Universitat Oberta de Catalunya

MirrorCrypt

José María García Martínez
Itinerario de Tecnologías de la Información
Seguridad Informática

Cristina Pérez Solà

14/04/2014

FICHA DEL TRABAJO FINAL

Título del trabajo:	MirrorCrypt
Nombre del autor:	José María García Martínez
Nombre del consultor:	Cristina Pérez Solà
Fecha de entrega (mm/aaaa):	06/2014
Área del Trabajo Final:	Seguridad Informática
Titulación:	*Grado en Ingeniería Informática, itinerario de Tecnologías de la Información.*

Resumen del Trabajo (máximo 250 palabras):

En el siguiente trabajo se explica el proceso de creación de la aplicación MirrorCrypt. Esta aplicación está pensada para ser usada con servicios de alojamiento en la nube proveyendo de un sistema de encriptación transparente al usuario encriptando todos los datos alojados en la nube. La aplicación no sólo encripta los datos sino que además también los comprime. El objetivo de dicho sistema es conseguir que la información alojada en la nube lo esté de manera encriptada y que se trabaje con la información original de modo local de una forma transparente, de tal manera que la aplicación automáticamente sincronizará los cambios producidos en el directorio de trabajo no encriptado con el directorio encriptado del servicio de alojamiento en la nube, todo ello en background y sin que el usuario se percate de ello.

Abstract (in English, 250 words or less):

In this paper is explained the process of creating the application MirrorCrypt. This application is designed for use with hosting services in the cloud providing a transparent user encryption by encrypting all data stored in the cloud. The application not only encrypts the data but also compress them. The purpose of this system is to get the information stored in the cloud is encrypted and to work with the original information locally in a transparent manner, so that the application will automatically synchronize the changes between unencrypted directory and the local encrypted directory for service cloud hosting, all in the background without the user being aware of it.

Palabras clave (entre 4 y 8):

Nube, Encriptación, Compresión, Transparente.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Desde hace ya algún tiempo se ha puesto de actualidad el almacenamiento de datos en la nube con servicios como DropBox, OneDrive (antes conocido como SkyDrive) o Google Drive. Estos servicios proporcionan un sistema de backup y sincronización transparente de cara al usuario y facilitan poder acceder a los datos en cualquier momento y lugar. También facilitan la compartición de estos datos con nuestros familiares y amigos.

En los últimos meses se ha venido escuchando en los medios de comunicación el sistema de espionaje masivo que ha seguido la agencia de seguridad nacional estadounidense (NSA) gracias a las filtraciones de Snowden. Como resultado de esas filtraciones se ha podido saber que la NSA ha obtenido datos de millones de usuarios introduciendo puertas traseras en software, ha participado en desarrollo de protocolos que podían ser fácilmente hakeados por sus sistemas, ha espiado las redes sociales…

Ante las preocupantes informaciones que se han filtrado en los medios surge enseguida una pregunta: ¿qué ha pasado con mis datos personales subidos a la nube? ¿Pueden haber accedido a ellos? Esta pregunta de momento no tiene respuesta aunque por las informaciones facilitadas no sería algo descabellado.

Con todo esto que ha ocurrido es hora de preguntarse qué sistemas de seguridad están siguiendo los proveedores de almacenamiento en la nube para evitar este acceso no autorizado. Los proveedores argumentan que usan sistemas de encriptación y que por lo tanto nuestros datos están cifrados en la nube. Sin embargo no aclaran si esa encriptación se realiza una vez que se ha subido el fichero (por lo que el proveedor podría conocer la clave de encriptación y en cualquier momento permitir el acceso a nuestros datos si una autoridad lo requiere) o se realiza en local y después se sube el fichero (por lo que en principio

el proveedor no conocería la clave de encriptación y por lo tanto no podría desencriptar los ficheros). Tampoco aclaran realmente cuál es el sistema de encriptación empleado (AES, TwoFish, etc).

Por todo ello se hace aconsejable que usemos algún sistema de encriptación que, independientemente del que realmente luego use nuestro proveedor de almacenamiento en la nube, mantenga nuestra información encriptada en la nube de tal forma que éste no tenga manera alguna de poder acceder a la información original.

1.2 Objetivos del Trabajo

La aplicación que aquí se presenta intenta solucionar el problema expuesto en el punto anterior mediante un sistema de encriptación transparente y en segundo plano que permita al usuario trabajar con sus datos originales en su máquina local mientras que los archivos en la nube son almacenados de manera encriptada evitando así el acceso no autorizado a su contenido.

De manera un poco más detallada esta aplicación deberá permitir:

- Cifrar el contenido de los archivos que se encuentren en un directorio así como de sus subdirectorios.

- Cifrar en un segundo plano, será transparente para el usuario que podrá seguir trabajando con los documentos originales sin cifrar con normalidad sin que se entere que están siendo cifrados en background.

