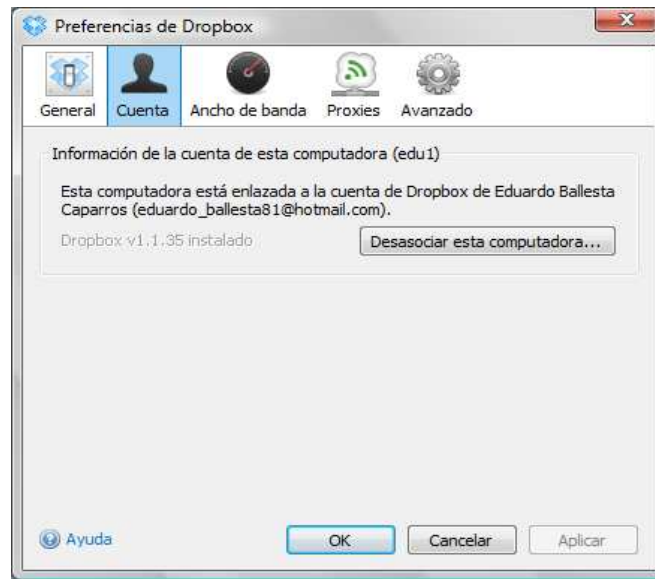


Figura 65: Opción para desasociar una cuenta de usuario desde Dropbox.

De esta manera, KonEncriptación obligará a que el nuevo usuario de *Dropbox* tenga que registrarse, eliminándose del archivo de registro al anterior usuario.



Figura 66: Error mostrado cuando el usuario de KonEncriptación y Dropbox no coinciden.

5.4.1.2. No existe el directorio asociado a Dropbox

Al iniciarse KonEncriptación valida, entre otras cosas, si el directorio asociado a Dropbox existe. En caso contrario se mostrará un mensaje indicándole al usuario que debe asociar Dropbox con un nuevo directorio para poder ejecutar KonEncriptación. Inmediatamente KonEncriptación se cerrará.

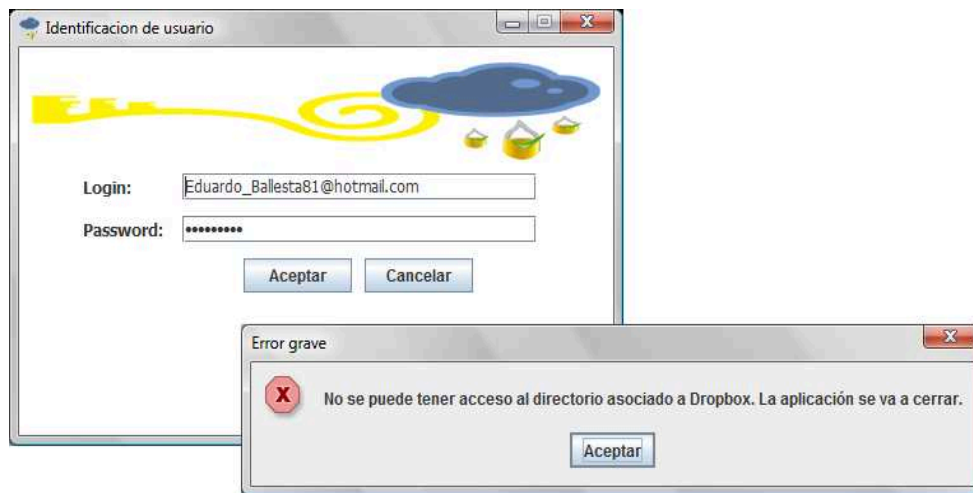


Figura 67: Error indicando que el directorio asociado a Dropbox no existe.

5.4.1.3. La ubicación del directorio asociado a Dropbox ha cambiado

El usuario de una cuenta de *Dropbox* puede cambiar la ubicación del directorio asociado a *Dropbox* mediante el menú Preferencias de dicha herramienta mostrada en la siguiente Figura.

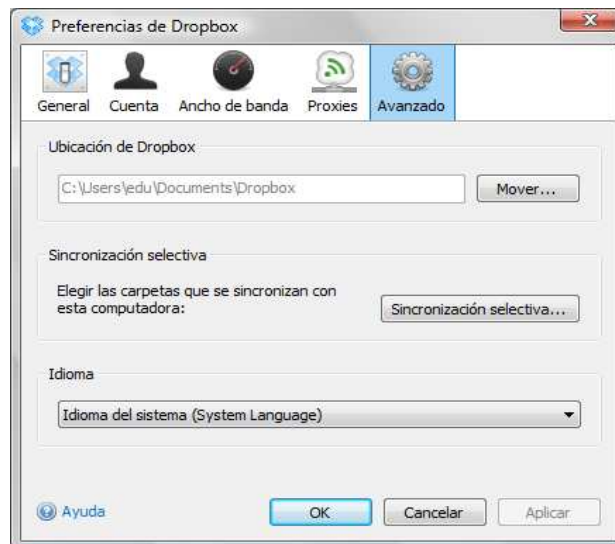


Figura 68: Opción del menú Preferencias de Dropbox para cambiar la ubicación del directorio de este.

Si el cambio de la misma se realiza mientras KonEncriptación no está ejecutándose, al iniciar la sesión comprobará que el directorio de *Dropbox* ha cambiado con respecto a la última sesión realizada y avisará al usuario de este cambio. Posteriormente a mostrar el mensaje de la [Figura 69](#) y la ejecución continuará su cauce normal, aunque la nueva ruta será almacenada en el archivo de configuración.



Figura 69: Aviso de cambio de ubicación del directorio Dropbox con respecto a la última sesión.

5.4.1.4. Validación del directorio local

Al iniciarse KonEncriptación valida si el directorio local donde trabaja de forma segura existe. Si el directorio no existe, KonEncriptación mostrará un mensaje indicándole al usuario que debe seleccionar un nuevo directorio con el que poder trabajar.

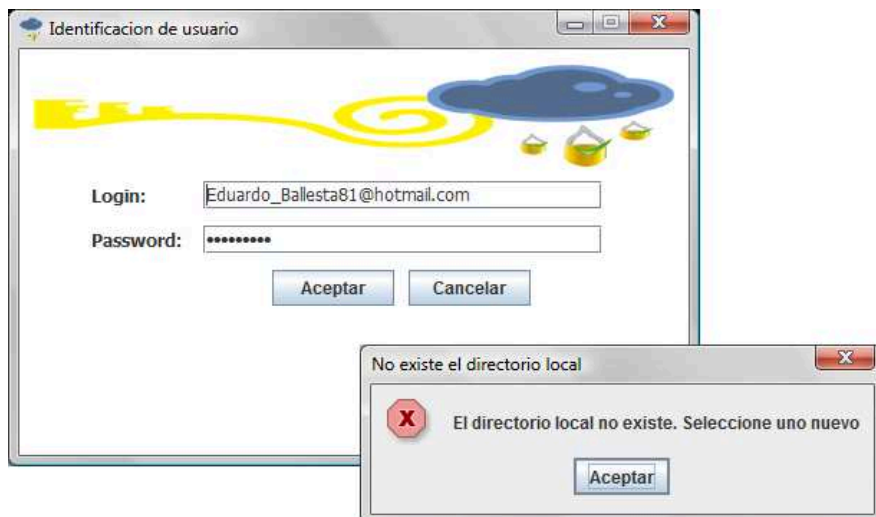


Figura 70: Aviso de que el directorio local no existe antes del inicio de sesión en KonEncriptación.

Una vez leído el mensaje, un explorador de archivos aparecerá y el usuario deberá escoger el directorio local donde desea trabajar de forma segura. Una vez seleccionado y validado el directorio, KonEncriptación se ejecutará de forma normal.

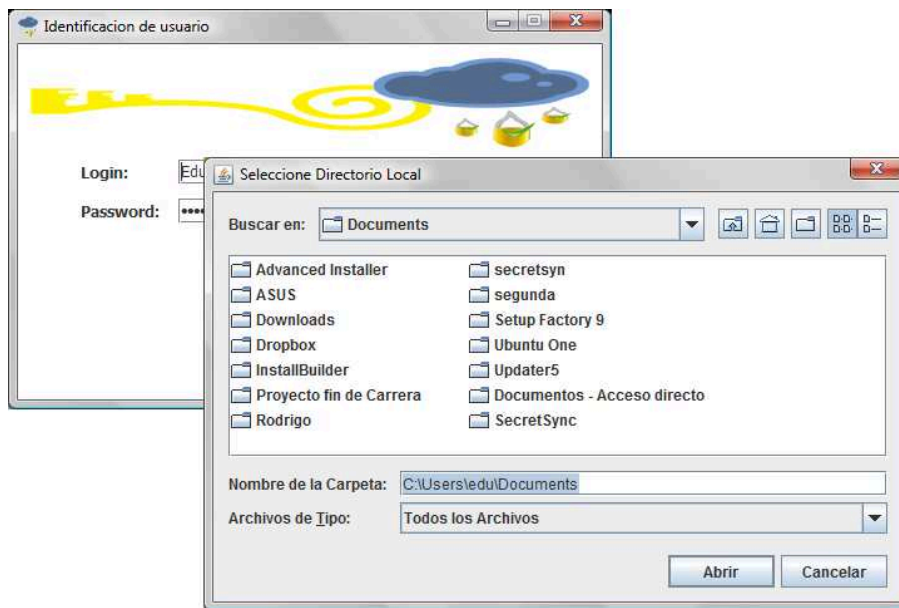


Figura 71: Explorador de archivos para seleccionar el nuevo directorio local.

5.5. Elementos de la ventana principal de la aplicación

En la **Figura 72** se puede la apariencia de la ventana principal de la aplicación. Dicha ventana se divide en 6 secciones que serán descritas brevemente en este apartado. Dichas secciones son:

- Menú principal
- Directorio local
- Directorio remoto
- Operaciones generales
- Barra de progreso de operaciones
- Menú sesión.



Figura 72: Apariencia y distribución de la ventana principal de KonEncriptación.

5.5.1. Menú principal

Desde el menú principal se pueden realizar todas las operaciones integradas en la herramienta. Éste se divide en varios submenús dependiendo del tipo o grupo de operación que vaya a desarrollar. Estos submenús son:

- Inicio
- Operaciones
- Edición
- Archivo
- *Dropbox*
- Agenda de usuarios
- Ayuda

5.5.1.1. Menú inicio

En él se agrupan operaciones de configuración como:

- Cambiar directorio local (ver apartado 5.7.3).
- Introducir número de usuario (ver apartado 5.8.6).

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Cambiar número de usuario (**ver apartado 5.8.7**).
- Seleccionar idioma (**ver apartado 5.9.9**).
- Salir de KonEncriptación (**ver apartado 5.10**).

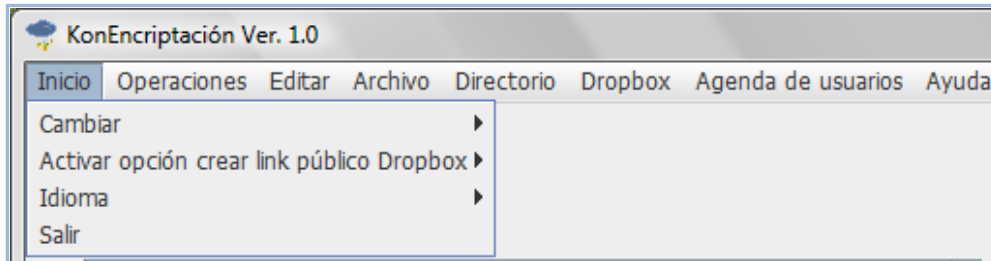


Figura 73: Operaciones del menú inicio.

5.5.1.2. Menú operaciones

Desde él el usuario puede realizar las operaciones generales entre directorios que ofrece KonEncriptación y que vienen descritas en el **apartado 5.6**.

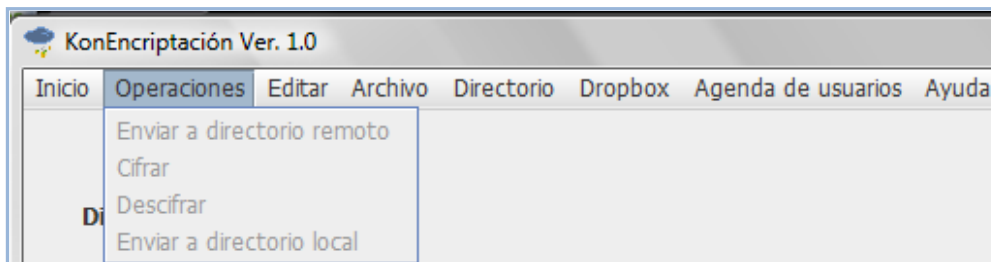


Figura 74: Operaciones del menú operaciones.

5.5.1.3. Menú edición

En este menú se integran todas las operaciones relacionadas con la edición de archivos y directorios, sin incluir las opciones de crear archivos y directorios. Las operaciones integradas en este menú son:

- Copiar archivo y/o directorio (**ver apartado 5.7.4.3**).
- Pegar archivos y/o directorios (**ver apartado 5.7.4.4**).
- Renombrar archivo y/o directorio (**ver apartados 5.7.4.5 y 5.7.4.6**).
- Eliminar archivo y/o directorio (**ver apartado 5.7.4.7**).



Figura 75: Operaciones del menú edición.

5.5.1.4. Menú archivo

En este menú se agrupan todas las operaciones locales (dentro de los directorios local o remoto) relacionadas con archivos cifrados y en claro, así como con el tratamiento y procesamiento de peticiones. Las operaciones que se pueden realizar son:

- Abrir archivo con aplicación del sistema operativo (**ver apartado 5.7.1**).
- Nuevo archivo (**ver apartado 5.7.4.1**).
- Cifrar aquí (**ver apartado 5.7.5.1**).
- Descifrar aquí (**ver apartado 5.7.5.2**).
- Ver permisos de acceso de un archivo cifrado (**ver apartado 5.7.6.1**).
- Agregar usuarios validado a un archivo cifrado desde la agenda (**ver apartado 5.7.7.11**).
- Aceptar peticiones de acceso (**ver apartado 5.7.6.2**).

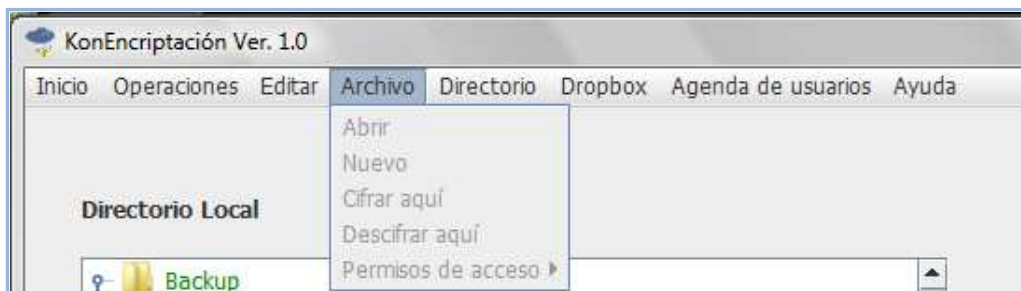


Figura 76: Operaciones del menú archivo.

5.5.1.5. Menú directorio

En este menú se agrupan todas las operaciones locales (dentro de los directorios local o remoto) relacionadas con directorios, así como con algunas operaciones de tratamiento y procesamiento de peticiones. Las operaciones que se pueden realizar son:

- Abrir directorio con el explorador de archivos de S.O (**ver apartado 5.7.2**).
- Nuevo directorio (**ver apartado 5.7.4.2**).
- Buscar peticiones de acceso dentro de un directorio (**ver apartado 5.7.6.4**).

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Enviar peticiones de acceso a archivos cifrados (**ver apartado 5.7.6.5**).

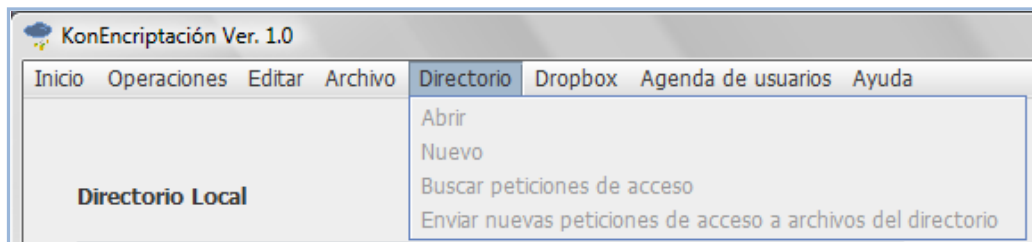


Figura 77: Operaciones del menú directorio.

5.5.1.6. Menú Dropbox

Se integran todas las operaciones de la barra de herramientas de *Dropbox*. Las operaciones que se pueden realizar son:

- Navegar al sitio Web de *Dropbox* (**ver apartado 5.8.1**).
- Copiar enlace público (**ver apartado 5.8.2**).
- Ver versiones anteriores (**ver apartado 5.8.3**).
- Compartir esta carpeta (**ver apartado 5.8.4**).
- Copiar el enlace de la galería pública (**ver apartado 5.8.5**).



Figura 78: Operaciones del menú Dropbox.

5.5.1.7. Agenda de usuarios

Este menú agrupa algunas de las opciones implementadas para la gestión de la agenda de usuarios.

- Ver usuarios de la agenda (**ver apartado 5.7.7.1**).
- Ver carpetas compartidas (**ver apartado 5.7.7.2**).
- Asociar un usuario con una carpeta compartida (**ver apartado 5.7.7.7**).
- Agregar un nuevo usuario a la agenda (**ver apartado 5.7.7.3**).

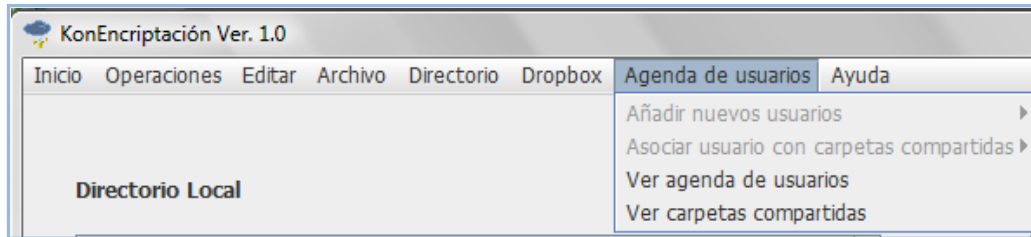


Figura 79: Operaciones del Menú Agenda de Usuarios.

5.5.1.8. Menú ayuda

El menú ayuda está compuesto por:

- Acerca de ...
- Manual rápido.

Acerca de

En este menú se muestra información acerca de la versión de la herramienta y del desarrollador de la misma.

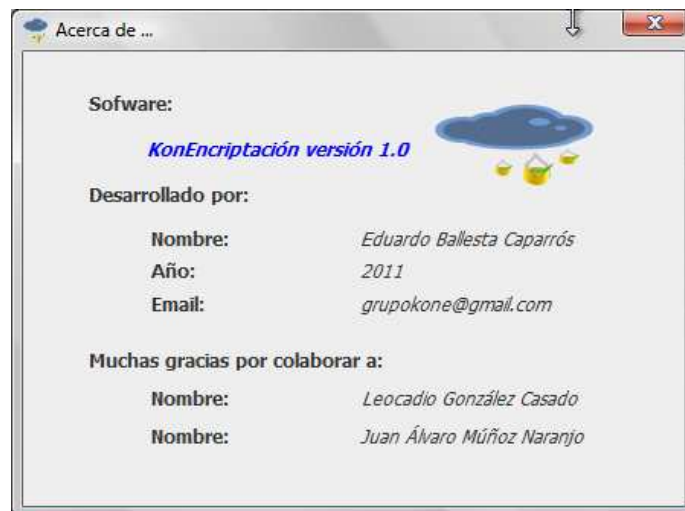


Figura 80: Ventana Acerca de.

Ayuda

Para la ayuda de KonEncriptación se ha desarrollado una página Web donde se integra el manual de usuario íntegramente. La página de inicio de la ayuda es **indice.html**.



Figura 81: Ventana de inicio de la ayuda de KonEncriptación.

5.5.2. Directorio local

El objetivo principal del directorio local es el de permitir al usuario de KonEncriptación trabajar de manera aislada con respecto al directorio asociado a *Dropbox*. En él, el usuario podrá tener un back up de la información que desee guardar y editarla sin que dichos archivos estén expuestos a los riesgos y problemas de seguridad que actualmente tiene *Dropbox*. Además, la información podrá ser enviada cifrada o sin cifrar a cualquier ubicación dentro del directorio *Dropbox* ofreciéndole la máxima seguridad a dicha información. Indicar también que existen algunas restricciones de edición de archivos y directorios descrita en el [apartado 5.7.6.6](#) y que todos los cambios realizados en los directorios y subdirectorios fuera de KonEncriptación serán actualizados de manera inmediata ([ver apartado 5.9.3](#)).

5.5.2.1. Menú contextual del directorio local

El directorio local tiene integrado un menú contextual donde se podrán realizar todas las operaciones locales integradas en la aplicación. Dichas operaciones vienen descritas en el [apartado 5.7](#).

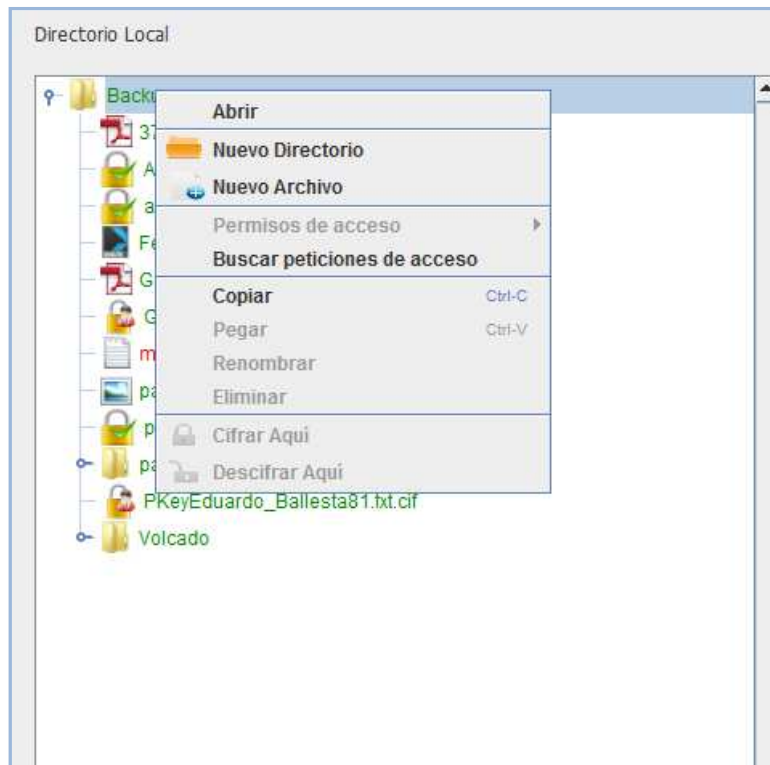


Figura 82: Menú contextual del directorio local.

5.5.3. Directorio remoto

El directorio remoto de KonEncriptación se corresponde con el directorio asociado a *Dropbox*. El uso idóneo para este directorio es el de gestión de peticiones de acceso a archivos cifrados por parte de los usuarios en carpetas compartidas y el uso de las operaciones del menú contextual de *Dropbox*. Se sugiere que si el usuario desea editar la información lo haga en el directorio local, aunque también se le está permitido aquí. Al igual que el directorio local, todos los cambios realizados en los directorios y subdirectorios fuera de KonEncriptación serán actualizados de manera inmediata (**ver apartado 5.9.3**).

5.5.3.1. Menú contextual del directorio remoto

El directorio remoto tiene integrado un menú contextual donde podrá realizar todas las operaciones locales integradas por la aplicación así como las del menú contextual de *Dropbox* y las de la agenda de usuario. Dichas operaciones vienen descritas en los **apartados 5.7 y 5.8**.

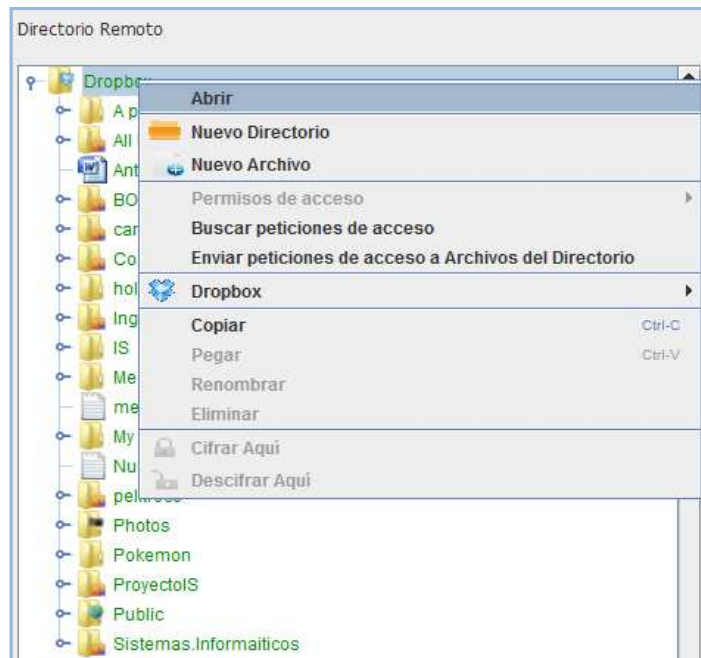


Figura 83: Menú contextual del directorio remoto.

5.5.4. Operaciones generales

Se trata de las principales operaciones que se pueden realizar para el procesamiento de información entre los directorios local y remoto. Estas operaciones vienen descritas en el [apartado 5.6](#).

5.5.5. Menú sesión

Muestra información sobre el usuario que tiene abierta la sesión actualmente y le ofrece la posibilidad de salir de KonEncriptación ([ver apartado 5.10](#)).

5.5.6. Barra de progreso de operaciones

En ella el usuario puede ver el tipo de operación que se está desarrollando actualmente y el progreso en la realización de la misma. Los tipos de operaciones en las que se muestra su progreso son: cifrar, descifrar y copiar archivos en otra ubicación.

5.6. Operaciones entre Directorios

En este apartado se describen todas las operaciones que un usuario de KonEncriptación puede realizar para el envío de información entre los directorios local y remoto. Estas operaciones vienen

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

integradas en Menú Principal → Menú Operaciones o en la sección Operaciones generales descrita en el [apartado 5.5.4](#).

5.6.1. Cifrar archivos

Esta opción permite al usuario de la sesión enviar cifrados uno o varios archivos en claro seleccionados en el directorio local al directorio remoto o viceversa.

En primer lugar, el usuario debe seleccionar uno o varios archivos en claro de cualquiera de los dos directorios (**local o remoto**) y, posteriormente, seleccionar obligatoriamente un directorio en el directorio opuesto (**local o remoto**) para que el botón cifrar de las operaciones generales o del menú operaciones se active.

Existen dos tipos de iconos que indican al usuario el sentido de la operación:



Enviar cifrados archivos en claro desde el directorio local al directorio remoto.



Enviar cifrados archivos en claro desde el directorio remoto al directorio local.

El envío de archivos cifrados puede generar avisos que le indiquen al usuario de sesión que ya existen archivos cifrados en el directorio destino y le ofrezca la opción de renombrarlos o reemplazarlos como se muestra en el [apartado 5.9.4](#).

5.6.2. Descifrar archivos

Esta opción permite al usuario de la sesión enviar descifrados uno o varios archivos cifrados seleccionados en el directorio local al directorio remoto o viceversa.

En primer lugar el usuario debe seleccionar uno o varios archivos cifrados de cualquiera de los dos directorios (**local o remoto**) y, posteriormente, seleccionar obligatoriamente un directorio en el directorio opuesto (**local o remoto**) para que el botón descifrar de las operaciones generales o del menú operaciones se active.

Existen dos tipos de iconos que indican al usuario el sentido de la operación:



Enviar descifrados archivos cifrados desde el directorio local al directorio remoto.



Enviar descifrados archivos cifrados desde el directorio remoto al directorio local.

El envío de archivos descifrados puede generar avisos que le indiquen al usuario de sesión que ya existen archivos en claro en el directorio destino y le ofrezca la opción de renombrarlos o reemplazarlos como se muestra en el [apartado 5.9.4](#).

5.6.3. Enviar archivos y/o directorios al directorio remoto

Esta opción permite al usuario de la sesión enviar una copia de los archivos y/o directorios seleccionados en el directorio local a un directorio seleccionado dentro del directorio remoto.

En primer lugar el usuario debe seleccionar uno o varios archivos y/o directorios del directorio **local** y, posteriormente, seleccionar obligatoriamente un directorio en el directorio **remoto** para que el botón de enviar de las operaciones generales o del menú operaciones se active.

El icono asociado a esta operación es el siguiente:



Enviar una copia de los archivos y/o directorios seleccionados en el directorio local a un directorio dentro del directorio remoto.

El envío de archivos y directorios puede generar avisos que le indiquen al usuario de sesión que ya existen los archivos o directorios en el destino como se muestra en [los apartados 5.9.4 y 5.9.5](#).

5.6.4. Enviar archivos y/o directorios al directorio local

Esta opción permite al usuario de la sesión enviar una copia de los archivos y/o directorios seleccionados en el directorio remoto a un directorio seleccionado dentro del directorio local.

En primer lugar el usuario debe seleccionar uno o varios archivos y/o directorios del directorio **remoto** y, posteriormente, seleccionar obligatoriamente un directorio en el directorio **local** para que el botón de enviar de las operaciones generales o del menú operaciones se active.

El icono asociado a esta operación es el siguiente:



Enviar una copia de los archivos y/o directorios seleccionados en el directorio remoto a un directorio dentro del directorio local.

El envío de archivos y directorios puede generar avisos que le indiquen al usuario de sesión que ya existen los archivos o directorios en el destino como se muestra en [los apartados 5.9.4 y 5.9.5](#).

5.6.5. Mover archivos y/o directorios arrastrándolos con el ratón

KonEncriptación permite que los archivos y/o directorios seleccionados en uno de los dos directorios (**local o remoto**) sean arrastrados con el ratón de un directorio a otro.

Dependiendo de la clase de archivos y/o directorios que sean arrastrados, KonEncriptación mostrará una ventana donde le indicará al usuario qué tipos de operaciones puede realizar.

Las operaciones permitidas para esta opción son las descritas en este mismo apartado.

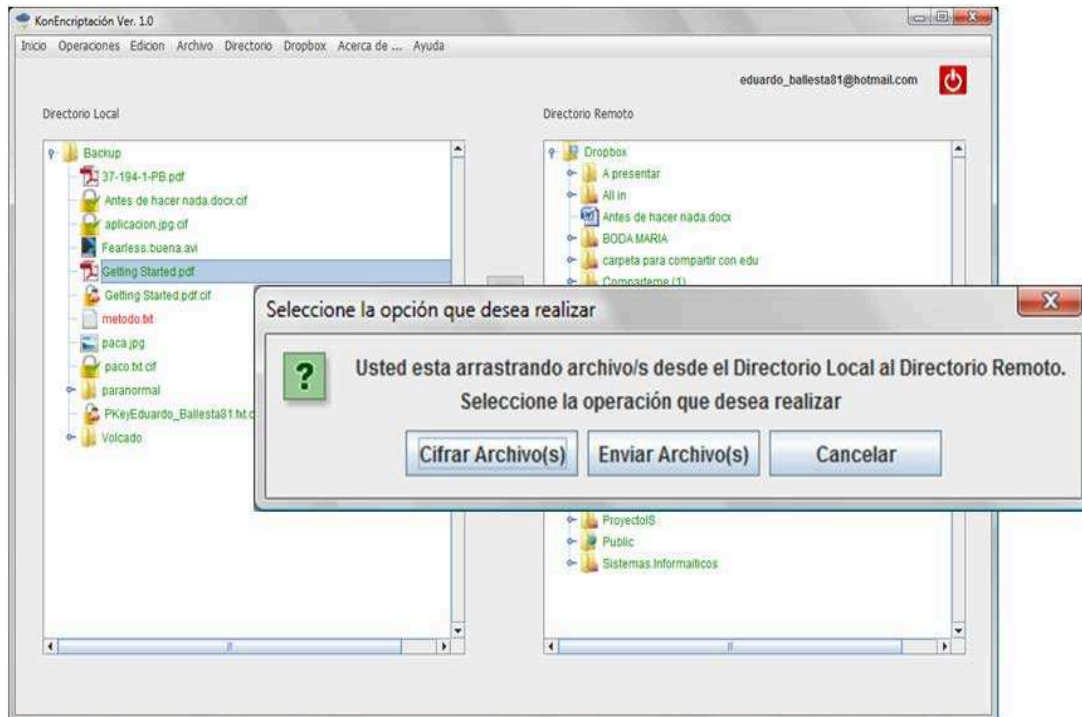


Figura 84: Ventana de selección de operaciones permitidas tras arrastrar archivos y/o carpetas entre los directorios local y remoto.

5.7. Operaciones Locales

Se trata de las operaciones que se pueden realizar localmente dentro del directorio local o remoto. Estas operaciones se pueden realizar desde los submenús edición, archivo y directorio del menú principal y con los menús contextuales de las secciones directorio local y directorio remoto de los [apartados 5.5.2.1 y 5.5.3.1](#).

5.7.1. Abrir archivo con la aplicación asociada por el S.O.

En esta opción se le permite al usuario abrir un archivo con la aplicación del S.O. correspondiente y visualizar el contenido del mismo. Las formas de hacerlo son las siguientes:

- Seleccionar archivo, botón derecho y escoger la opción abrir del menú contextual.
- Hacer doble clic sobre el archivo seleccionado.
- Pulsar la tecla ENTER cuando se ha seleccionado un archivo.

5.7.2. Abrir directorio con el explorador de archivos del S.O.

KonEncriptación permite al usuario de sesión explorar un directorio para visualizar su contenido. Para ello el usuario de sesión tiene que:

- Seleccionar directorio, botón derecho y escoger opción abrir del menú contextual.

5.7.3. Cambiar el directorio local

Si el usuario de sesión desea cambiar el directorio local en el que está trabajando actualmente por otro nuevo tiene que:

- Ir a Menú inicio → Opción cambiar → Directorio local.

Una ventana de selección de archivos se mostrará y el usuario deberá escoger el directorio en el que desea trabajar. Una vez realizada esta operación, el directorio local de la aplicación se actualizará completamente y se guardará la nueva ruta en el archivo de configuración de KonEncriptación.

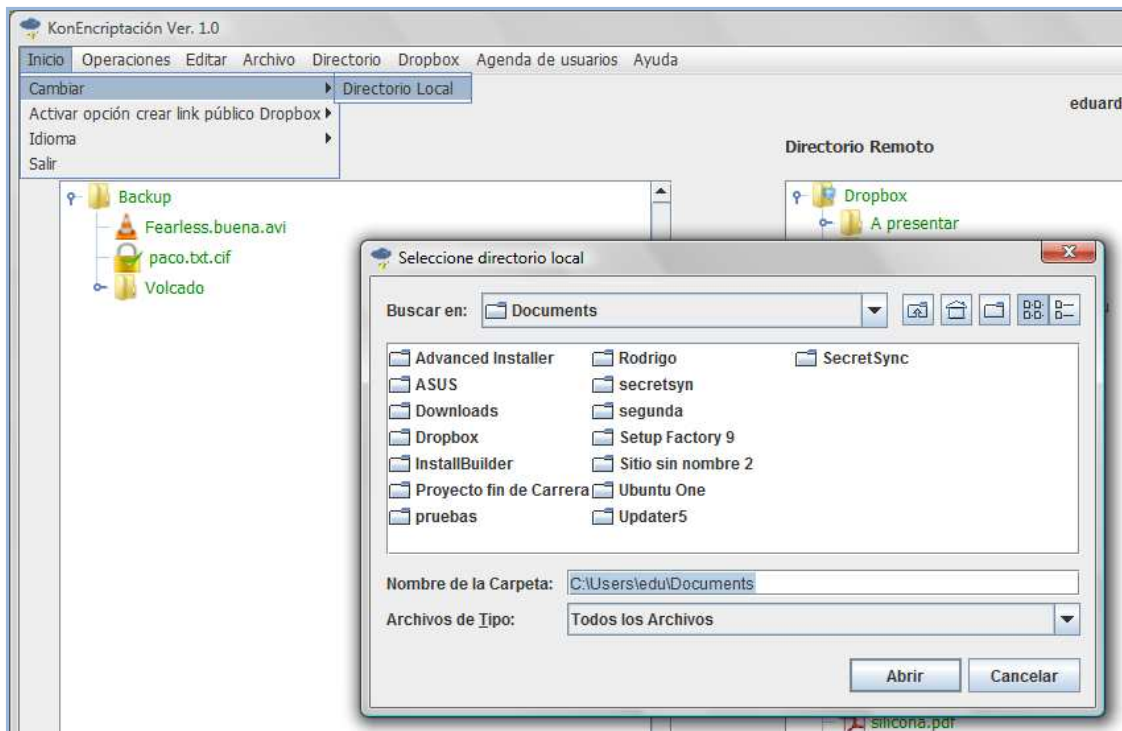


Figura 85: Explorador de archivos para seleccionar el directorio local.

5.7.4. Operaciones de Edición

En este apartado se describirán todas las operaciones de edición que se pueden realizar con archivos y directorios.

5.7.4.1. Crear un archivo nuevo

Esta opción permite crear un archivo nuevo dentro del directorio que tenga seleccionado el usuario de sesión. Esta opción está permitida tanto para el directorio local como para el remoto.

En primer lugar, se deberá introducir el nombre del archivo que se desea crear junto con la extensión del mismo. Existen **caracteres no permitidos** (*,?,/, \, <, >, |) que no podrán ser utilizados para darle nombre al archivo.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Posteriormente, se deberá pulsar el botón de Aceptar para terminar este proceso. La aplicación validará si el nombre tiene un formato correcto y si el nuevo archivo existe en el directorio donde va a ser creado, ofreciéndole la oportunidad de renombrarlo o de reemplazarlo (**ver apartado 5.9.4**).

Esta opción puede ser realizada desde:

- Menú archivo → Opción nuevo (menú principal).
- Botón derecho → Opción nuevo. (menú contextual de cualquiera de los dos directorios (local o remoto)).

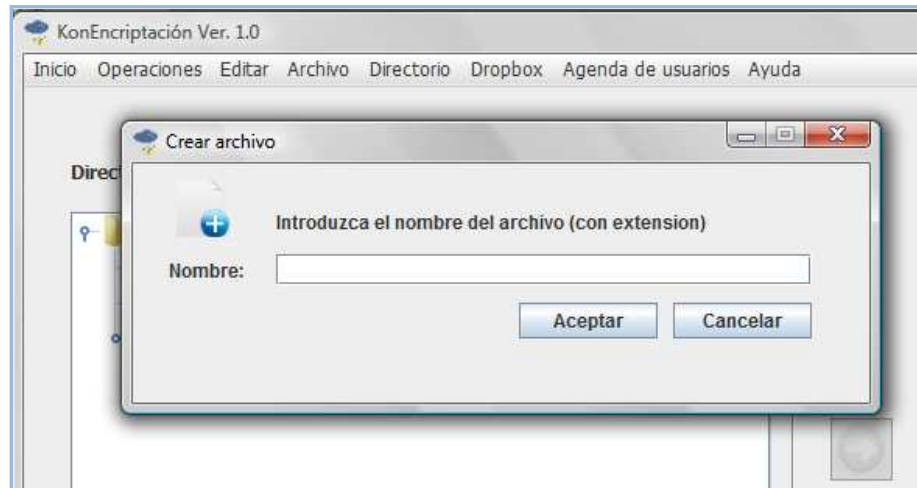


Figura 86: Formulario para crear un archivo nuevo.

5.7.4.2. Crear un directorio nuevo

Esta opción permite crear un directorio nuevo dentro del directorio que tenga seleccionado el usuario de sesión ya sea en el directorio local o en el remoto.

En primer lugar, se deberá introducir el nombre del directorio que se desea crear. Existen **caracteres no permitidos** (*,?,/, \, <, >, |) que no podrán ser utilizados para darle nombre al directorio.

Posteriormente, se deberá pulsar el botón de Aceptar para terminar este proceso. La aplicación validará si el nombre tiene un formato correcto y si el nuevo directorio existe en el directorio donde va a ser creado, ofreciéndole la oportunidad de combinar ambos directorios o cancelar la operación (**ver apartado 5.9.5**).

Esta opción puede ser realizada desde:

- Menú directorio → Opción nuevo (menú principal).
- Botón derecho → Opción nuevo (menú contextual de cualquiera de los dos directorios, local o remoto).

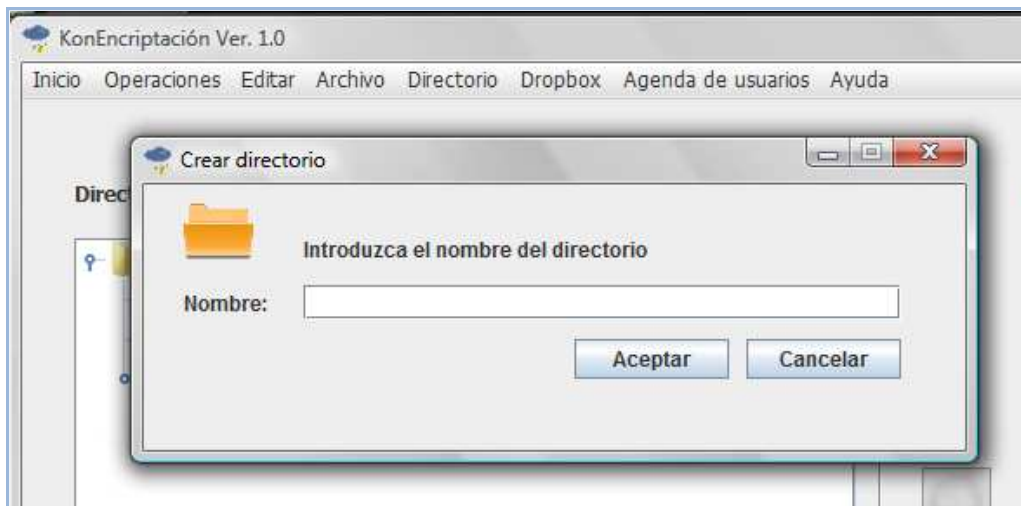


Figura 87: *Formulario para crear un directorio nuevo.*

5.7.4.3. Copiar archivos y/o directorios

Esta opción permite copiar los archivos y/o directorios seleccionados en cualquiera de los dos directorios (local o remoto) para posteriormente pegarlos en el directorio que el usuario desee. Esta operación podrá ser realizada desde:

- Menú edición → Opción copiar (menú principal).
- Botón derecho en el directorio → Opción copiar (menú contextual de cualquiera de los dos directorios, local o remoto).
- Pulsar CTR + C.

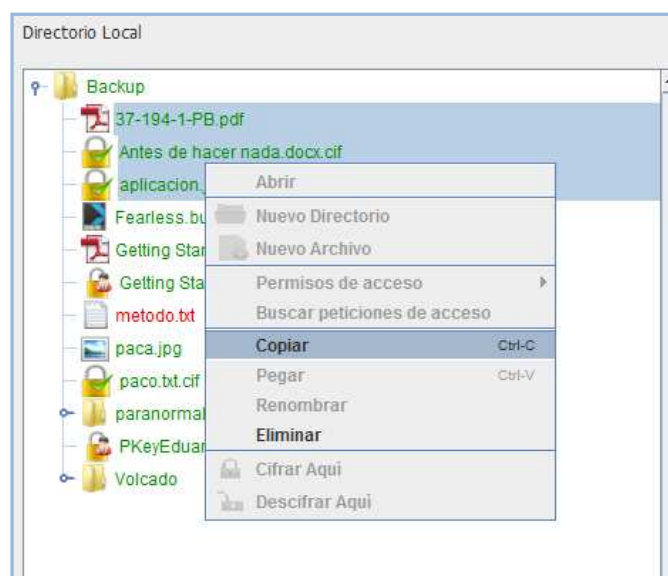


Figura 88: *Opción copiar del menú contextual del directorio local*

5.7.4.4. Pegar archivos y/o directorios

Esta opción permite pegar los archivos que están guardados en el portapapeles del sistema en el directorio seleccionado en dentro del directorio local o remoto. Tanto los archivos y/o directorios copiados, ya se haya utilizado anteriormente la opción copiar de KonEncriptación o la opción copiar de la plataforma utilizada, pueden ser pegados en el directorio seleccionado.