- Sincronizar automáticamente el contenido de los directorios entre el local no cifrado y el cifrado, de tal manera que el cambio producido en cualquier fichero del directorio no cifrado provocará la encriptación por parte de la aplicación del mismo y su almacenamiento en el directorio cifrado.

- Automáticamente desencriptar en local un directorio encriptado para poder trabajar de manera transparente sincronizando automáticamente los cambios efectuados en la carpeta encriptada con la carpeta local.

1.3 Enfoque y método seguido

Para conseguir la funcionalidad requerida se implementará un producto nuevo ya que actualmente no existe ningún producto en el mercado que satisfaga los requerimientos exigidos.

1.4 Planificación del Trabajo

La creación y desarrollo del proyecto requerirá de la realización de las siguientes tareas:

- Definición y alcance de proyecto.
- Establecer los objetivos a cumplir.
- Definición de hitos a cumplir en cada PEC.
- Establecer la tecnología a usar.
- Realizar estimación inicial de la planificación temporal.
- Crear los casos de uso.
- Diagramas de caso de uso y secuencia.
- Diagramas de clases.
- Desarrollar la aplicación usando las tecnologías propuestas.
- Testear la aplicación.
- Crear la documentación para el usuario.
- Crear la documentación para instalación/configuración.

Para el análisis y diseño de la aplicación se usarán los siguientes sistemas:

- Planificación de las fases del proyecto
- Recogida de datos y requisitos.
- Casos de uso.

- Diseño de la aplicación a través de UML (Unified Modeling Language) enfocado al desarrollo de una aplicación por objetos.
- Diseño visual de la interfaz gráfica.
- Implementación de la aplicación mediante .NET.

Para llevar a cabo todos estos objetivos se usarán las siguientes herramientas:

- Microsoft Project 2013 para la planificación de las fases y tareas del proyecto.
- Microsoft Visio 2013 para la creación de los diagramas UML.
- Microsoft Word 2013 para la documentación.
- Microsoft PowerPoint 2013 para la generación de las presentaciones relativas a este proyecto.
- Microsoft Visual Studio 2013 para la implementación de la aplicación en lenguaje C#.

Para poder usar la aplicación será necesario:

- Ordenador PC con sistema operativo Microsoft Windows Vista Service Pack 2 o superior.
- Microsoft .Net Framework 4.51.

Para el desarrollo de este proyecto se necesitará:

- 1 ordenador PC con 4 GB de memoria RAM, 100 GB de disco duro y procesador Intel i3.

- Monitor a resolución 1024x768.

- Sistema operativo Windows 8.1.

- Microsoft Visual Studio .NET 2013, edición Premium.

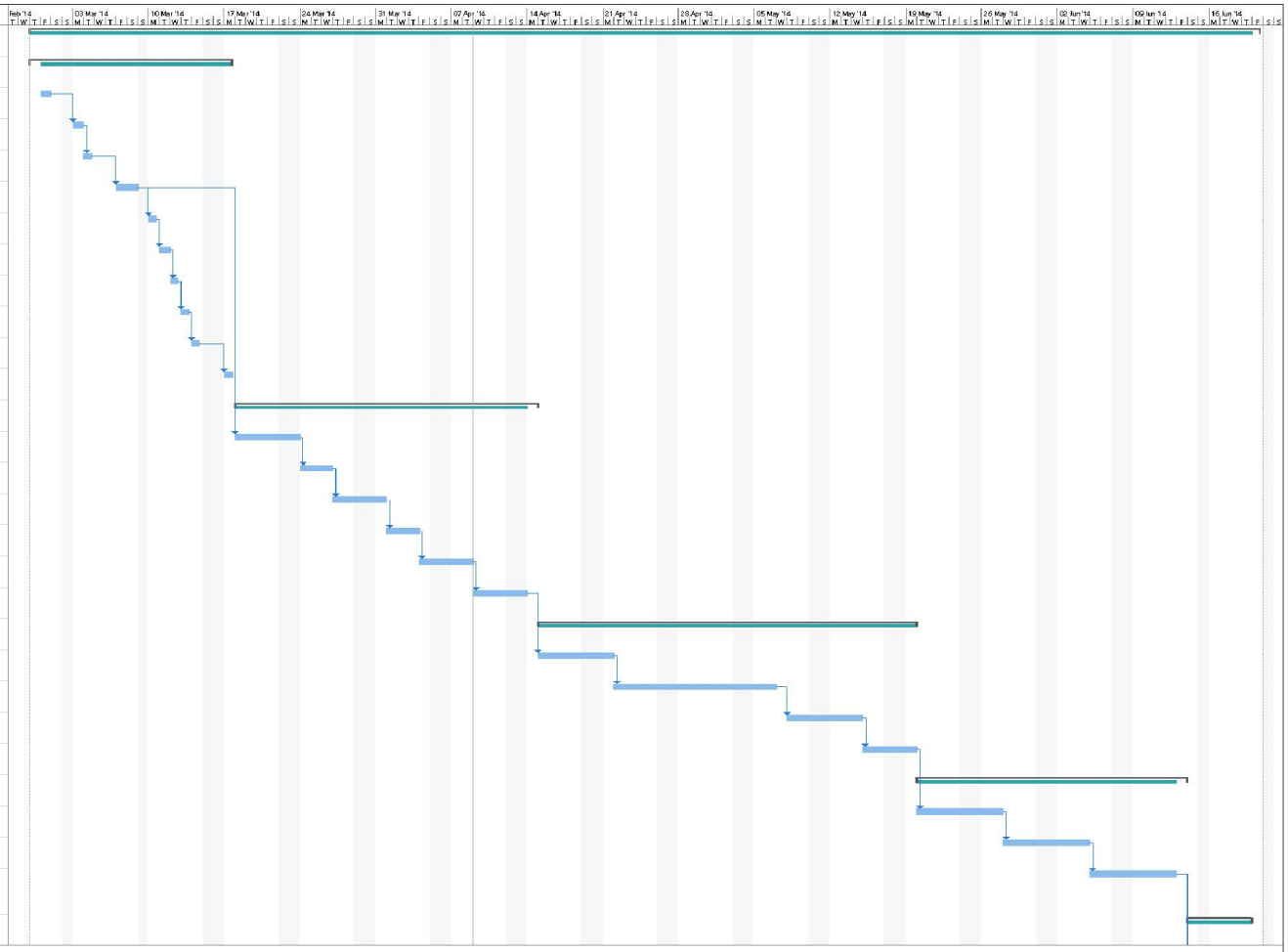
- Un rol de analista en el tiempo que esté previsto el análisis de la aplicación y la recogida de requisitos.