Un archivo cifrado en el que el usuario de sesión no tiene permiso de acceso no puede ser pegado debido a las restricciones descritas en el [apartado 5.7.6.6](#).

Los archivos copiados utilizando la opción copiar de KonEncriptación pueden ser pegados en cualquier ubicación fuera de KonEncriptación en las versiones desarrolladas para plataformas Linux. En plataformas Windows esta opción no está disponible debido al formato en el que se almacena la información en el portapapeles.

Esta operación podrá ser realizada desde:

- Menú edición → Opción pegar (menú principal).
- Botón derecho en el directorio → Opción pegar (menú contextual de cualquiera de los dos directorios, local o remoto).
- Pulsar CTR + V.



Figura 89: Opción pegar del menú contextual del directorio local

5.7.4.5. Renombrar un archivo

Esta opción permite renombrar un archivo seleccionado en el directorio local o remoto.

En primer lugar, se deberá introducir solamente el nuevo nombre del archivo que se desea utilizar con su extensión. Existen caracteres **no permitidos** (*,?,/,\\,<,>,|) que no podrán ser utilizados para darle nombre al archivo.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Posteriormente, se deberá pulsar el botón de Aceptar para terminar este proceso. La aplicación validará si el nombre tiene un formato correcto y si el archivo que se va a crear al renombrar existe en el directorio donde va a ser renombrado, ofreciéndole la oportunidad al usuario de renombrarlo o de reescribirlo (**ver apartado 5.9.4**).

Esta opción puede ser realizada desde:

- Menú archivo → Opción renombrar (menú principal).
- Botón derecho → Opción renombrar (menú contextual de cualquiera de los dos directorios, local o remoto).

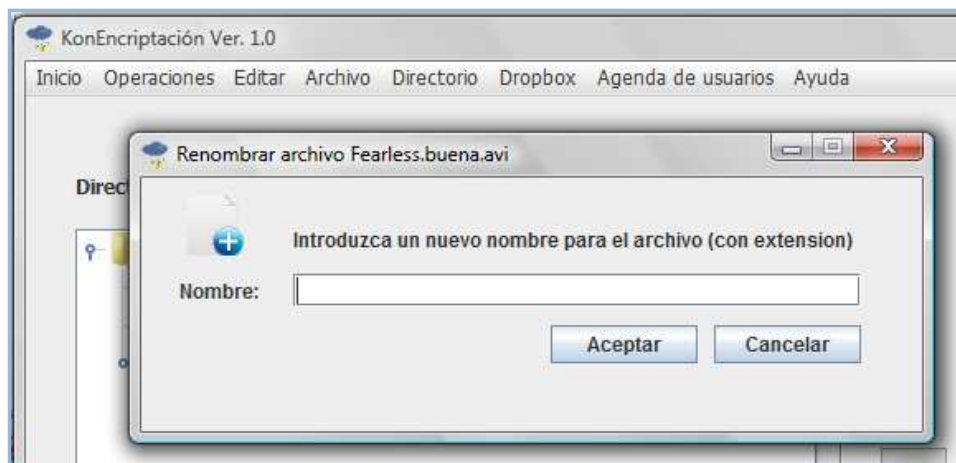


Figura 90: Formulario para renombrar un archivo existente.

5.7.4.6. Renombrar un directorio

Esta opción permite renombrar un directorio seleccionado en el directorio local o remoto.

En primer lugar, se deberá introducir el nuevo nombre que se desea dar al directorio. Existen caracteres no permitidos (*,?,/,\\,<,>,|) que no podrán ser utilizados para darle nombre al archivo.

Posteriormente, se deberá pulsar el botón de Aceptar para terminar este proceso. La aplicación validará si el nombre tiene un formato correcto y si el nuevo directorio que se va a crear al renombrar existe en el directorio donde va a ser renombrado, ofreciéndole la oportunidad al usuario de combinar ambos directorios o cancelar la operación (**ver apartado 5.9.5**).

Esta opción puede ser realizada desde:

- Menú directorio → Opción renombrar (menú principal).
- Botón derecho → Opción renombrar (menú contextual de cualquiera de los dos directorios, local o remoto).

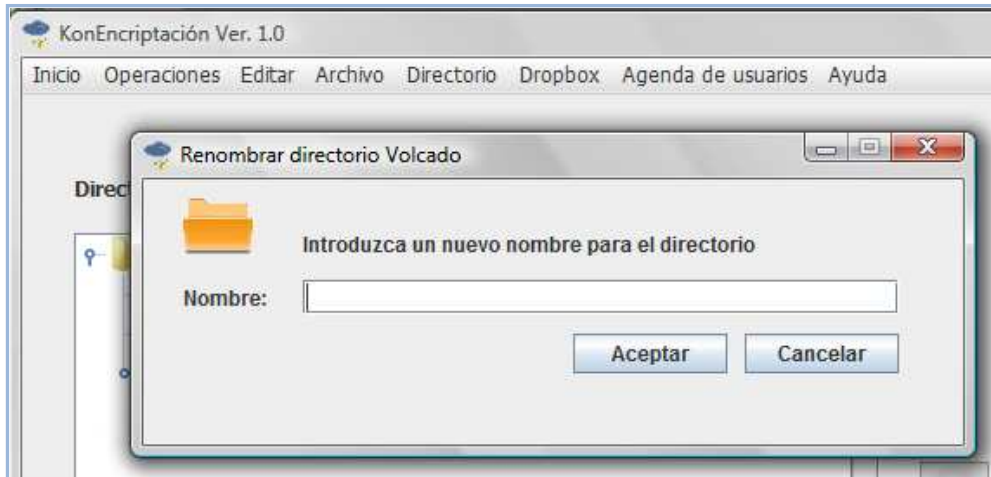


Figura 91: Formulario para renombrar un directorio existente.

5.7.4.7. Eliminar archivos y/o directorios.

Mediante esta opción se podrán eliminar los archivos y/o directorios seleccionados en el directorio local o remoto.

Si alguno de los archivos seleccionado está cifrado y el usuario de la sesión no tiene acceso a él, no podrá eliminarlo por las restricciones descritas en el [apartado 5.7.6.6](#).

Esta opción puede ser realizada desde:

- Menú directorio → Opción eliminar (menú principal).
- Botón derecho → Opción eliminar (menú contextual de cualquiera de los dos directorios, local o remoto).
- Pulsando la tecla SUPRIMIR.



Figura 92: Opción eliminar del menú contextual del directorio local.

5.7.4.8. Mover archivos y/o directorios localmente

Esta opción permite cambiar de ubicación los archivos y/o directorios seleccionados arrastrándolos hacia la nueva ubicación deseada. El proceso de arrastrar eliminará los archivos y/o directorios del directorio origen y serán copiados en la nueva ubicación.

El final del arrastre de estos archivos y/o directorios no tiene que ser un directorio necesariamente sino que puede ser un archivo y el directorio padre de este archivo será su destino.

Si alguno de los archivos seleccionados es cifrado y el usuario de la sesión no tiene acceso a él no podrá cambiarlo de ubicación por las restricciones descritas en el [apartado 5.7.6.6](#).

Si en el destino existe un archivo o directorio con el mismo nombre se mostrará una ventana de aviso para que el usuario de la sesión pueda elegir la opción que desee. [Ver apartados 5.9.4 y 5.9.5](#).

5.7.5. Operaciones con archivos cifrados

En este apartado se describen las dos operaciones relacionadas con el cifrado y descifrado de ámbito local.

5.7.5.1. Cifrar aquí

La operación cifrar aquí permite cifrar un archivo en claro seleccionado en la misma ubicación donde se encuentra dicho archivo, ya sea en el directorio local o en el remoto.

Si en la ubicación existe un archivo cifrado con el mismo nombre que el que se generará al cifrar el archivo en claro y el usuario de la sesión no tiene permiso de acceso a éste la operación no se podrá realizar por las restricciones descritas en el [apartado 5.7.6.6](#).

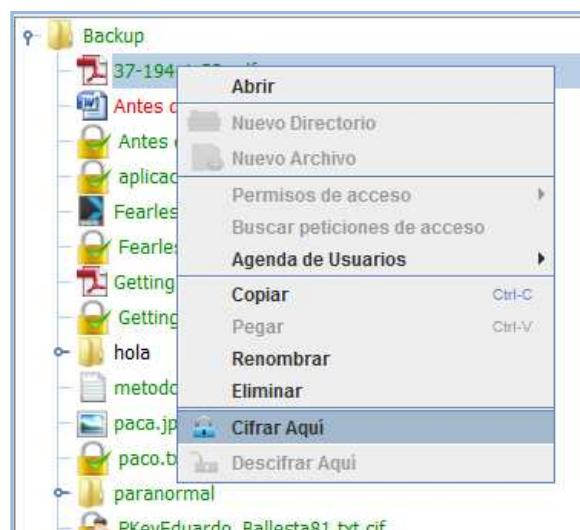


Figura 93: Opción cifrar aquí del menú contextual del directorio remoto.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

En caso contrario, un aviso para reemplazar o renombrar el archivo se mostrará (**ver apartado 5.9.4**).

- Menú directorio → Opción cifrar aquí (menú principal).
- Botón derecho → Opción cifrar aquí (menú contextual de cualquiera de los dos directorios, local o remoto).

5.7.5.2. Descifrar aquí

La operación descifrar aquí permite descifrar un archivo cifrado seleccionado en la misma ubicación donde se encuentra dicho archivo, ya sea en el directorio local o en el remoto.

Si el usuario de la sesión no tiene permiso de acceso al archivo cifrado no podrá realizar esta operación. Si existe un archivo en claro con el mismo nombre que el que se generará al descifrar el archivo cifrado, se mostrará un aviso para reemplazar o renombrar el archivo **ver apartado 5.9.4**.

- Menú directorio → Opción descifrar aquí (menú principal).
- Botón derecho → Opción descifrar aquí (menú contextual de cualquiera de los dos directorios, local o remoto).

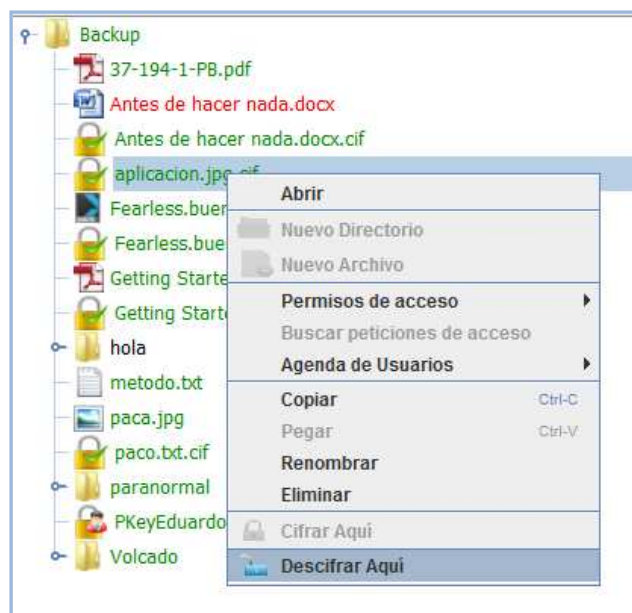


Figura 94: Opción descifrar aquí del menú contextual del directorio local.

5.7.6. Operaciones colaborativas

En este apartado se describen todas las operaciones correspondientes con la gestión y tratamiento de las peticiones de acceso a un archivo cifrado.

5.7.6.1. Ver estado de los permisos de acceso de los usuarios

Para poder ver el estado de los permisos de acceso de los usuarios a un archivo cifrado, el usuario de la sesión tendrá que hacerlo desde:

- Menú directorio → Opción archivo → Ver permiso de acceso → Usuarios (menú principal).
- Botón derecho → Opción permisos de acceso → Usuarios (menú contextual de cualquiera de los dos directorios, local o remoto).

KonEncriptación utiliza dos iconos diferentes para indicar el estado de los permisos de acceso:



Usuario con permiso de acceso.

Usuario en espera de que su petición de acceso sea aprobada.

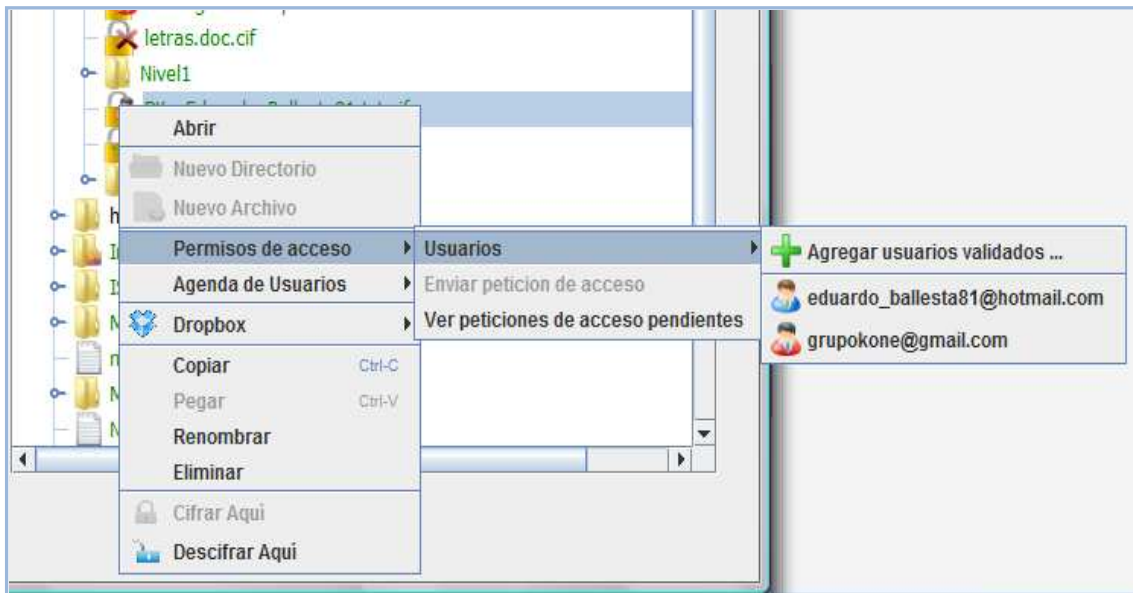


Figura 95: Opción ver estado de los permisos del menú contextual.

5.7.6.2. Aceptar petición de acceso a archivo cifrado

KonEncriptación ofrece una forma sencilla y directa de aceptar una única petición de acceso a un archivo cifrado en estado pendiente. Para realizarlo existen dos opciones:

- Menú directorio → Opción archivo → Ver permiso de acceso → Usuarios y hacer clic sobre el usuario que se encuentra en espera de que su petición sea aprobada (menú principal).
- Botón derecho → Opción permisos de acceso → Usuarios y hacer clic sobre el usuario que se encuentra en espera de que su petición sea aprobada (menú contextual de cualquiera de los dos directorios, local o remoto).

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Un usuario sólo podrá aceptar la petición de acceso de otros usuarios si tiene permiso de acceso sobre el archivo cifrado.

Existen varios tipos de iconos asociados a los archivos cifrados que se muestran en el explorador de archivos del directorio local y remoto que le indican al usuario de la sesión su estado de acceso y el estado de dicho archivo. Estos iconos son:



Usuario con permiso de acceso y archivo sin peticiones de acceso pendientes.



Usuario sin permiso de acceso.



Usuario con permiso de acceso y archivo con peticiones de acceso pendientes



Archivo en estado de sincronización. El usuario no tendrá acceso a la información de este archivo hasta que cambie a alguno de los estados anteriores.

Esta información permite conocer los estados descritos anteriormente sin tener que acceder a ninguna opción del menú.

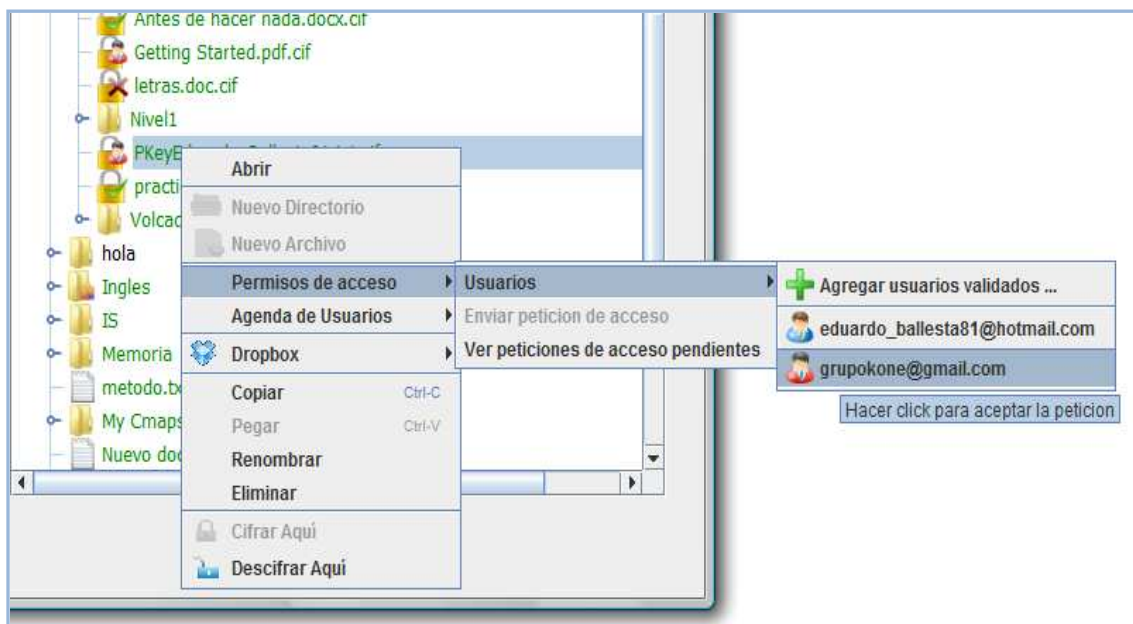


Figura 96: Opción para aceptar petición de acceso de forma directa del Menú contextual remoto.

5.7.6.3. Ver peticiones de acceso pendientes

Las peticiones pendientes de un archivo cifrado pueden verse agrupadas y ser aceptadas de forma selectiva desde las siguientes opciones:

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Menú directorio → Opción archivo → Ver permiso de acceso → Ver peticiones de acceso pendientes (menú principal).
- Botón derecho → Opción permisos de acceso → Ver peticiones de acceso pendientes (menú contextual de cualquiera de los dos directorios, local o remoto).

Esta opción estará disponible sólo si el usuario tiene permiso de acceso sobre el archivo cifrado.

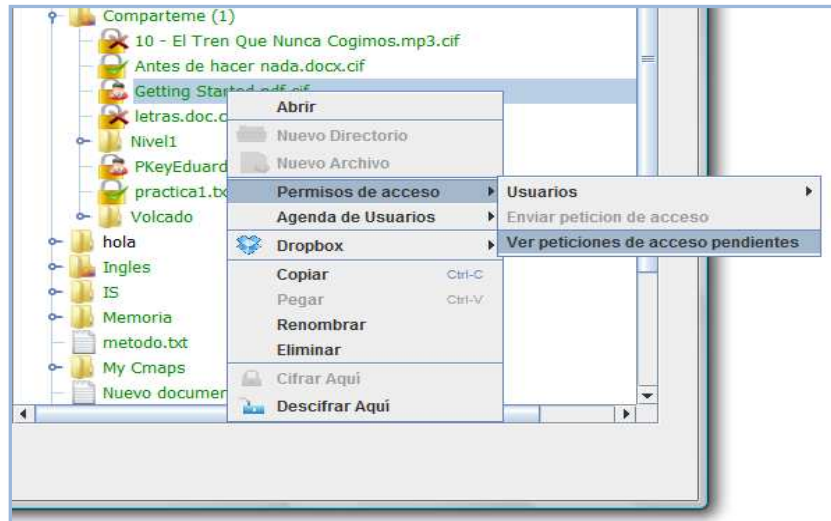


Figura 97: Opción ver peticiones de acceso pendientes del menú contextual local.

Una vez que el usuario haga clic sobre la opción ver peticiones de acceso pendientes aparecerá una nueva ventana mostrando todas las peticiones de acceso pendientes de dicho archivo. **Ver Figura 98.**

El formato de la información presentada es:

- Nombre del archivo cifrado + [...\Ruta hasta el directorio raíz (local o remoto)].
- Usuarios con peticiones pendientes.

Por otra parte, el usuario de sesión tendrá la posibilidad de realizar algunas operaciones con la agenda de usuarios del sistema. Estas operaciones son:



Eliminar a un usuario del árbol de peticiones (**ver apartado 5.7.7.10**).



Asociar usuarios seleccionados a carpetas compartidas (**ver apartado 5.7.7.7**).



Añadir a un nuevo usuario a la agenda de usuarios (**ver apartado 5.7.7.3**).



Agregar usuarios al árbol de peticiones desde la agenda de usuarios (**ver apartado 5.7.7.9**).

El usuario de la sesión puede seleccionar aquellas peticiones que desee aceptar y posteriormente serán procesadas por KonEncriptación.

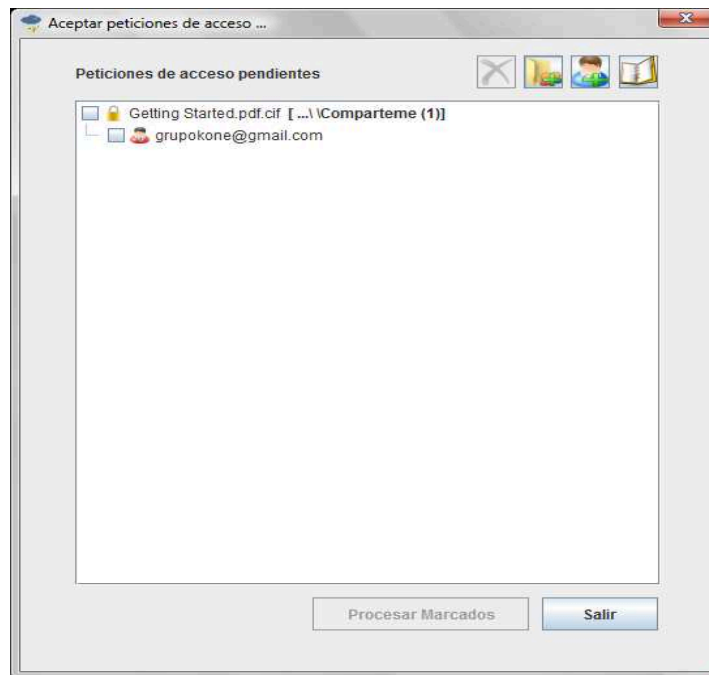


Figura 98: Ventana para aceptar peticiones pendientes de un archivo cifrado de forma selectiva.

5.7.6.4. Buscar peticiones de acceso dentro de un directorio

Esta opción permite buscar todas las peticiones de acceso pendientes dentro un directorio y subdirectorios de este, de tal forma que si existen se muestren en una lista de peticiones de acceso ordenadas en un primer nivel por los usuarios con peticiones pendientes y, en un segundo nivel y ligado a cada usuario, la lista de archivos donde este usuario ha realizado esas peticiones de acceso.

Para realizar esta opción existen dos formas de hacerlo:

- Menú directorio → Opción directorio → Buscar peticiones de acceso (menú principal).
- Botón derecho → Opción buscar peticiones de acceso (menú contextual de cualquiera de los dos directorios, local o remoto).

Una vez que es escogida esta opción un formulario de búsqueda aparecerá mientras se realiza este proceso. El proceso de búsqueda solo considerará aquellos archivos cifrados donde el usuario tiene acceso a la información del archivo cifrado.



Figura 99: Proceso de búsqueda de peticiones de acceso pendientes.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Si el proceso de búsqueda de peticiones de acceso encuentra alguna petición, una nueva ventana aparecerá mostrando todas las peticiones de acceso pendientes en el siguiente formato:

- Directorio de la búsqueda
- Usuarios con peticiones pendientes.
- Listado de archivos cifrados donde el usuario tiene peticiones de acceso pendientes + **[...\Ruta hasta el Directorio Raíz (Local o Remoto)].**

El usuario podrá seleccionar aquellas peticiones que desee aceptar y posteriormente serán procesadas por KonEncriptación.

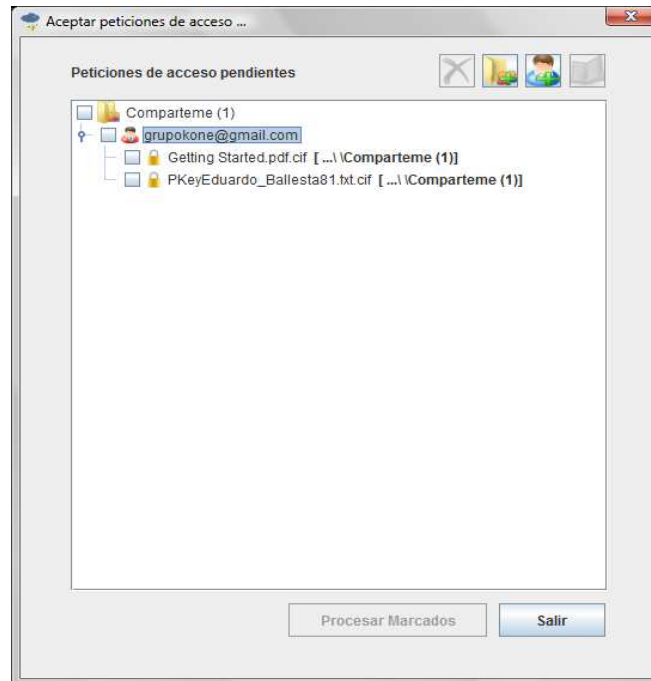


Figura 100: Ventana para aceptar peticiones pendientes de acceso a archivos cifrados de cada uno de los usuarios de forma selectiva.

Por otra parte, el usuario tendrá también la opción de utilizar diferentes opciones de la agenda de usuarios como insertar usuarios al árbol de peticiones desde la agenda o insertar usuarios que se encuentran en estado de petición a la agenda.

Estas son las opciones que el usuario de sesión podrá realizar:



Eliminar a un usuario del árbol de peticiones (**ver apartado 5.7.7.10**).



Asociar usuarios a carpetas compartidas (**ver apartado 5.7.7.7**).



Añadir a un nuevo usuario a la agenda de usuarios (**ver apartado 5.7.7.3**).



Agregar usuarios al árbol de peticiones desde la agenda de usuarios (**ver apartado 5.7.7.9**).

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Las opciones de insertar y eliminar usuarios desde la agenda estarán desactivadas para esta opción.

5.7.6.5. Enviar peticiones de acceso a archivos cifrados dentro de un directorio

Esta opción ofrece la comodidad de poder enviar, de forma inmediata, peticiones de acceso a los archivos cifrados que se encuentran dentro del directorio seleccionado o de sus subdirectorios.

Para realizar esta opción existen dos formas de hacerlo:

- Menú directorio → Opción directorio → Enviar peticiones de acceso a archivos del directorio (menú principal).
- Botón derecho → Opción enviar peticiones de acceso a archivos del directorio (menú contextual del directorio remoto).

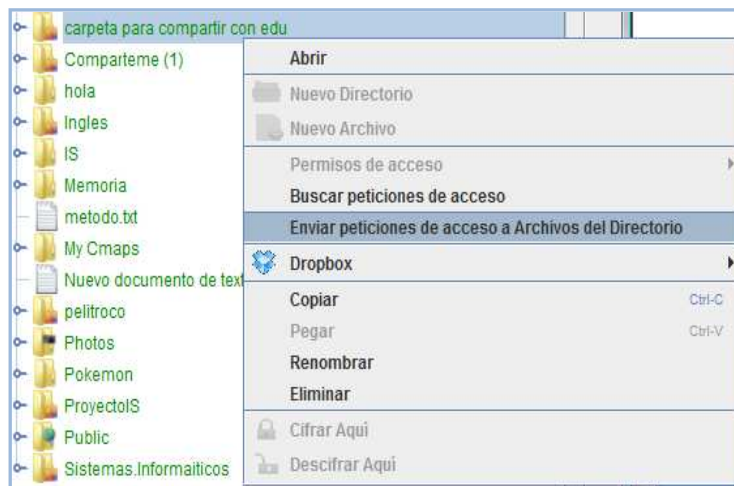


Figura 101: Opción enviar peticiones de acceso a archivos del directorio del menú contextual remoto.

5.7.6.6. Restricciones a la hora de editar archivos cifrados

Existen una serie de restricciones de edición que evitan que usuarios que no tienen acceso a un archivo cifrado puedan interferir en el trabajo del resto de usuarios que si lo están. Estas restricciones son las siguientes:

- Un usuario sin acceso a un archivo cifrado no podrá renombrarlo.
- Un usuario sin acceso a un archivo cifrado no podrá eliminarlo.
- Un usuario que intente reemplazar un archivo cifrado en el que no tiene acceso utilizando otro archivo con el mismo nombre no podrá reemplazarlo.
- Un usuario sin acceso a un archivo cifrado no podrá descifrar dicho archivo cifrado.
- Un usuario sin acceso a un archivo cifrado no podrá pegar un archivo cifrado copiado desde el portapapeles si no tiene acceso a este.
- Un usuario sin acceso a un archivo cifrado no podrá realizar ninguna de las operaciones generales de KonEncriptación con este archivo.

5.7.7. Agenda de Usuarios

La agenda de usuarios almacena la información de los distintos usuarios con los que se comparten carpetas con el fin de facilitar que el usuario de la sesión pueda añadir a dichos usuarios como validados en los archivos cifrados sin tener que esperar a que estos le envíen las peticiones de acceso previamente. La información que en la agenda se almacena es:

- **Login:** email del usuario.
- **Alias:** para reconocer de una forma más sencilla al usuario.
- **Clave pública:** asociada a la cuenta del usuario. *Pasa desapercibida al usuario.*
- **Carpetas compartidas:** donde pertenece el usuario.

Las operaciones que se pueden realizar con la agenda de usuarios se describen en los siguientes apartados.

5.7.7.1. Ver usuarios de la agenda

Con esta opción el usuario de sesión puede ver a todos los usuarios que están dados de alta en la agenda.

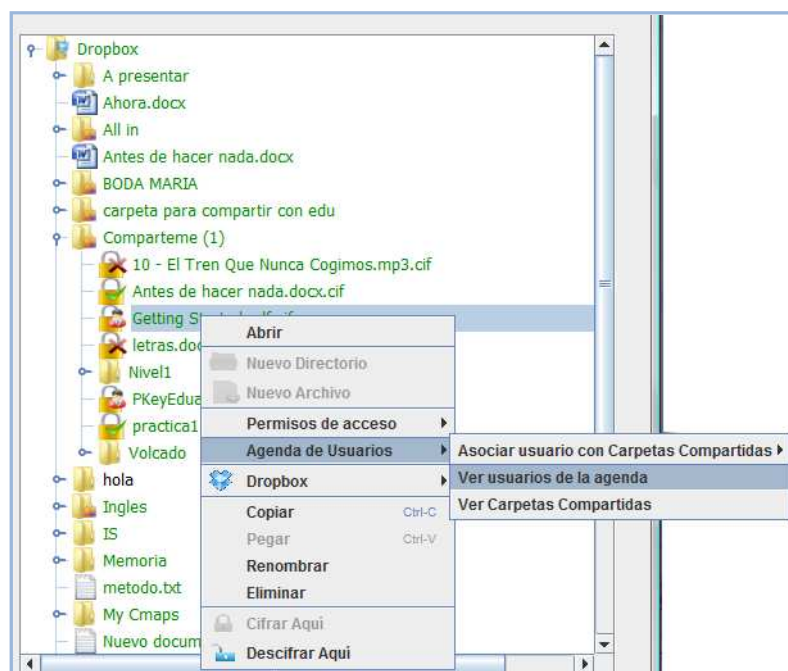


Figura 102: Opción ver usuarios de la agenda del menú contextual remoto.

Para realizar esta opción existen dos formas de hacerlo:

- Menú agenda de usuarios → Ver usuarios de la agenda.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Botón derecho → Menú agenda de usuarios → Ver usuarios de la agenda (menú contextual del directorio local o remoto).

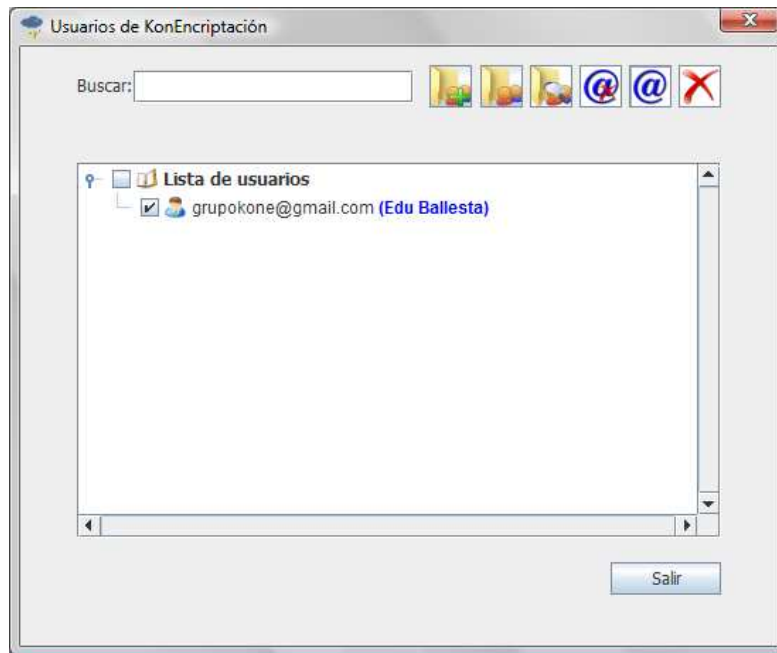


Figura 103: Ventana para ver los usuarios de la agenda.

Una vez abierto el formulario para ver los usuarios de la agenda se podrán realizar las siguientes operaciones:



Asociar usuarios a carpetas compartidas (**ver apartado 5.7.7.7**).



Ver carpetas asociadas con los usuarios de la agenda (**ver apartado 5.7.7.12**).



Buscar nuevos usuarios en carpetas compartidas (**ver apartado 5.7.7.3**).



Editar el alias de un usuario (**ver apartado 5.7.7.5**).



Eliminar el alias de un usuario (**ver apartado 5.7.7.6**).



Eliminar a un usuario de la agenda (**ver apartado 5.7.7.4**).

Buscar usuarios dentro de la lista de usuarios: *por login o por alias*.

5.7.7.2. Ver Carpetas Compartidas

Con esta opción el usuario de la sesión puede ver las carpetas compartidas que existen actualmente en *Dropbox* junto a los usuarios de la agenda que han sido asociados a ellas por el usuario de sesión.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

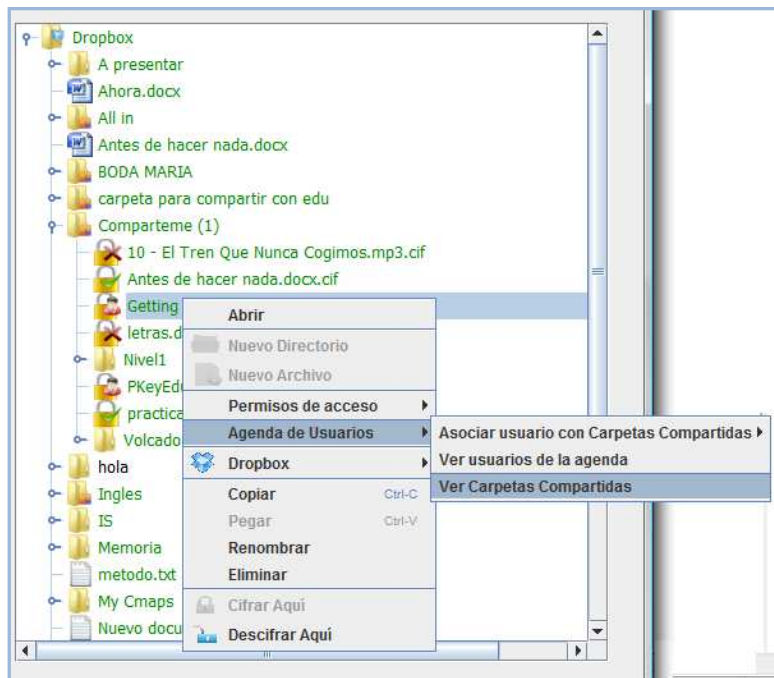


Figura 104: Ventana para Ver Carpetas Compartidas.

Para realizar esta opción existen dos formas de hacerlo:

- Menú agenda de usuarios → Ver carpetas compartidas
- Botón derecho → Menú agenda de usuarios → Ver carpetas compartidas (menú contextual del directorio local o remoto).

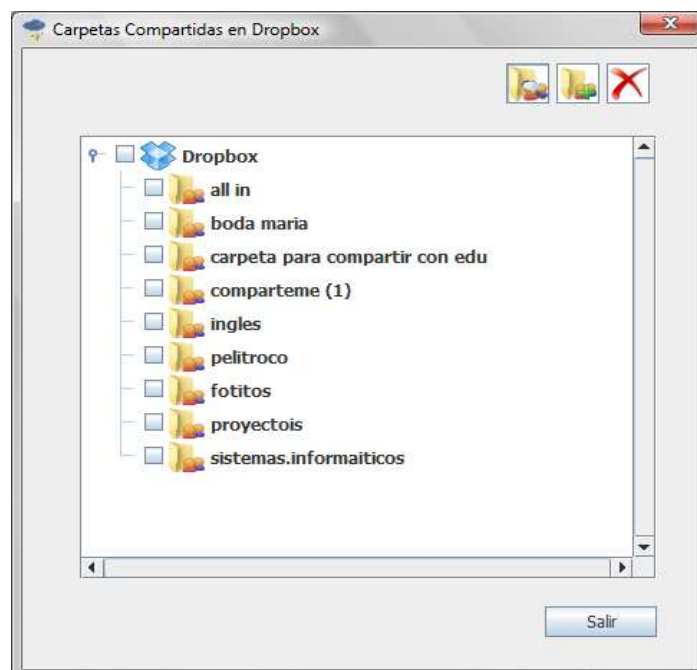
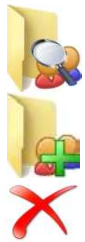


Figura 105: Ventana para ver las carpetas compartidas juntos a sus usuarios asociados.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Cuando el formulario se muestre se pueden realizar las siguientes operaciones:



Buscar nuevos usuarios en carpetas compartidas (**ver apartado 5.7.7.3**).

Asociar usuarios a carpetas compartidas (**ver apartado 5.7.7.7**).

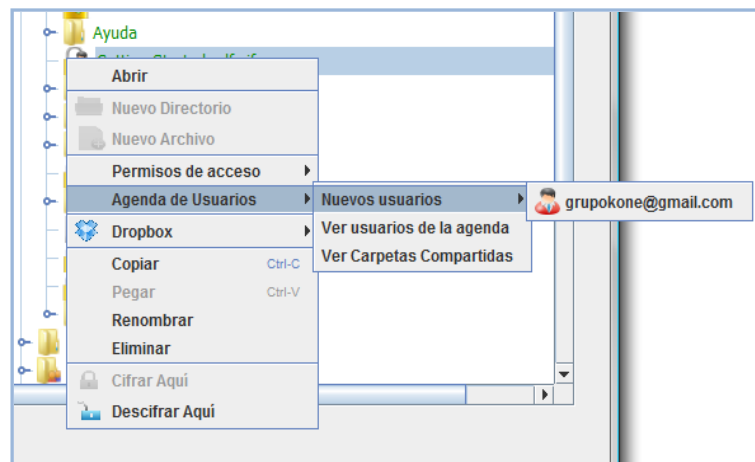
Desasociar un usuario de una carpeta compartida (**ver apartado 5.7.7.8**).

5.7.7.3. Añadir un nuevo usuario a la agenda

Un usuario puede ser añadido a la agenda desde cualquier ubicación donde haya una petición de acceso a un archivo cifrado, puesto que en ella está contenida su clave pública y su identificador de usuario (el login).

Hay varias maneras de agregar a un nuevo usuario:

- Menú contextual de cualquiera de los dos directorios (local o remoto) seleccionando un archivo cifrado → Agenda de usuarios → Nuevos usuarios → hacer clic sobre los usuarios que aparezca.
- Menú Agenda de usuarios → Nuevos usuarios → hacer clic sobre uno de los usuarios que aparezca.
- Opción buscar nuevos usuarios en el formulario de carpetas compartidas. **Apartado 5.7.7.2**.
- Opción buscar nuevos usuarios en el formulario de agregar peticiones de acceso. **Apartado 5.7.7.11**.
- Opción buscar nuevos usuarios en el formulario de ver peticiones de acceso pendientes. **Apartado 5.7.6.3**.
- Opción buscar nuevos usuarios en el formulario de combinar peticiones de acceso. **Apartado 5.9.4**.



P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Figura 106: Opción añadir nuevos usuario a la agenda del menú contextual del directorio remoto.

Si el usuario es añadido desde las opciones:

- Agenda de usuarios → Nuevos usuarios → hacer clic sobre los usuarios que aparezcan en el menú contextual de los directorios local o remoto de KonEncriptación
- Agenda de usuarios → Nuevos usuarios → hacer clic sobre los usuarios que aparezcan en el menú principal de KonEncriptación.

Posteriormente, aparecerá un formulario con las carpetas compartidas del sistema y el usuario de sesión tendrá la posibilidad de asociar al usuario añadido con cualquier carpeta compartida que desee (**ver apartado 5.7.7.7**).

Por el contrario, si las opciones de se realizan desde los procesos de búsqueda:

- Opción buscar nuevos usuarios en el formulario carpetas compartidas. **Apartado 5.7.7.2.**
- Opción buscar nuevos usuarios en el formulario de agregar peticiones de acceso. **Apartado 5.7.7.11.**
- Opción buscar nuevos usuarios en el formulario de ver peticiones de acceso pendientes. **Apartado 5.7.6.3.**
- Opción buscar nuevos usuarios en el formulario de combinar peticiones de acceso. **Apartado 5.9.4.**

Antes de realizarse el proceso de búsqueda, el usuario de sesión deberá seleccionar las carpetas compartidas donde desea buscar a los nuevos usuarios. Una vez seleccionadas, una ventana de búsqueda aparecerá mostrando el proceso íntegro de la búsqueda de usuarios en dichas carpetas.

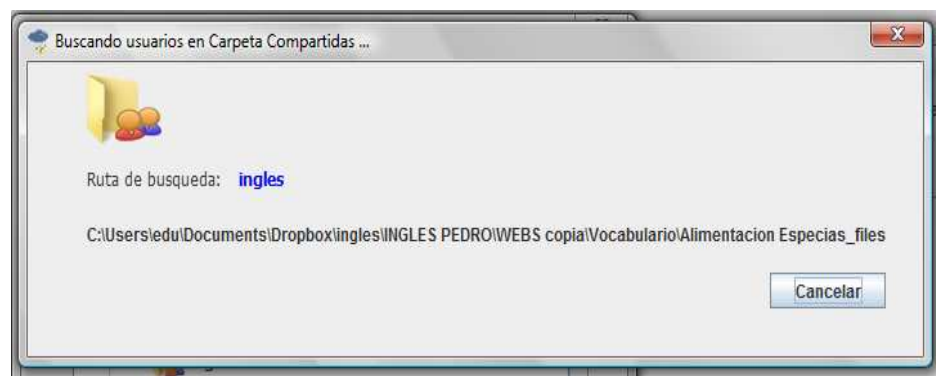


Figura 107: Ventana de búsqueda de nuevos usuarios en carpetas compartidas.

Cuando este proceso termine, el formulario con los nuevos usuarios encontrados aparecerá y el usuario de sesión podrá escoger los usuarios que desea agregar a la agenda.

5.7.7.4. Eliminar usuario de la agenda

La única opción para eliminar a un usuario de la agenda es desde la opción eliminar usuario de la agenda del formulario ver usuarios de la agenda (ver apartado 5.7.7.1).

En este caso, un usuario será eliminado con toda su información, alias y carpetas compartidas a las que pertenece, hasta que sea dado de alta nuevamente por el usuario de la sesión.