- Un rol de desarrollador en el tiempo que esté previsto la implementación del proyecto.

- Un rol de testeador en el tiempo que esté previsto el testeo de la aplicación.

- Un rol de documentalista durante el tiempo que esté prevista la creación de la documentación de la aplicación.

ID	Task Mode	Task Name	Duration	Start	Finish	Predecessors
1		**Trabajo Final de Grado en Seguridad Informatica**	**85 days**	**Thu 27/02/14**	**Fri 20/06/14**	
2		**PEC 1 - Plan de trabajo**	**15 days**	**Thu 27/02/1**	**Mon 17/03/**	
3		Definición y alcance del proyecto	1 day	Fri 28/02/14	Fri 28/02/14	
4		Establecer objetivos a cumplir	1 day	Mon 03/03/14	Mon 03/03/14	3
5		Definición de hitos a cumplir en cada PEC	1 day	Tue 04/03/14	Tue 04/03/14	4
6		Estado del arte	2 days	Fri 07/03/14	Sat 08/03/1	5
7		Establecer metodología y tecnologías a usar	1 day	Mon 10/03/14	Mon 10/03/14	6
8		Realizar planificación temporal	1 day	Tue 11/03/14	Tue 11/03/14	7
9		Análisis de riesgos	1 day	Wed 12/03/	Wed 12/03/	8
10		Análisis de viabilidad	1 day	Thu 13/03/1	Thu 13/03/1	9
11		Descripción de recursos necesarios	1 day	Fri 14/03/14	Fri 14/03/14	10
12		Presupuesto del proyecto	1 day	Mon 17/03/	Mon 17/03/	11
13		**PEC 2 - Análisis y diseño de la aplicación**	**20 days**	**Tue 18/03/14**	**Mon 14/04/14**	
14		Análisis de requerimientos formales	4 days	Tue 18/03/14	Mon 24/03/14	6
15		Definición de actores	3 days	Mon 24/03/	Thu 27/03/1	14
16		Análisis y diagrama de casos de uso	3 days	Thu 27/03/14	Tue 01/04/14	15
17		Diagrama de clases	3 days	Tue 01/04/1	Fri 04/04/14	16
18		Diagrama de secuencia	3 days	Fri 04/04/14	Wed 09/04/	17
19		Diseño del interfaz	3 days	Wed 09/04/	Mon 14/04/	10
20		**PEC 3 - Implementación de la aplicación**	**25 days**	**Tue 15/04/14**	**Mon 19/05/14**	
21		Implementación del interfaz de usuario	5 days	Tue 15/04/14	Tue 22/04/14	19
22		Implementación de los algoritmos de encriptación	11 days	Tue 22/04/14	Wed 07/05/14	21
23		Implementación de los algoritmos de sincronización	5 days	Thu 08/05/14	Wed 14/05/14	22
24		Testeos integrados	3 days	Thu 15/05/1	Mon 19/05/	23
25		**PEC 4 - Creación de la documentación**	**19 days**	**Tue 20/05/14**	**Fri 13/06/14**	
26		Elaboración de la memoria	6 days	Tue 20/05/1	Wed 28/05/	24
27		Elaboración del manual de usuario	6 days	Wed 28/05/14	Thu 05/06/14	26
28		Elaboración de la presentación PowerPoint para el Tribunal	6 days	Thu 05/06/14	Fri 13/06/14	27
29		**Presentación virtual**	**5 days**	**Sat 14/06/1**	**Fri 20/06/14**	