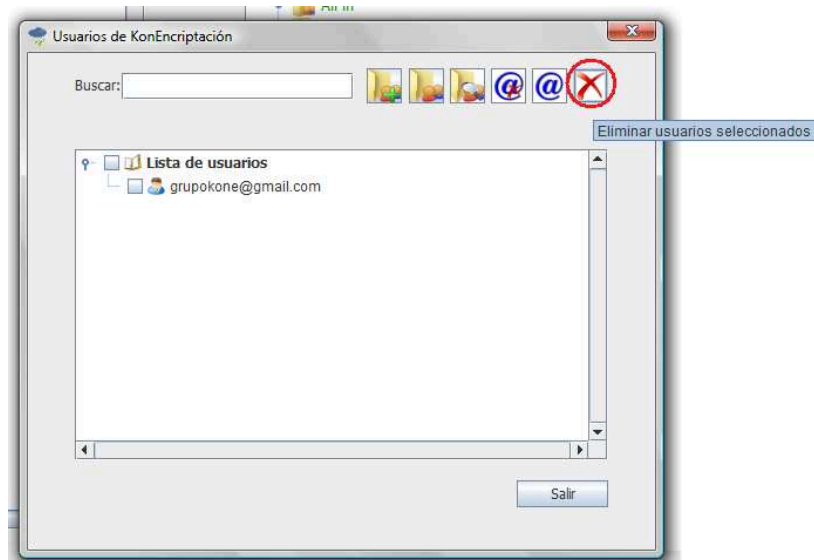


Figura 108: Opción eliminar usuario de la agenda del formulario ver usuarios de agenda.

5.7.7.5. Editar el alias de un usuario

La única opción de editar el alias de un usuario de la agenda es desde la opción editar alias del formulario ver usuarios de la agenda (ver apartado 5.7.7.1).

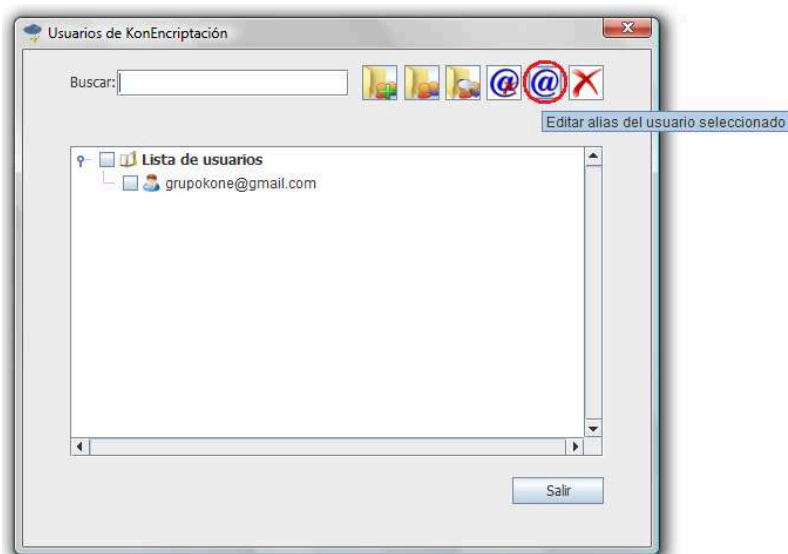


Figura 109: Opción editar usuario de la agenda del formulario ver usuarios de agenda.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Una vez pulsada esa opción, el formulario para poder editar el alias del usuario aparecerá. El usuario de la sesión deberá introducir el alias que desea darle al usuario y guardarlo mediante la opción aceptar.

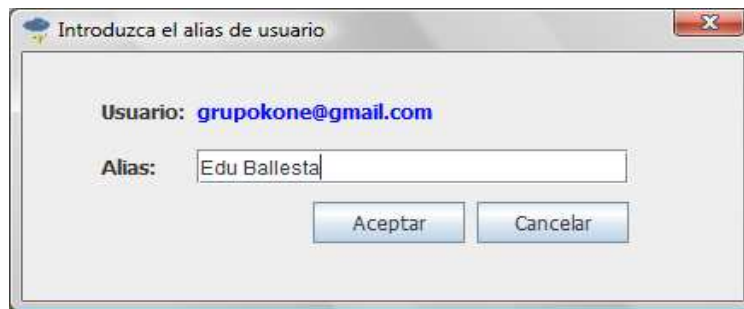


Figura 110: Ventana para introducir alias del usuario.

Cuando se haya introducido el alias, este se mostrará de color azul en los formularios:

- Ver carpetas compartidas.
- Ver usuarios de la agenda.
- Agregar peticiones de acceso.

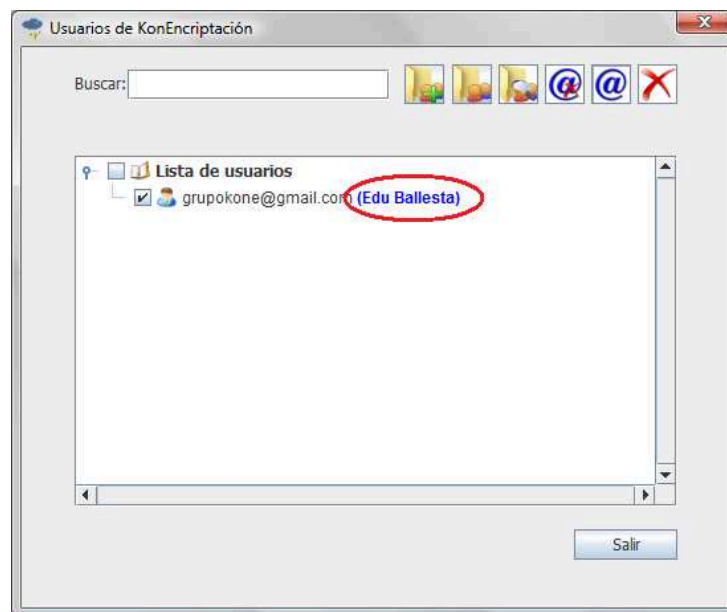


Figura 111: Ventana ver usuarios de la agenda. Edu Ballesta es el alias de grupokone@gmail.com.

5.7.7.6. Eliminar el alias de un usuario

La única opción para eliminar el alias de un usuario de la agenda es desde la opción editar alias de un usuario de la agenda del formulario ver usuarios de la agenda (**ver apartado 5.7.7.1**).

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

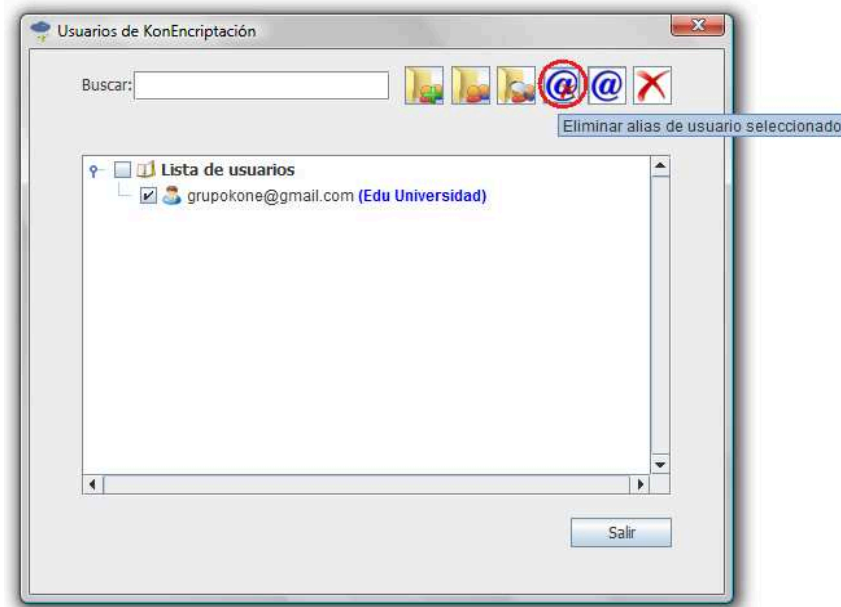


Figura 112: Opción eliminar usuario de la agenda del formulario ver usuarios de agenda.

El usuario deberá seleccionar a un usuario que contenga un alias y pulsar la opción eliminar alias. Inmediatamente, el alias asociado al usuario seleccionado desaparecerá.

5.7.7.7. Asociar un usuario a una carpeta compartida

Mediante esta opción, el usuario de sesión asocia a uno o varios usuarios que están almacenados en la agenda o que van a serlo con las carpetas compartidas que existen actualmente en el sistema.

Hay varias formas de asociar a un usuario con una carpeta compartida:

- Menú agenda de usuarios → Opción asociar usuarios de la agenda a carpetas compartidas del menú contextual de los directorios local o remoto de KonEncriptación.
- Asociar usuarios de la agenda a carpetas compartidas del menú agenda de usuarios de KonEncriptación.
- Buscar nuevos usuarios en el formulario de ver peticiones de acceso pendientes del **apartado 5.7.6.3**.
- Buscar nuevos usuarios en el formulario de combinar peticiones de acceso del **apartado 5.9.4**.
- Opción asociar usuarios a carpetas compartidas de la ventana ver usuarios de la agenda del **apartado 5.7.7.1**.
- Opción asociar usuarios a carpetas compartidas de la ventana ver carpetas compartidas de la agenda del **apartado 5.7.7.2**.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

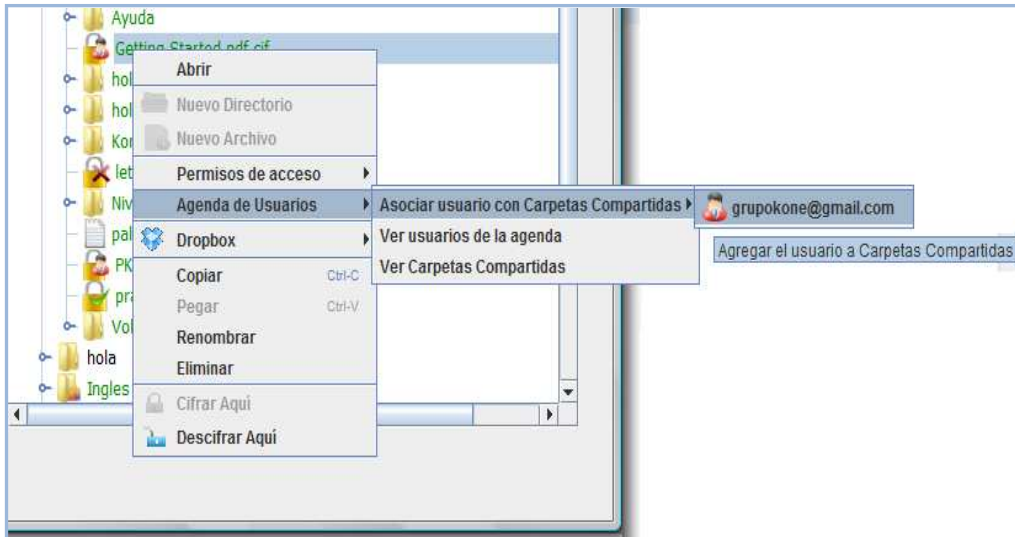


Figura 113: Opción asociar usuario a carpeta compartida del menú contextual remoto.

5.7.7.8. Desasociar un usuario de una carpeta compartida de Dropbox

El usuario de sesión puede desasociar (eliminar) de una carpeta a uno o varios usuarios que forman parte de esa carpeta.

La opción para desasociar a un usuario de una carpeta compartida se puede realizar desde:

- Opción eliminar usuario en ver agenda de usuarios (**ver apartado 5.7.7.1**).
- Opción desasociar un usuario de una carpeta compartida (**ver apartado 5.7.7.2**).

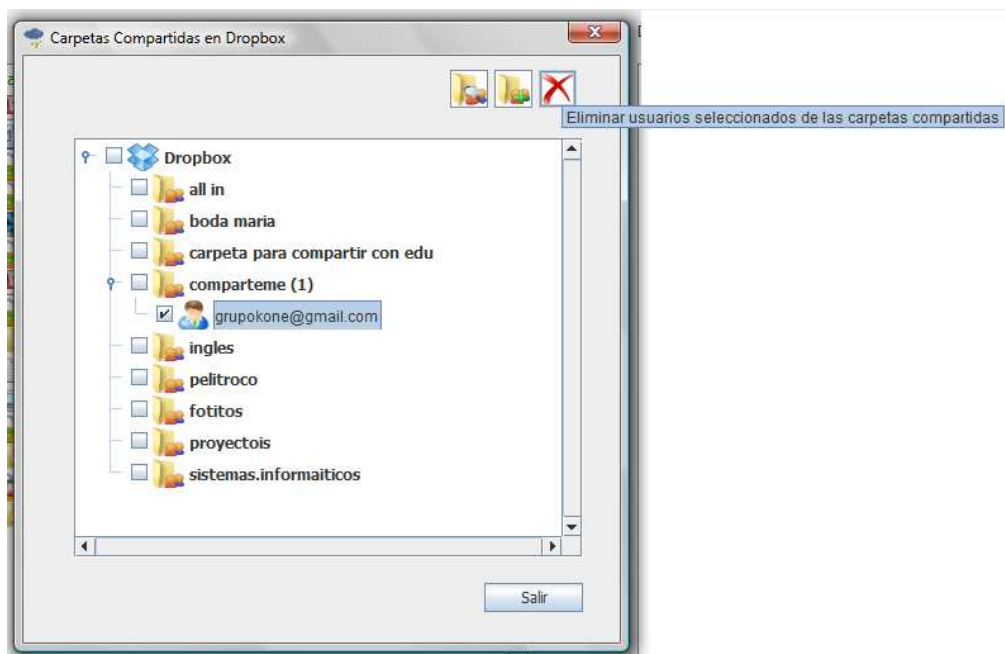


Figura 114: Desasociar un usuario de una carpeta compartida desde el formulario ver carpetas compartidas.

5.7.7.9. Agregar usuarios desde la agenda a los formularios de edición de peticiones de acceso pendientes

Tanto en las opciones para ver las peticiones de acceso pendientes de un archivo (**apartado 5.7.6.3**) como en la de combinar peticiones de acceso de archivos cifrados (**apartado 5.7.4.**), los usuarios de la agenda pueden ser insertados dentro del árbol provisional de permisos de acceso generado en ambas opciones para que puedan formar parte así, en estado de validado, de los usuarios que tendrán acceso a dicho archivo.

El tratamiento de estos usuarios será distinto a los que ya aparecen en la ventana como usuarios propios del archivo, puesto que se le permitirá al usuario eliminarlos de dicho árbol (**ver apartado 5.7.7.10**) y solo se guardarán en el archivo cifrado en estado validado una vez que el usuario procese las peticiones.

Al pulsar la opción agregar usuarios al árbol de peticiones desde la agenda de usuarios la ventana que aparecerá será la siguiente:

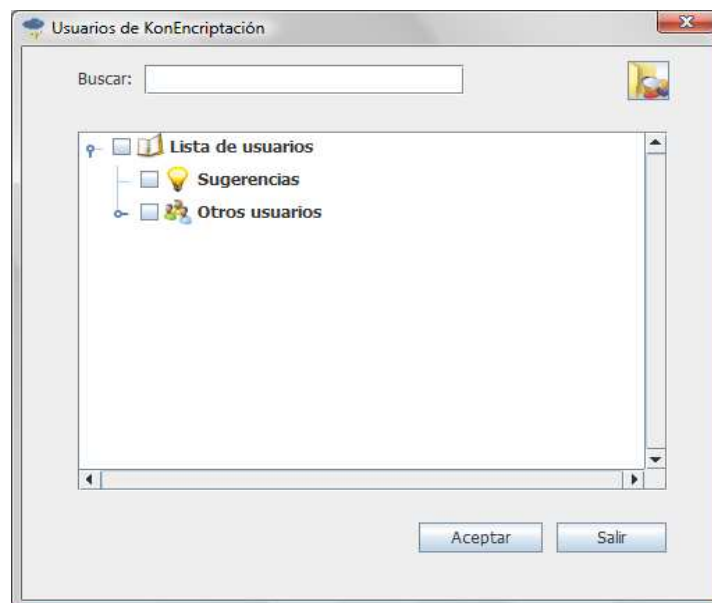


Figura 115: Ventana para agregar usuarios desde la agenda a los formularios de edición de peticiones de acceso pendientes.

Los iconos que se aprecian en el árbol de usuarios en esta ventana tienen el siguiente significado:



Raíz de la agenda de usuarios.



Sugerencias: Indica si los usuarios están asociados a las carpetas compartidas donde pertenece el archivo cifrado, si este pertenece a alguna carpeta compartida.



Otros Usuarios: Indica el resto de usuarios que no pertenecen la carpeta compartida donde se encuentra el archivo cifrado.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Las únicas operaciones que se pueden realizar en esta ventana son las siguientes:



Buscar nuevos usuarios en carpetas compartidas ([ver apartado 5.7.7.3](#)).

Buscar usuarios *por alias y por nombre* en el árbol de usuarios.

Los usuarios que estén en el árbol de peticiones de acceso desde donde se ha llamado a esta opción ([ver apartados 5.7.6.3 y 5.9.4](#)), no aparecerán en esta nueva ventana. Cuando el usuario de sesión seleccione a uno o varios usuarios y pulse el botón aceptar, estos usuarios se añadirán al ventana de peticiones de acceso desde donde fue llamado esta opción.

5.7.7.10. Eliminar usuarios insertados desde la agenda a los formularios de edición de peticiones de acceso pendientes

Tanto en el formulario para ver peticiones de acceso pendientes ([apartado 5.7.6.3](#)) como en el de combinar cabeceras de archivos cifrados ([apartado 5.9.4](#)), los usuarios insertados desde la agenda pueden ser eliminados (quitados de la cabecera provisional) por el usuario de la sesión antes de que estas sean procesadas.

5.7.7.11. Agregar usuarios de la agenda como validados a un archivo cifrado

Uno o varios usuarios pueden ser insertados directamente en estado validado a un archivo cifrado desde la agenda de usuarios. El usuario de sesión podrá realizar esta opción desde:

- Menú archivos → Permisos de acceso → Usuarios → Agregar usuarios validados ...
- Botón derecho → Permisos de acceso → Usuarios → Agregar usuarios validados (menú contextual del directorio local o remoto). Se debe tener seleccionado un archivo cifrado.

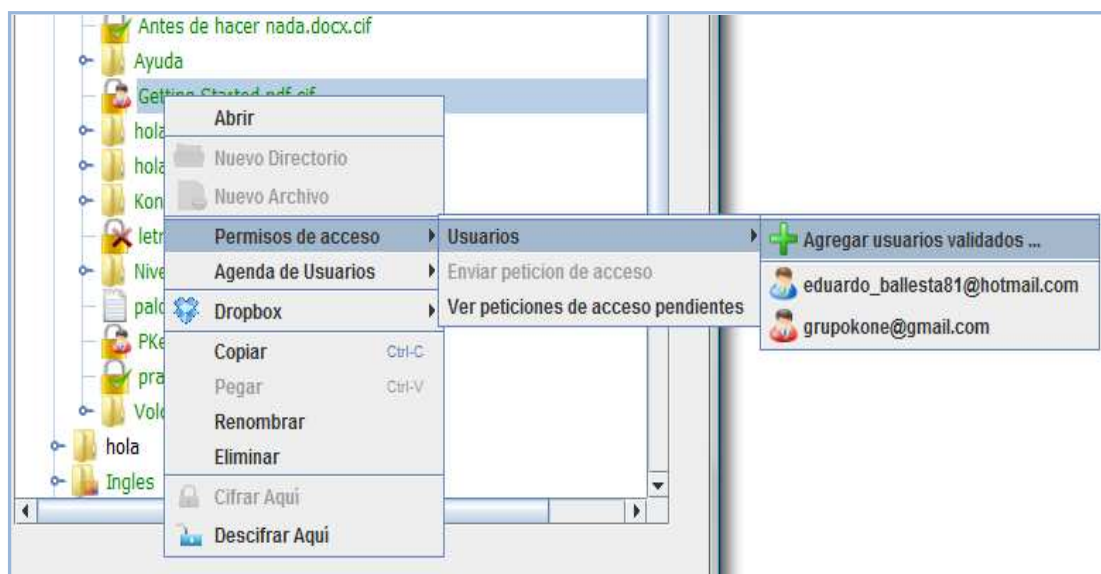


Figura 116: Opción agregar usuarios validados del menú contextual del directorio remoto.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Al pulsar el botón de **Agregar usuarios validados...** la ventana que aparecerá será la siguiente:

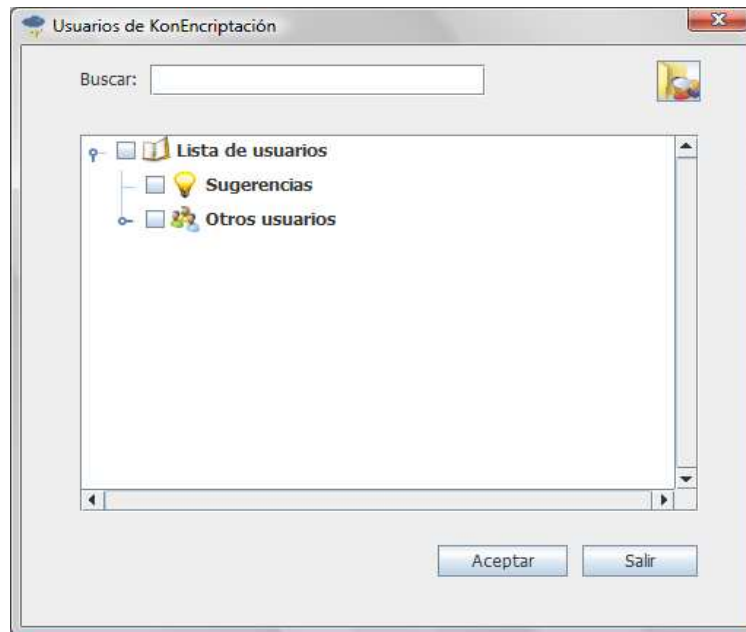


Figura 117: Ventana para agregar usuarios desde la agenda a formularios con peticiones de acceso pendientes.

Los iconos que se aprecian en el árbol de usuarios de la ventana tienen el siguiente significado:



Raíz de la agenda de usuarios.



Sugerencias: Indica si los usuarios están asociados a las carpetas compartidas donde pertenece el archivo cifrado en el caso de estarlo.



Otros Usuarios: Indica el resto de usuarios que no pertenecen la carpeta compartida donde se encuentra el archivo cifrado.

Las operaciones que se puede realizar en esta ventana son las siguientes:



Buscar nuevos usuarios en carpetas compartidas (**ver apartado 5.7.7.3**).

Buscar usuarios por alias y por nombre en el árbol de usuarios.

En esta ventana no aparecerán los usuarios que ya estén validados en el archivo cifrado. Cuando el usuario de sesión seleccione a uno o varios usuarios y pulse el botón aceptar, dichos usuarios serán añadidos al archivo cifrado en estado validado.

5.7.7.12. Ver las carpetas asociadas con los usuarios de la agenda.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Si el usuario de sesión desea conocer qué carpetas compartidas están asociadas a uno o varios usuarios de la agenda, sólo podrá hacerlo desde la opción ver carpetas asociadas a los usuarios de la agenda del formulario ver usuarios de la agenda (**apartado 5.7.7.1**).

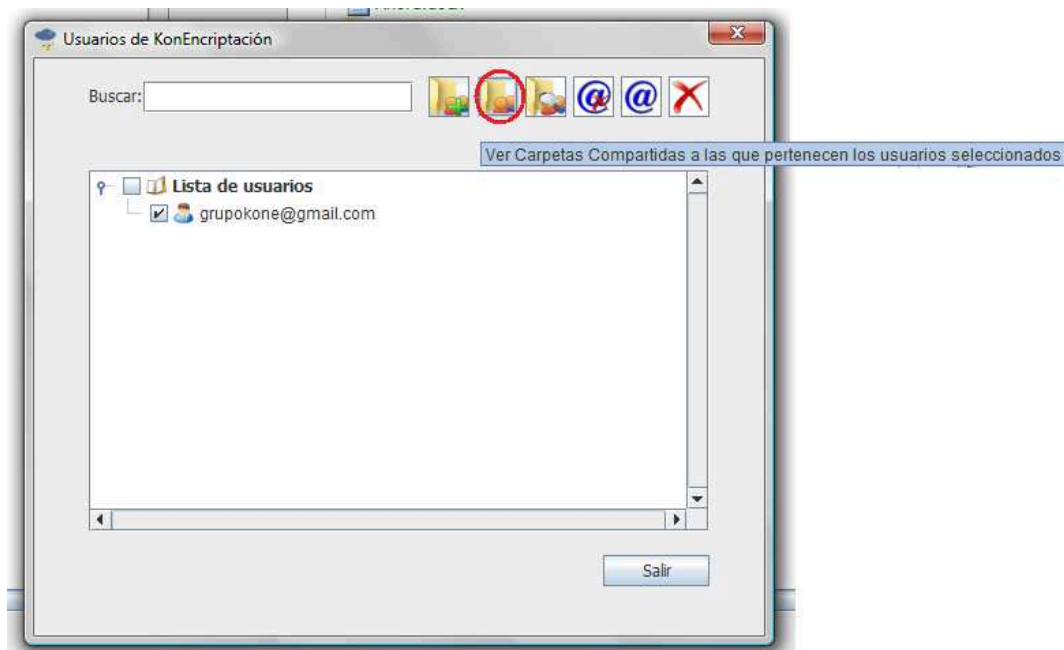


Figura 118: Opción ver carpetas asociadas a los usuarios del formulario ver usuarios de la agenda.

Al pulsar esta opción aparecerá la ventana de ver carpetas compartidas mostrando sólo las carpetas compartidas donde forman parte los usuarios seleccionados en el formulario ver usuarios de la agenda.

5.8. Operaciones integradas de Dropbox

En este apartado, se van a describir las operaciones que se pueden realizar desde la barra de herramientas integrada de *Dropbox*.

5.8.1. Navega al sitio web de Dropbox

Esta opción permite explorar el archivo o directorio seleccionado dentro del directorio remoto en el sitio web de *Dropbox*.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

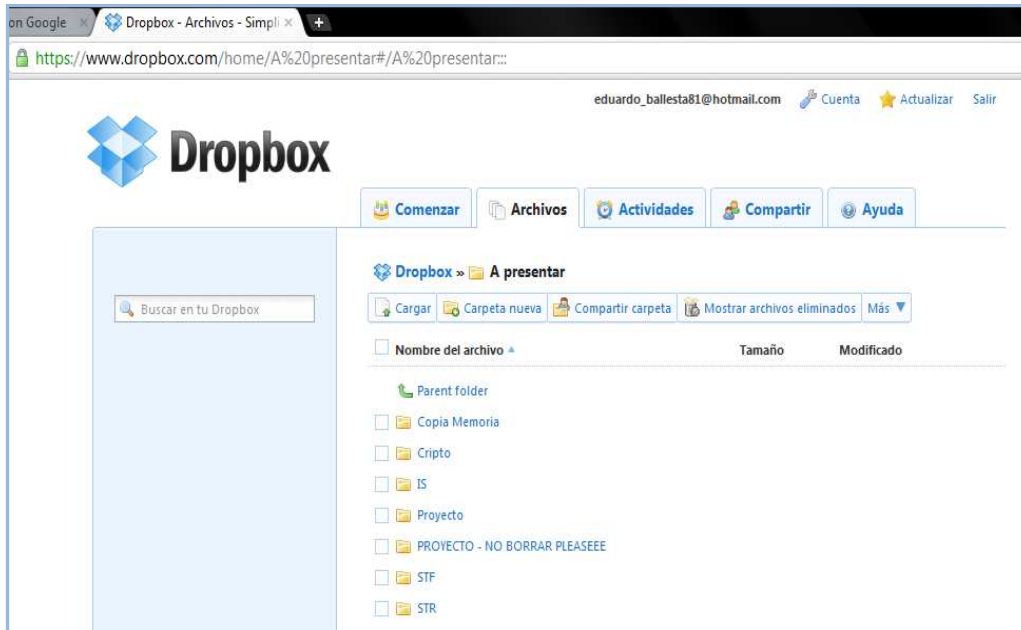


Figura 119: Ventana mostrada en el navegador después de pulsar ir al sitio Web del directorio **A presentar**

Existen dos formas de realizar esta operación:

- Menú *Dropbox* → Opción Navega el sitio web de *Dropbox* → (menú principal).
- Botón derecho → *Dropbox* → Opción navega el sitio web de *Dropbox* (menú contextual del directorio remoto).



Figura 120: Opción navega el sitio web de *Dropbox* de la barra de herramientas de *Dropbox*

5.8.2. Copiar enlace público

Esta opción permite compartir un archivo que se encuentre dentro del directorio *Public* mediante una URL generada automáticamente. Para ello se debe seleccionar un archivo dentro de dicho directorio o un subdirectorio de éste y pulsar esta opción.

La URL obtenida puede ponerse en conocimiento de otros usuarios para que tengan acceso al archivo. Cabe mencionar que si dichos usuarios no usan KonEncriptación el archivo no debería estar cifrado.

Esta opción estará disponible si el usuario de sesión la ha activado previamente ([ver apartado 5.8.6.](#)).

Para realizar esta opción existen dos formas de hacerlo:

- Menú *Dropbox* → Opción copiar enlace público de *Dropbox* → (menú principal).
- Botón derecho → *Dropbox* → Opción copiar enlace público (menú contextual del directorio remoto).



Figura 121: Opción copiar enlace público de la barra de herramientas de Dropbox

5.8.3. Ver versiones anteriores

Permite ver el historial de modificaciones de un archivo y revertirlo a una versión anterior si el usuario lo desea. Cuando el usuario ejecuta esta opción, se abre el portal web de *Dropbox* para mostrar el listado de versiones del archivo seleccionado.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.



Figura 122: Ventana mostrada en el navegador después pulsar la opción Ver versiones anteriores del archivo Ahora.docx

Para realizar esta opción existen dos formas de hacerlo:

- Menú *Dropbox* → Opción ver versiones anteriores de *Dropbox* → (menú principal).
- Botón derecho → *Dropbox* → Opción ver versiones anteriores (menú contextual del directorio remoto).

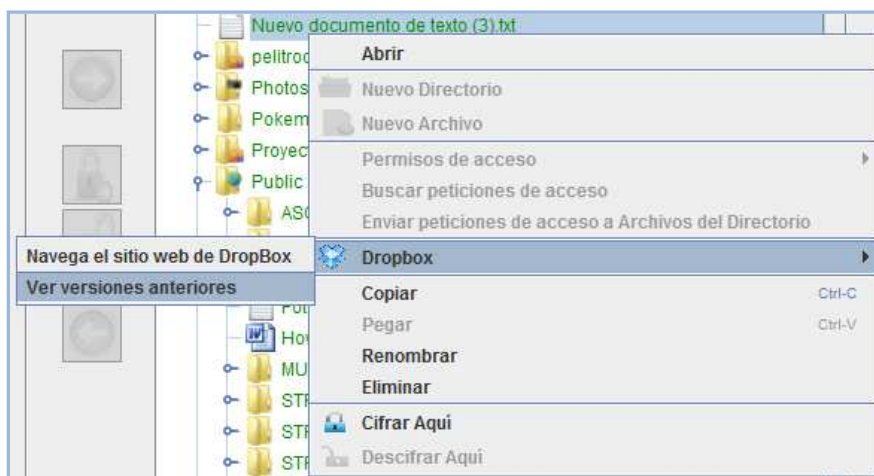


Figura 123: Opción ver versiones anteriores de la barra de herramientas de Dropbox

5.8.4. Compartir esta carpeta

Opción para invitar a otros usuarios amigos a acceder a una carpeta en *Dropbox*. Esa carpeta y su contenido aparecerán también en sus carpetas de *Dropbox* una vez que haya aceptado la invitación. Cuando se selecciona esta opción se abrirá el portal web directamente por la opción compartir esta carpeta.

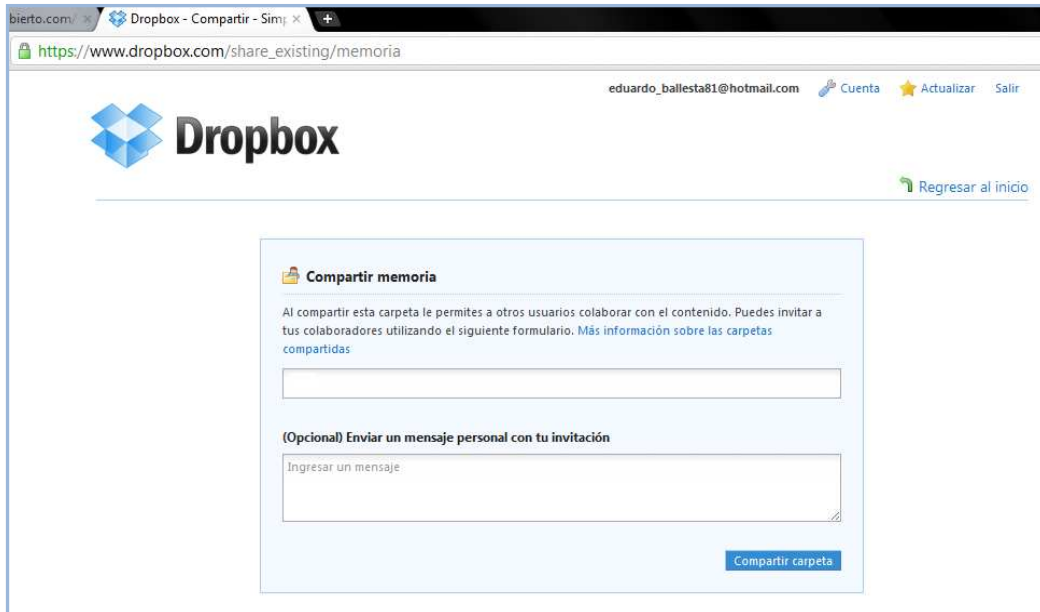


Figura 124: Ventana del navegador después pulsar compartir esta carpeta en el Directorio *memoria*

Para realizar esta opción existen dos formas de hacerlo:

- Menú *Dropbox* → Opción compartir esta carpeta de *Dropbox* → (menú principal).
- Botón Derecho → *Dropbox* → Opción compartir esta carpeta (menú contextual del directorio remoto).

Existen varias restricciones para esta opción:

- No se puede compartir la carpeta de *Dropbox*.
- Si se comparte una carpeta, los directorios de niveles superiores o niveles inferiores a esta no podrán ser compartidos.

Nota: esta opción en plataformas Linux puede que no funcione correctamente en algunas ocasiones debido a que el archivo de configuración de donde se extraen la lista de carpetas compartidas almacena las rutas en minúscula y Linux, tiene sensibilidad a las minúsculas y mayúsculas para los nombres de archivos y directorios.

5.8.5. Copiar el enlace de la galería pública

Esta opción permite compartir una carpeta de fotos (*galería*) que se encuentre dentro del directorio *Photos* mediante la URL generada en el portal web de *Dropbox*. Debido a los motivos descritos en el [apartado 4.1.5](#), la URL no podrá ser creada automáticamente desde KonEncriptación sino que el usuario deberá obtenerla desde el portal web de *Dropbox*. Para ello se debe haber seleccionado una

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

carpeta dentro del directorio *Photos* o dentro de un subdirectorio de este y posteriormente escoger esta opción. Es necesario tener acceso a Internet para poder realizar esta opción.

La URL obtenida puede ponerse en conocimiento de otros usuarios para que tengan acceso a la galería de fotos compartida y ver así su contenido. Cabe mencionar que si dichos usuarios no usan KonEncriptación los archivos contenidos por la galería no deberían estar cifrados.

Esta opción está disponible siempre que el usuario de sesión la haya activado previamente (**ver apartado 5.8.6**).

Para realizar esta opción existen dos formas de hacerlo:

- Menú *Dropbox* → Opción copiar el enlace de la galería pública → (menú principal).
- Botón Derecho → *Dropbox* → Opción copiar el enlace de la galería pública (menú contextual del directorio remoto).

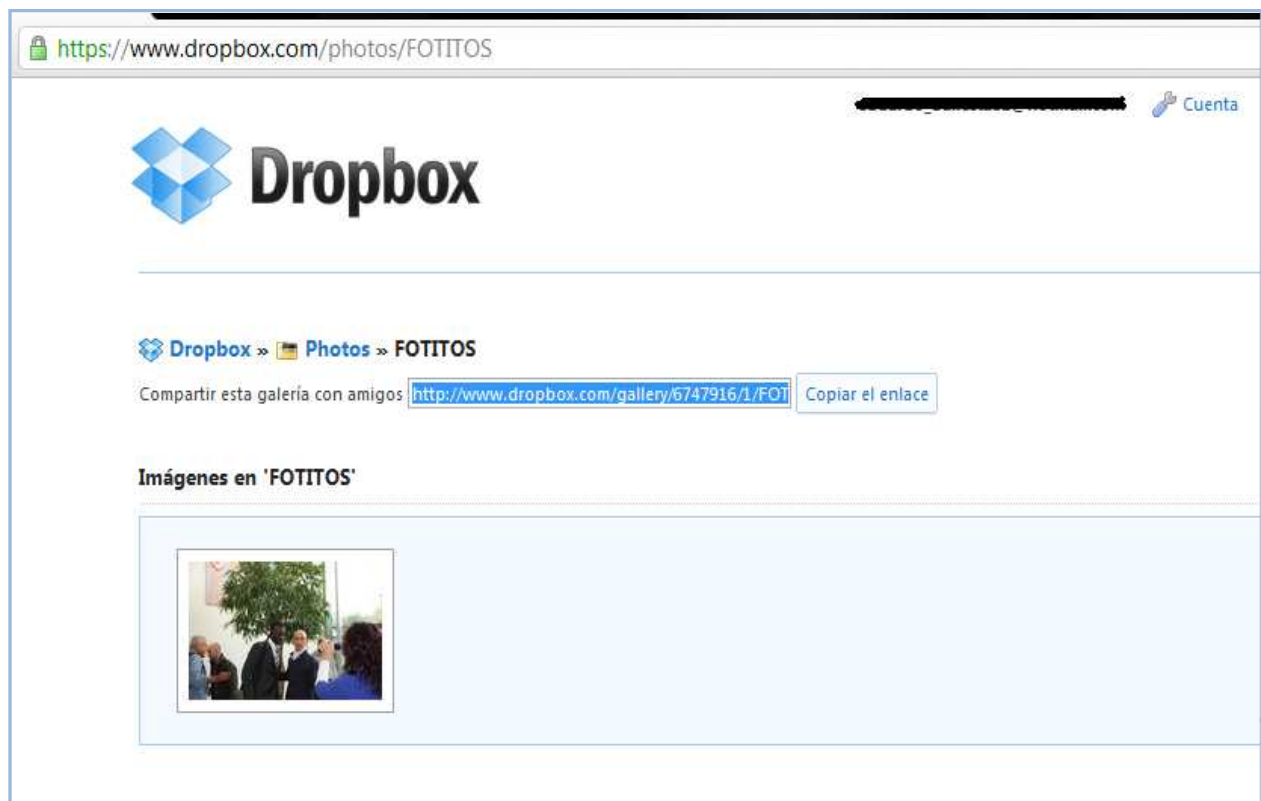


Figura 125: Forma de crear un enlace para la galería de fotos mediante el portal web de Dropbox.

5.8.6. Activar opción copiar enlaces públicos de Dropbox

Permite al usuario de KonEncriptación activar la opción de copiar enlaces públicos de *Dropbox* (**apartado 5.8.2**) introduciendo el número de usuario correspondiente a la cuenta de *Dropbox*.

Para realizar esta opción hay que ir a:

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Menú Inicio → Activar opción crear link público → Opción introducir número de usuario (menú principal).

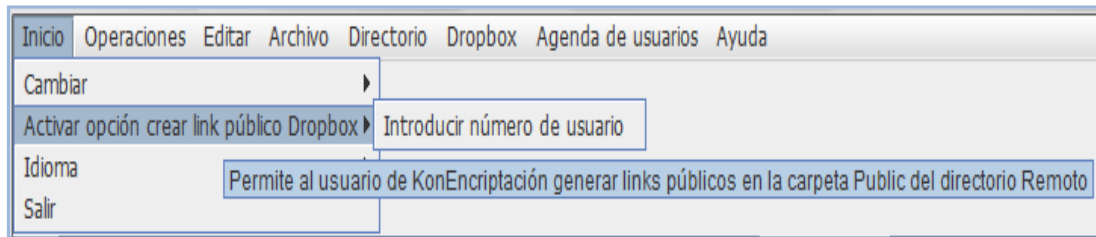


Figura 126: Opción del Menú inicio para activar la opción de link público de Dropbox.

Una vez escogida la opción introducir número aparecerá un formulario donde se deberá introducir el número de usuario de la cuenta de *Dropbox*. Para terminar este proceso el usuario tendrá que pulsar el botón guardar para que KonEncriptación pueda generar los enlaces públicos.

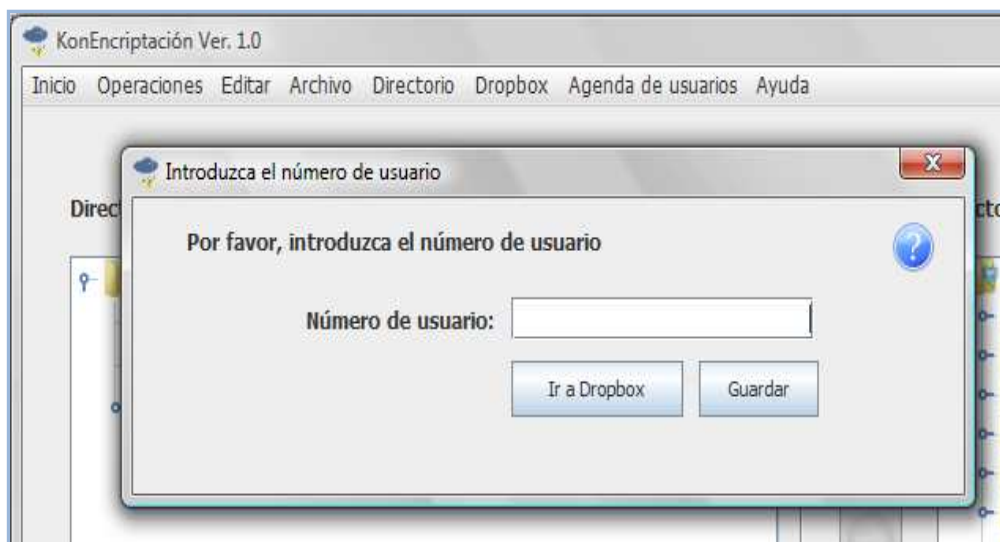


Figura 127: Formulario para cambiar el número de usuario actualmente utilizado para generar enlaces públicos.

El botón **Ir a Dropbox** de esta ventana abrirá el portal web por la carpeta *Public* para que el usuario pueda generar un enlace público y extraer el número de usuario.

El **icono de ayuda** le explica al usuario de sesión qué es el número de usuario y de dónde extraerlo. El número de usuario es el número que aparece cuando creamos un enlace público en *Dropbox*. Podemos obtenerlo de diferentes maneras.

- Ir a la carpeta *Public* de *Dropbox* desde el portal web y seleccionar un archivo. Seleccionar la opción copiar enlace público y este se mostrará en una pequeña ventana.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

- Ir a la carpeta *Public* desde el explorador de archivos de *Dropbox*, y generar un enlace público. Al pegar este enlace en un editor de texto encontraremos un número como el de la siguiente Figura:



Figura 128: Ventana para extraer el número de usuario desde la aplicación Web de Dropbox.

5.8.7. Cambiar número usuario

Permite al usuario de sesión cambiar el número de usuario asociado a su cuenta de *Dropbox*. Esta operación es útil en los casos donde el usuario de sesión se haya equivocado al introducir dicho número.

Para realizar esta opción hay que ir a:

- Menú inicio → Activar opción crear link público → Opción cambiar número de usuario (menú principal).

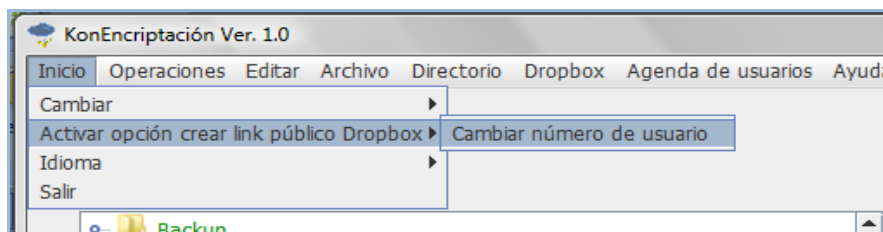


Figura 129: Opción del Menú Inicio para cambiar el numero de usuario.

Una vez pulsada la opción aparecerá un formulario donde se deberá introducir el nuevo número de usuario de la cuenta de *Dropbox*. Para terminar el proceso se deberá pulsar el botón guardar y *KonEncriptación* comenzará a utilizar este nuevo valor cuando genere nuevos enlaces públicos.

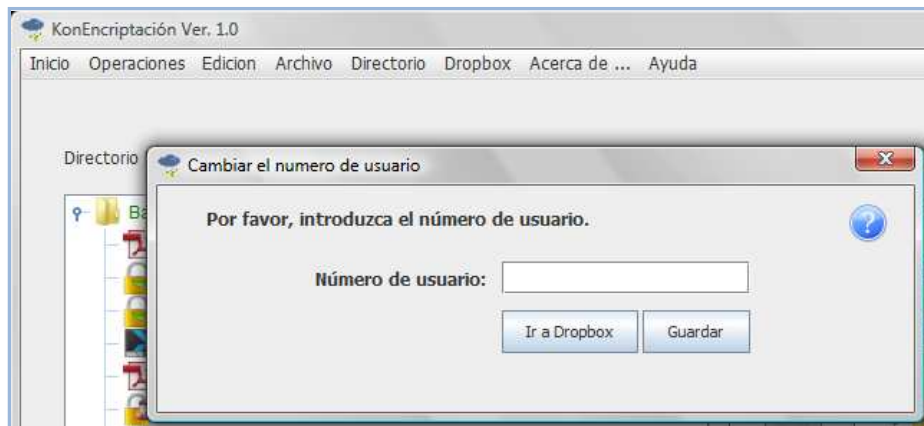


Figura 130: Formulario para cambiar el número de usuario actualmente utilizado para generar enlaces públicos.

El **botón Ir a Dropbox** de esta ventana abrirá el portal web por la carpeta *Public* para que el usuario pueda generar un enlace público y extraer el número de usuario.

El **icono de ayuda** le explica al usuario de sesión qué es el número de usuario y de dónde extraerlo (**ver apartado 5.8.6**).

5.9. Otras Operaciones

En este apartado se describirán operaciones que aseguran el buen funcionamiento de KonEncriptación durante su ejecución, la gestión de reemplazo de archivos y la combinación de directorios.

5.9.1. Control de cambio de usuario asociado a la cuenta de Dropbox

Como se indica en el **apartado 5.4.1.1** el usuario registrado en KonEncriptación y el de *Dropbox* tienen que ser el mismo obligatoriamente. Si se cambia la cuenta de usuario asociada a *Dropbox* mientras que KonEncriptación está ejecutándose la herramienta inmediatamente se percatará de que ambas cuenta no coinciden y forzará el cierre de la sesión tras mostrar un mensaje de error.

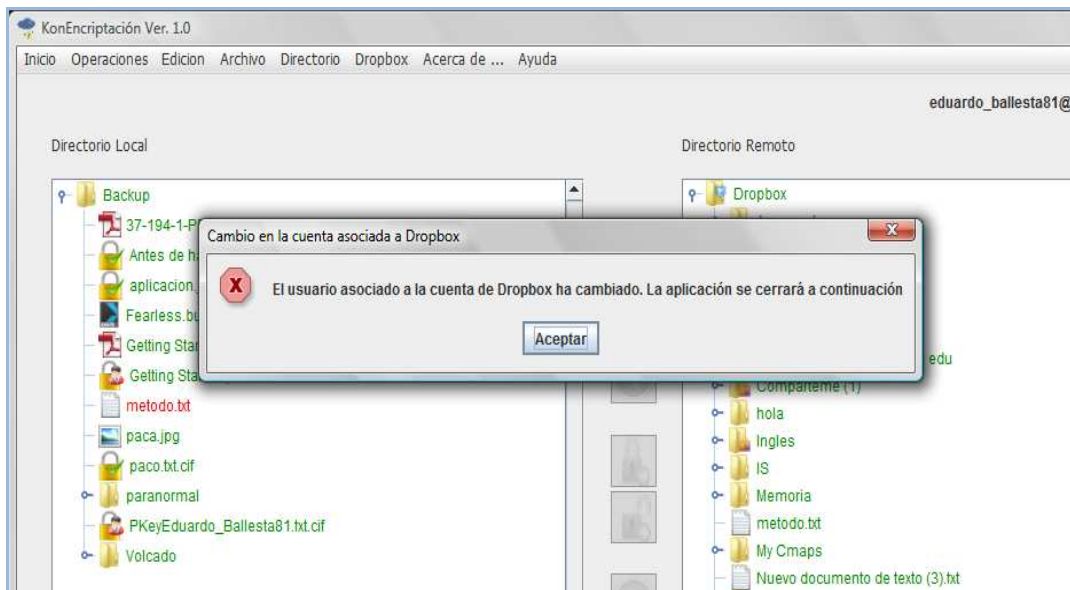


Figura 131: Mensaje de aviso de cambio de usuario mientras se ejecuta KonEncriptación.

5.9.2. Control de ediciones externas a KonEncriptación de los directorios raíz local y virtual

Los directorios local y remoto pueden ser editados durante la ejecución de KonEncriptación. Si estos directorios son eliminados o renombrados desde el explorador de archivos del sistema operativo, KonEncriptación lo detectará inmediatamente y se percata de que alguno de los directorios local o remoto ya no existe y forzará el cierre de la sesión tras mostrar un mensaje de error.

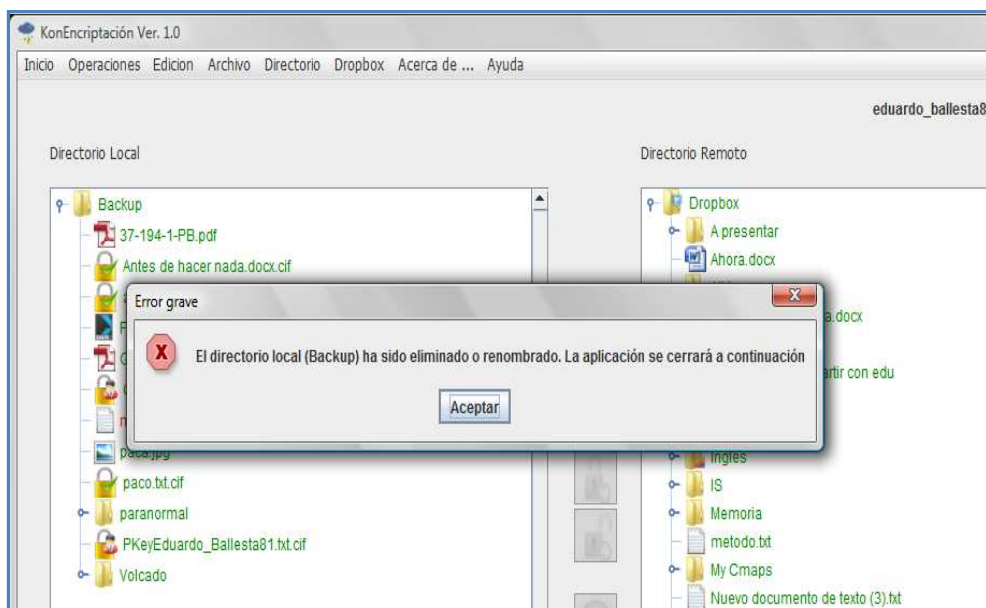


Figura 132: Mensaje de aviso de eliminación del directorio local durante la ejecución de KonEncriptación.

5.9.3. Actualización en tiempo real de los directorios

Los directorios local y remoto tienen que estar en continua concordancia con la información que contienen los directorios que muestran. Para ello, cada edición que suceda en los archivos y subdirectorios es reflejada en tiempo real.

5.9.4. Ventana de aviso en caso de reemplazo de archivo

Cuando se realizan alguna de las operaciones descritas en los apartados 5.6 y 5.7 con archivos de cualquier tipo, existen ocasiones donde los usuarios de KonEncriptación se van a encontrar con situaciones donde una ventana de aviso les indica que ya existe un archivo con el mismo nombre en el directorio destino y tendrá que decidir qué hacer.

Como se aprecia en la **Figura 133**, existen diferentes características a describir:

- La ventana de aviso va a estar formada por la parte del archivo original, la del archivo que se va a reemplazar y la del archivo cifrado o en claro dependiendo de qué tipo sea el original.
- Cada archivo tiene una descripción de sus propiedades (*Nombre, ruta, tamaño y fecha de modificación*).
- Existen entradas en rojo en los archivos original y a reemplazar que le indican al usuario qué archivo es más reciente. Cabe la posibilidad de que la ventana indique que tienen la misma fecha.
- Si el usuario quiere ver el contenido de los archivos antes de decidirse por la operación a realizar puede hacer clic sobre los iconos de los tipos de archivo y estos se abrirán con su aplicación correspondiente. Los archivos cifrados se descifrarán para poder ver su contenido.



Figura 133: Ventana de aviso de reemplazo de archivos.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Puede ocurrir que el archivo en claro o cifrado no exista y un mensaje aparecerá indicándoselo como sucede en la siguiente Figura:

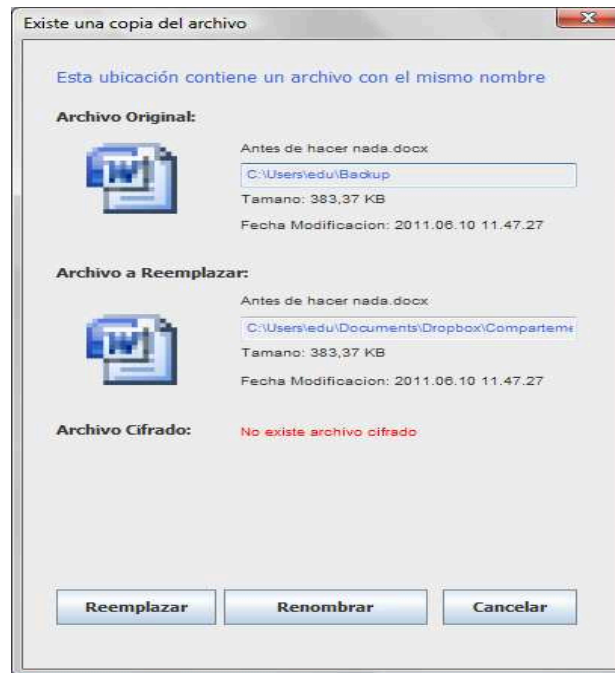


Figura 134: Ventana de aviso de reemplazo de archivo donde aparece el archivo original, el archivo a reemplazar y pero no existe el archivo cifrado.

Existen tres operaciones que el usuario de la sesión puede realizar llegado el caso:

- **Reemplazar:** se elimina el archivo del destino.
- **Renombrar:** se genera un nombre nuevo con formato: **copia +nombre + número** y se mantienen ambos archivos.
- **Cancelar:** no se realiza la operación.

Es importante indicar que si el archivo origen y el archivo a reemplazar están ambos cifrados la aplicación tendrá en cuenta las restricciones descritas en el **apartado 5.7.6.6**. En ese caso, si un usuario escoge la opción reemplazar de la **Figura 133** y el usuario cumple las restricciones sobre archivos cifrados del **apartado 5.7.6.6**. KonEncriptación pondrá en marcha un proceso de fusión de permisos de ambos archivos. Esta **estrategia de fusión de permisos** es la siguiente:

- Los usuarios que tengan permiso de acceso a alguno de los dos archivos tendrán permiso de acceso en nuevo archivo cifrado generado.
- Los usuarios que no tengan permiso de acceso en ninguno de los dos archivos pero si alguna petición pendiente de aceptar mantendrán este estatus en el nuevo archivo cifrado generado si el usuario no quiere validarlo antes.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Después de realizar esta estrategia de fusión y antes de que se termine la opción de reemplazar el archivo se abrirá una ventana que mostrará el estado final de los permisos de acceso del nuevo archivo que se va a generar.

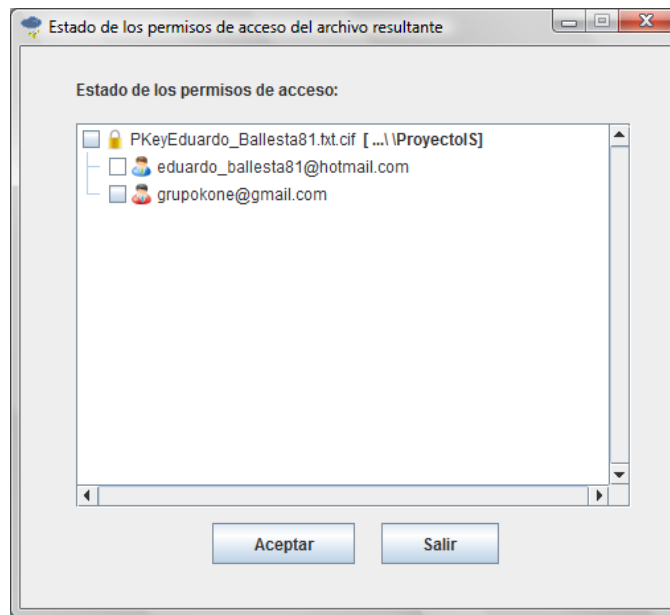


Figura 135: Estado de los permisos de acceso por fusión de permisos de dos archivos cifrados.

El formato de la información presentada será:

- Nombre del archivo cifrado + [...\Ruta hasta el directorio raíz (Local o remoto)]
- Usuarios que van a tener acceso al archivo cifrado (**deshabilitado**).
- Usuarios que van a mantener las peticiones pendientes (**habilitado**).

El usuario de la sesión tendrá la oportunidad de aceptar las peticiones de acceso pendientes que desee antes de que al aceptar se complete la operación de reemplazo.

Para ello deberá seleccionar aquellos usuarios en estado de petición que desea validar. *Los usuarios que estén validados no podrán ser seleccionados* puesto que KonEncriptación ya cuenta con que van a tener acceso al archivo cifrado.

Por otra parte, el usuario tendrá opción de utilizar diferentes opciones de la agenda como insertar usuarios en el árbol de peticiones desde la agenda o insertar en la agenda usuarios que se encuentran en estado de petición. Estas son las opciones que el usuario de sesión podrá realizar:



Eliminar a un usuario de la agenda (**ver apartado 5.7.7.4**).



Asociar usuarios a carpetas compartidas (**ver apartado 5.7.7.7**).



Añadir a un nuevo usuario a la agenda de usuarios (**ver apartado 5.7.7.3**).



Agregar usuarios al árbol de peticiones desde la agenda de usuarios (**ver apartado 5.7.7.9**).

Si el usuario quiere completar la operación de reemplazo del archivo cifrado deberá pulsar el botón aceptar. En caso contrario deberá pulsar el botón salir o cerrar la ventana.

5.9.5. Ventana de aviso en caso de combinación de directorios

Cuando se realizan algunas de las operaciones descritas en los **apartados 5.6 y 5.7** con directorios existen ocasiones donde los usuarios de KonEncriptación se van a encontrar con situaciones donde una ventana de aviso les indique que ya existe el directorio con el mismo nombre dentro del directorio destino y tendrá que decidir qué hacer.

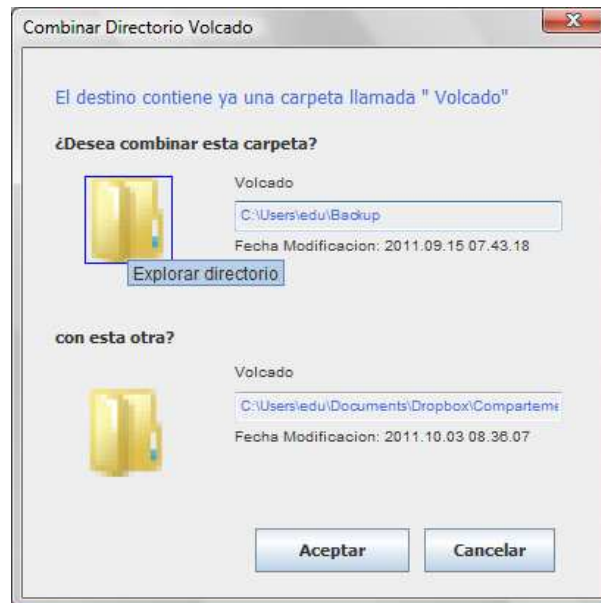


Figura 136: Ventana de aviso de combinación de directorios

Como se aprecia en la **Figura 136** existen diferentes características:

- La ventana de aviso va a estar formada por la parte de la carpeta origen y la del directorio destino donde se va a combinar la información.
- Cada archivo tiene una descripción de sus propiedades (*Nombre, ruta y fecha de modificación*).
- Si el usuario quiere ver el contenido de los directorios antes de decidirse si combinar los directorios puede hacer clic sobre los iconos de ambas carpetas y estas se abrirán con el explorador de archivos de la plataforma en la que se esté trabajando.

Si el usuario quiere combinar los directorios deberá pulsar aceptar. En caso contrario, deberá pulsar la opción cancelar o cerrar la ventana.

5.9.6. Ver propiedades de los Archivos

Si un usuario de sesión quiere ver las propiedades de un archivo (*fecha de modificación y tamaño*) sólo deberá pasar el ratón por encima del archivo deseado y estas propiedades se mostrarán.

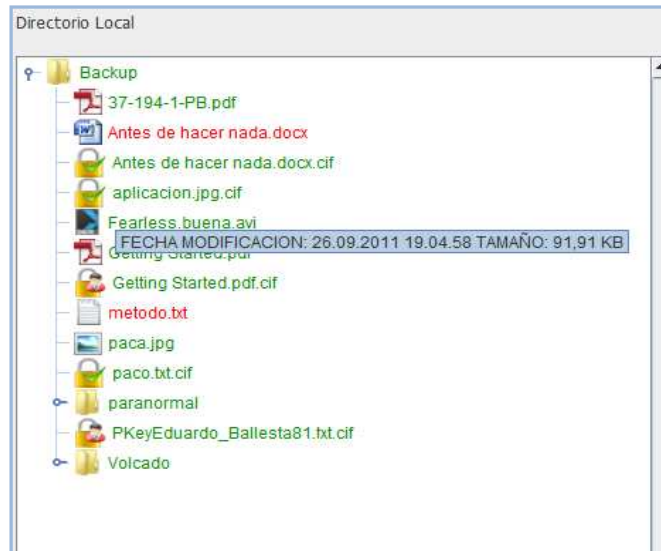


Figura 137: Ver propiedades de un archivo.

5.9.7. Control de versiones

Para el control de versiones entre archivos y directorios se utilizan diferentes colores para indicarle al usuario que la versión del archivo o directorio es más reciente, igual, o más antigua que la que hay dentro del otro directorio (local o remoto). Los colores utilizados son:



El archivo es más antiguo que su copia en la misma ubicación en el otro directorio (remoto o local) .Esta opción no es válida para directorios.



El archivo o directorio es más reciente que su copia en la misma ubicación en el otro directorio (remoto o local). También puede indicar que el archivo o copia no existe en la misma ubicación



El archivo o directorio es el mismo que su copia en la misma ubicación en el otro directorio (remoto o local)

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

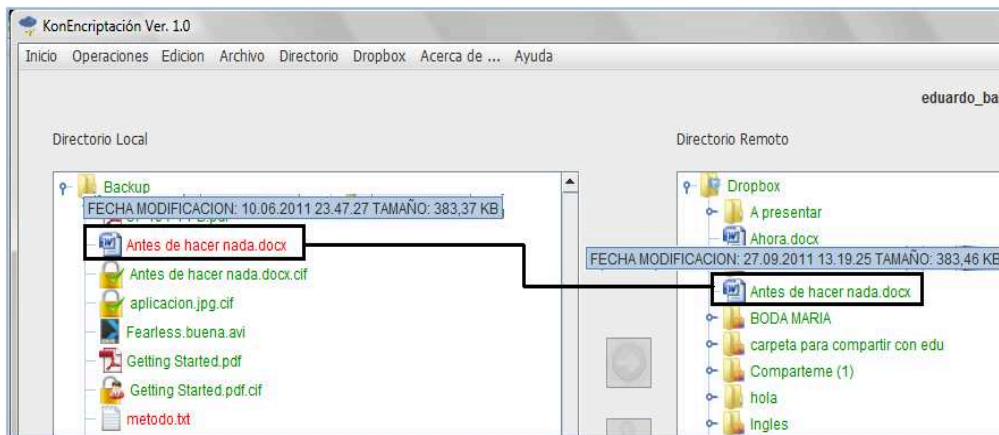


Figura 138: La versión del archivo **Antes de hacer nada.docx** del directorio remoto es más reciente que la copia del directorio local

En la Figura anterior se puede ver como la versión **Antes de hacer nada.docx** del directorio local es más antigua que la que hay dentro del directorio remoto.

5.9.8. Arrastrar Archivos y/o directorios desde una ubicación externa a KonEncriptación

KonEncriptación permite arrastrar archivos y/o directorios desde ubicaciones externas a la herramienta. Por ejemplo, arrastrar desde el Escritorio o desde una carpeta del explorador de archivos. Si alguno de los archivos que se arrastra es cifrado se tendrán en cuenta las restricciones descritas en el [apartado 5.7.6.6](#). En caso de que el archivo o directorio exista en el destino donde se va a realizar la operación las ventanas de aviso de reemplazo de archivos y directorios serán mostradas ([apartado 5.9.4](#) y [5.9.5](#)).

Al igual que el [apartado 5.6.5](#), las operaciones permitidas tras terminar de arrastrar serán las operaciones generales ([apartado 5.6](#)) y dependerán del tipo de archivos y/o directorio arrastrado. Cuando el usuario termine la acción de arrastrar, se mostrará una ventana con las operaciones que se pueden realizar y el usuario deberá escoger la que desea realizar.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

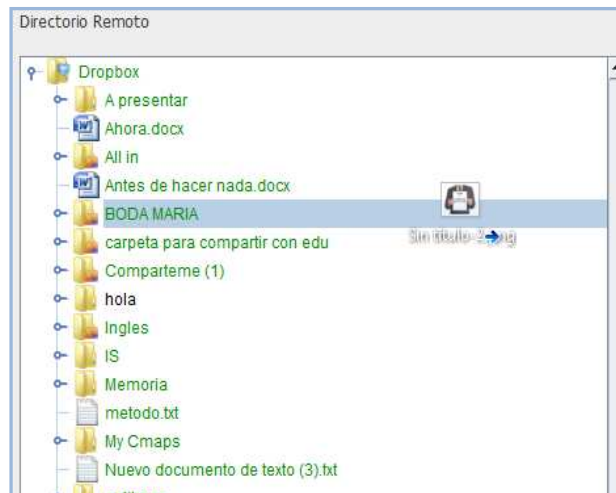


Figura 139: Arrastrar archivo *Sin título -2.jpg* desde una ubicación externa.

5.9.9. Cambio de idioma

El usuario podrá escoger entre los dos idiomas que hay disponibles en KonEncriptación.

- Inglés
- Español

Para ello deberá de hacerlo desde:

Menú Inicio → Idioma → Seleccionar el idioma en el que desea trabajar.

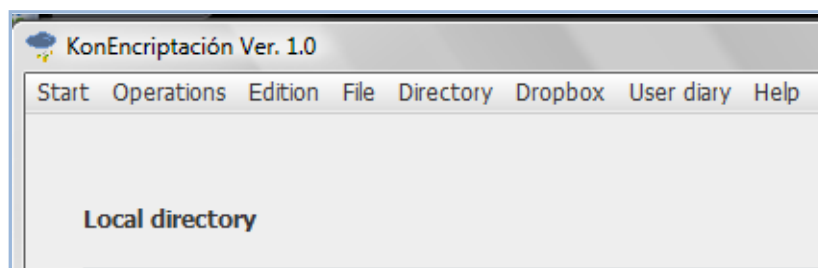


Figura 140: Opción de selección de idioma.

En la figura anterior se muestra el menú de selección de idioma en inglés. Si el usuario quisiera cambiar a español sólo deberá pulsar la opción Spanish e inmediatamente la configuración de KonEncriptación cambiará a español. En caso contrario ocurriría lo mismo.

5.10. Salida de la Aplicación

Existen varias formas para salir de la aplicación:

- Pulsar el botón salir de la parte derecha de la pantalla.
- Ir a menú inicio y pulsar la opción salir.
- Pulsar la tecla de cerrar la ventana del formulario principal de KonEncriptación.
- Pulsar la opción salir de la entrada de la barra de tareas.

5.11. Desinstalación

Si un usuario quiere dejar de hacer uso de KonEncriptación y eliminarlo completamente del equipo donde está trabajando deberá escoger una de las varias opciones de desinstalación que existen:

- Pulsando el botón el acceso directo *uninstall* que hay en el menú inicio de KonEncriptación.
- Pulsando la opción *uninstall.exe* del directorio de instalación de KonEncriptación.
- Desinstalarlo de las opción desinstalar o cambiar programas desde el sistema operativo.

La siguiente imagen muestra una de las opciones descritas para desinstalar KonEncriptación del equipo.

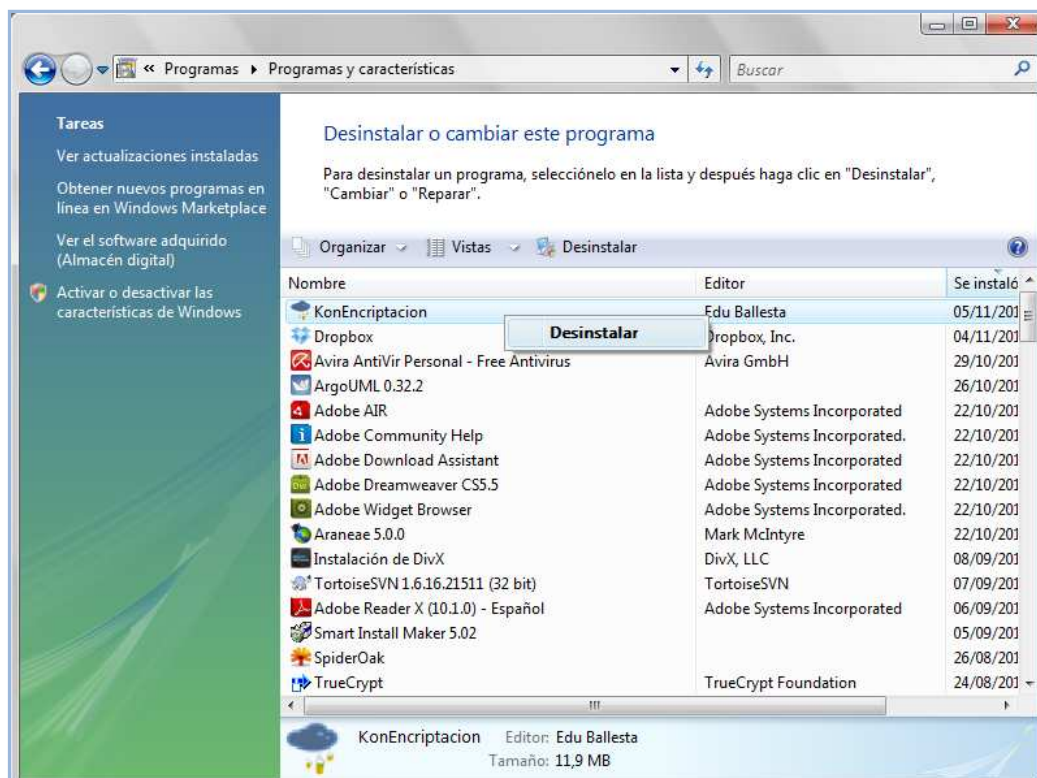


Figura 141: Desinstalar KonEncriptación de la opción desinstalar un software en Windows Vista.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

Una vez seleccionadas alguna de las opciones descritas en el apartado anterior, el asistente de desinstalación comenzará. La primera ventana que aparecerá será la de confirmación de desinstalación de KonEncriptación.

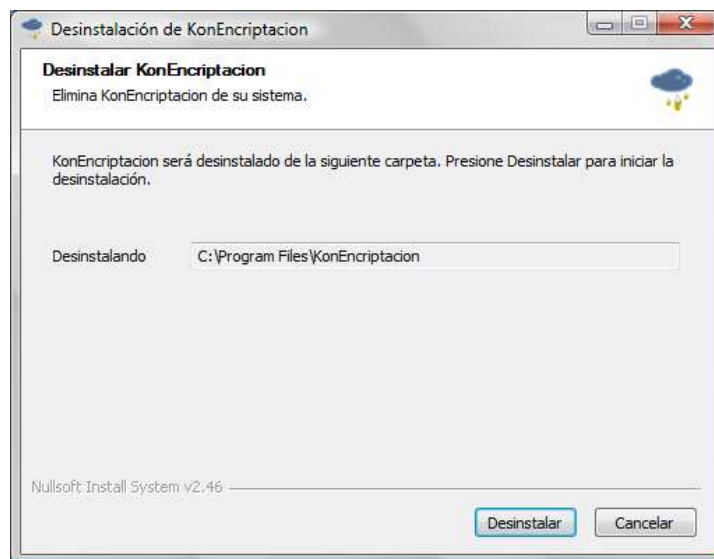


Figura 142: Ventana para desinstalar KonEncriptación.

Una vez pulsada la opción desinstalar el proceso de desinstalación se llevará a cabo. Tanto el directorio donde ha sido instalado como el acceso directo de KonEncriptación serán eliminados en este proceso.

La entrada del menú inicio será eliminada una vez que el usuario haya reiniciado el equipo.

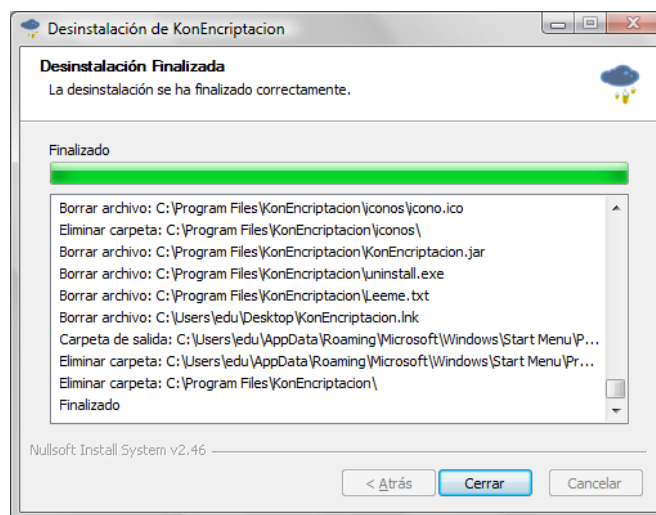


Figura 143: Ventana de desinstalación de KonEncriptación.

Cuando el usuario pulse la opción cerrar, el proceso de desinstalación se habrá completado.

P.F.C: *Herramienta de encriptación adicional para almacenamientos virtuales.*

6. Bibliografía

6.1. Referencias

- [1] **Ataques a la memoria compartida de los servidores EC2 de Amazon para el robo de información,**
http://www.computerworld.com/s/article/9137507/Researchers_find_a_new_way_to_attack_the_cloud?taxonomyId=172&pageNumber=2
- [2] **Cambios en los términos de servicio de Dropbox,** <http://www.genbeta.com/seguridad/dropbox-cambia-de-nuevo-algunos-de-sus-terminos-de-servicio>
- [3] **Cambios en los términos de servicio de Dropbox,**
<http://www.genbeta.com/herramientas/cuidado-con-dropbox-podrian-tener-posibilidad-de-acceder-a-tus-archivos>.
- [4] **Características principales de seguridad de SpiderOAK,** <https://spideroak.com/whyspideroak>
- [5] **Cloud Computing, características,** <http://www.societic.com/2010/03/cloud-computing-caracteristicas-de-las-aplicaciones-en-cloud/>
- [6] **Cloud Computing, definición,** <http://www.desarrolloWeb.com/articulos/cloud-computing.html>
- [7] **Cloud Computing, ventajas y desventajas,**
<http://www.Webtaller.com/maletin/articulos/computacion-nube-riesgos-beneficios.php>
- [8] **Cómo resuelve los conflictos entre archivos Ubuntu One,**
<https://one.ubuntu.com/help/faq/how-do-i-resolve-conflict-files/>
- [9] **Cómo sincronizar carpetas fuera del directorio asociado a Ubuntu One,**
<https://one.ubuntu.com/help/faq/can-i-sync-folders-outside-the-ubuntu-one-folder/>
- [10] **Control de versión de archivos por parte de Ubuntu One,**
<https://answers.launchpad.net/ubuntuone-client/+question/110275>
- [11] **Control de versión de archivos por parte de Ubuntu One,**
<http://askubuntu.com/questions/22163/does-will-ubuntu-one-have-a-version-control-system>
- [12] **Ejemplo gráfico de la técnica de sincronización y de control de versiones de SpiderOAK,**
<https://spideroak.com/blog/20090112220000-what-does-i-mn--v-r- -- - - c>
- [13] **Fallo de seguridad de autenticación de usuarios en el servicio Web de Dropbox,**
<http://carlosadlrs.wordpress.com/2011/06/22/un-fallo-en-dropbox-permite-acceder-a-las-cuentas-sin-la-contrasena-correcta/>

- [14] **IAAS, definición**, <http://www.error500.net/software/infraestructura-como-servicio-iaas-cloud-computing>
- [15] **IAAS, características**, <http://blog.Webstudio.es/archives/444>.
- [16] **Integración de sincronización selectiva de carpetas para Dropbox en Linux**, <http://www.genbeta.com/linux/ya-se-puede-descargar-dropbox-10-rc-con-sincronizacion-selectiva>
- [17] **La autenticación de Dropbox es insegura por diseño**, artículo de Derek Newton, <http://dereknewton.com/2011/04/dropbox-authentication-static-host-ids/>
- [18] **Mejora en los servicios de Ubuntu One**, <http://www.muylinux.com/2011/05/09/ubuntu-11-04-el-analisis/11/>
- [19] **PAAS, definición**, <http://www.dosideas.com/noticias/actualidad/504-ique-es-una-plataforma-como-servicio-paas.html>
- [20] **PAAS, características**, <http://www.anexom.es/servicios-en-la-red/Web-20/que-es-plataforma-como-servicio-paas/>
- [21] **Página Web de detalles técnicos de Ubuntu One**, <https://wiki.ubuntu.com/UbuntuOne/TechnicalDetails>
- [22] **Página Web de descripción de herramientas para sincronizar carpetas fuera del directorio asociado a la cuenta de Dropbox**, <http://wiki.dropbox.com/TipsAndTricks/SyncOtherFolders>
- [23] **SaaS, definición**, http://www.mercadeo.com/63_saas.htm
- [24] **SaaS, características**, <http://www.traceone.com/es/servicios/software-as-a-service/ventajas-del-saas.html>
- [25] **Software para sincronizar en Mac carpetas que se encuentran fuera del directorio asociado a la cuenta de Dropbox**, <http://wiki.dropbox.com/DropboxAddons/MacDropAny>
- [26] **Software para sincronizar en Windows carpetas que se encuentran fuera del directorio asociado a la cuenta de Dropbox**, <http://wiki.dropbox.com/DropboxAddons/DropboxFolderSync>
- [27] **Técnica unidireccional de sincronización utilizada por SpiderOAK**, <http://blog.daemon.com.au/blog-post/file-synching-dropbox-vs-spideroak>
- [28] **Técnica de autenticación de usuario utilizada por Dropbox**, <http://www.hispasec.com/unaaldia/4558>
- [29] **Técnica de autenticación mediante certificados utilizada por Ubuntu One** <http://www.openauthentication.org/certification> ,

<http://translate.google.es/translate?hl=es&sl=en&tl=es&u=http%3A%2F%2Fapachelog.wordpress.com%2F2010%2F08%2F21%2Fubuntu-one-technical-aspects%2F>

- [30] **Técnica de autenticación utilizada por Ubuntu One,**
<https://wiki.ubuntu.com/UbuntuOne/Security>
- [31] **Técnica de autenticación “zero-knowledge” privacy utilizada por SpiderOAK,**
https://spideroak.com/engineering_matters
- [32] **Técnicas para envío seguro de información utilizada por SpiderOAK,**
https://spideroak.com/faq/questions/28/are_there_any_special_firewall_settings_spideroak_needs/
- [33] **Riesgos a los que están sometidos los clientes de los servicios ofrecidos por Cloud Computing,** <http://www.blogoff.es/2009/12/30/seguridad-en-la-nube-una-tarea-pendiente-que-nos-deja-2009/>
- [34] **Servicio backup para mantener la información cifrada localmente ofrecida por SpiderOAK,**
https://spideroak.com/engineering_matters#infrastructure
- [35] **Software recomendado por Dropbox para el cifrado adicional de la información localmente, TrueCrypt,** <http://wiki.dropbox.com/TipsAndTricks/IncreasePrivacyAndSafety>
- [36] **Script utilizado por Ubuntu One para el cifrado adicional de la información localmente, Ubuntu One Encrypt/Decrypt,** <http://gnome-look.org/content/show.php?content=142064>
- [37] **Versión de Ubuntu One para Windows,**
<https://wiki.ubuntu.com/UbuntuOne/Windows#Overview>
- [38] **Video tutorial de cómo tener un backup de la información cifrada con SpiderOAK,**
<https://spideroak.com/howitworks/Backup>
- [39] **Video tutorial de cómo tener es la sincronización de archivos y directorios en SpiderOAK,**
<https://spideroak.com/howitworks/Sync>
- [40] **Video tutorial de estado de la sincronización de los archivos y directorios en SpiderOAK,**
<https://spideroak.com/howitworks/Status>

6.2. Bibliografía adicional

- Alfred J. Menezes. Handbook of Applied Cryptography. CRC Press, 2001.
- Douglas R. Stinson. Cryptography. Theory and Practice. CRC Press, 2005.

- Jennifer Seberry and Josed Pieprzyk. *Cryptography: An Introduction to Computer Security*. Prentice Hall, 1989.
- Oded Goldreich. *Foundations of cryptography*. Vols. 1 y 2. Cambridge University Press, 2004.
- Jonathan Knudsen. *Java Cryptography*. O'Reilly, 1998.

6.3. Glosario de términos

AES (*Advanced Encryption Standart*): algoritmo de clave simétrica. Las distintas nomenclaturas **AES 128**, **AES 128** y **AES 256** se refieren al tamaño de clave usado.

Amazon EC2 (*Elastic Compute Cloud*): servicio Cloud Computing de tipo IaaS que ofrece capacidad de cómputo variable. **Página oficial**: <http://aws.amazon.com/es/ec2/>

App Engine: servicio Cloud Computing de tipo IaaS que ofrece capacidad de cómputo variable.
Página oficial: https://accounts.google.com/ServiceLogin?service=ah&passive=true&continue=https://appengine.google.com/_ah/conflogin%3Fcontinue%3Dhttps://appengine.google.com/<mpl=ae

Blue Cloud: proyecto de IBM para ofrecer servicios de tipo IaaS, PaaS y SaaS en la nube. **Página oficial**: <http://www.ibm.com/cloud-computing/us/en/>

Bungee Connect: servicio de tipo PaaS para desarrolladores de aplicaciones. **Página oficial**: <http://www.bungeelabs.com/>

CBC (*Cipher Block Chaining*): método de operación utilizado por los métodos de cifrado donde a cada bloque a cada bloque de texto en claro que va a ser cifrado se le aplica una operación XOR.

Cloud Computing o Computación en la nube: servicio de procesamiento en red (**ver apartado 1.2**).

Cloud (o nube): sinónimo de internet. Se usa el término para referirse a un conjunto de servidores que prestan un servicio de computación a terceros:

- **Cloud públicas**: servicios y aplicaciones alojados y gestionados de forma remota por un tercero y el cliente accede a ellas.
- **Cloud privadas**: servicios y aplicaciones alojados remotamente, pero son gestionados de forma por el propietario de esta.

DES (*Data Encryption Standard*): método de cifrado de clave simétrica que utiliza un tamaño de clave 56 bits. Se trata de un método inseguro y de él se deriva el método de Triple DES.

Dropbox: software de almacenamiento virtual. **Página oficial**: <http://www.dropbox.com>.

Enlaces entre archivos: es una técnica que permite crear enlaces simbólicos entre archivo mediante el uso del comando ln. **Ver ejemplo**: <http://dns.bdat.net/documentos/cursos/ar01s15.html>.

Google App: ofrece servicios SaaS, centrándose en herramientas colaborativas y de mensajería. **Página oficial**: <http://www.google.com/apps/intl/es/group/index.html>

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

ECB: (*Electronic Code Book*): modo de operación utilizado por los métodos de cifrado donde la información se divide en bloques y estos se van cifrando por separado.
<http://spi1.nisu.org/recop/al01/skar/tema2.html>

IaaS: infraestructura como servicio (**ver apartado 1.2.2.1**).

Máquina virtual: software que emula a una computadora con unas determinadas características tanto de hardware como de software y se ejecuta como una computadora real.

Ordenamiento de burbuja: algoritmo de ordenación cuyo orden de complejidad algorítmica es $O(n)$.

PaaS: plataforma como servicio (**ver apartado 1.2.2.2**.)

PKCS5: estándar definido para el cifrado de claves pública basada en contraseña.
ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-5v2/pkcs5v2_1.pdf

Recorrido en inorden: tipo de recorrido de árboles binarios donde se obtiene de forma ordenada la información almacenada.

RIPMD-160: algoritmo de resumen de mensaje de 160 bits desarrollado en Europa en 1996 por Hans Dobbertin, Antoon Bosserlaers y Bart Preneel.

RSA (*Rivest, Shamir y Adleman*): método de cifrado de clave asimétrica cuyas siglas toman el nombre de sus creadores. Las distintas nomenclaturas **RSA 1024** y **RSA 2048** se refieren al tamaño de clave usado.

SaaS: software como Servicio. Ver definición en **apartado 1.2.2.3**.

SalesForce: portal Web que ofrece PaaS para empresas. **Página oficial:**
<http://www.salesforce.com/es/>

SecretSync: único software conocido de cifrado diseñado para cifrar información adicionalmente en Dropbox. **Página oficial:** <http://getsecretsync.com/ss/>.

Serpents: algoritmo de clave simétrica por bloques cuyo tamaño de bloque es de 128 bits y el tamaño de la clave puede ser de 128,192 o 256 bits.

SHA-512: algoritmo de resumen de mensajes utilizado para la integridad de datos y que genera resúmenes de 512 bits.

SpiderOAK: software de almacenamiento virtual. **Página oficial:** <https://spideroak.com/>.

SSL (*Secure Socket Layer*): protocolo de conexión segura que utiliza protocolos criptográficos para asegurar la comunicación segura por la red.

TI (*Tecnologías de la Información*): según la ITAA (*Information Technology Association of America*) es “el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras.”

Triple DES: método de cifrado de clave simétrica que realiza un triple cifrado de tipo DES y da como resultado una clave de 192 bits de los que 112 bits son los utilizados realmente como clave.

P.F.C: Herramienta de encriptación adicional para almacenamientos virtuales.

TrueCrypt: software para cifrado de información que utiliza distintos criptosistemas para cifrar la información. **Página oficial:** <http://www.truecrypt.org/>.

Tunneling: técnica donde se encapsula un protocolo de red sobre otro creando un canal o túnel donde se envía la información de forma segura entre los extremos de la comunicación y sin que los nodos intermedios (switch, routers,...) puedan ver el contenido de los paquetes enviados.

TwoFish: algoritmo de clave simétrica por bloques cuyo tamaño de bloque a procesar es de 128 bits y el de la clave puede ser de hasta 256 bits.

Ubuntu One: software de almacenamiento virtual. **Página oficial:** <https://one.ubuntu.com/>.

Ubuntu One Encrypt/Decrypt: script utilizado por Ubuntu One para cifrar la información localmente.

Virtualización de plataforma: técnica donde se utilizan equipos suficientemente potentes o configurados para trabajar en paralelo, creando máquinas virtuales capa que sean capaces de soportar los servicios demandados por sus huéspedes.

WhirPool: algoritmo resumen de mensajes para generar resúmenes de 512 bits.

Windows Azure: servicio Cloud Computing de tipo IaaS ofrecido por Microsoft. **Página oficial:** <http://www.microsoft.com/windowsazure/>.