Project: Project1
Date: Wed 09/04/14

Task | Split | Milestone | Summary | Project Summary | Inactive Task | Inactive Milestone | Inactive Summary | Manual Task | Duration-only | Manual Summary Rollup | Manual Summary | Start-only | Finish-only | External Tasks | External Milestone | Deadline | Progress | Manual Progress

Page 1

1.5 Breve sumario de productos obtenidos

Como resultado de la implementación se ha obtenido una aplicación capaz de encriptar y sincronizar automáticamente el contenido de dos directorios, uno encriptado y el otro sin encriptar.

1.6 Breve descripción de los otros capítulos de la memoria

2.1- Estado del arte: se explica brevemente el panorama actual del sector al que va enfocada la aplicación.

2.2- Análisis de riesgo: se muestra brevemente los riesgos que se pueden producir en la implementación de la aplicación.

2.3- Análisis de viabilidad: se explica si el proyecto es o no viables.

2.4- Presupuesto del proyecto: se muestra el precio que costará implementar el poyecto.

2. Diseño e implementación de la solución

2.1.- Estado del arte

Actualmente existen diversas aplicaciones de encriptación de ficheros que podemos agrupar en diferentes tipos dependiendo de cómo trabajan con la encriptación de archivos:

2.1.1- Encriptación de una partición del disco duro.

Este tipo de aplicaciones encriptan una partición completa del disco duro y trabajan con ella encriptando/desencriptando la información contenida en ella de manera transparente para el usuario. Entre este tipo de aplicaciones encontramos los que pueden encriptar cualquier partición, incluida la partición de arranque del sistema donde está alojado el sistema operativo, y aquellas aplicaciones que sólo pueden encriptar una partición que no sea la del sistema.

Entre las aplicaciones más conocidas que trabajan con este modo de encriptación se encuentran Microsoft BitLocker, incluido en el sistema operativo desde Windows 7; y TrueCrypt (1) y DiskCryptor (2) que son aplicaciones open source.

2.1.2- Encriptación con volúmenes virtuales.

En este tipo de encriptación la aplicación crea una unidad de disco virtual donde todo lo que se aloje en ella estará encriptado. La encriptación es transparente para el usuario que ve el contenido de la unidad como si no estuviera encriptada.

A nivel físico la unidad virtual se aloja en un único fichero del disco duro, que se monta y se desmonta como unidad virtual mediante la aplicación. Toda la información queda guardada en un único fichero contenedor que se encuentra encriptado.

Este fichero suele ser un ‘sparse file’, por lo que realmente no se usa físicamente el tamaño de la unidad que se definió en el momento de su creación, si no que el tamaño comienza siendo muy pequeño y va creciendo según se va almacenando información en él (es lo que se conoce como una unidad de disco dinámica).

Como ejemplo de este tipo de encriptación la aplicación más conocida es TrueCrypt, que es open source.

El problema que tiene este sistema de encriptación es que cualquier modificación, por mínima que sea, en cualquier fichero del volumen encriptado provoca una modificación del fichero físico en el que se aloja el volumen. Puesto que este fichero puede ser de un tamaño muy grande (de varios GB e incluso TB), este sistema no es viable para trabajar con aplicaciones de hospedaje en la nube como DropBox ya que, teniendo el fichero contenedor en la carpeta de trabajo de DropBox, tendría que subir cada vez el fichero contenedor aunque sólo se hubiera modificado en un 1 byte cualquier fichero del volumen encriptado.

2.1.3- Encriptación independiente de ficheros.

En este modo de encriptación los ficheros de la unidad son encriptados independientemente, manteniéndose normalmente el nombre original del fichero (por lo que su nombre puede delatar el contenido).

Entre las aplicaciones más conocidas que hacen uso de este modo de encriptación está el propio sistema operativo Windows, MacOS X y Linux -véase EnCFS (3) -, que permiten encriptar parte de los ficheros de su unidad atendiendo al usuario. En Windows, por ejemplo, para encriptar un fichero es tan simple como pinchar sobre él para ver sus propiedades avanzadas y seleccionar la opción ‘Encriptar el contenido’.

El problema de este sistema de encriptación es que no es viable para trabajar con hospedaje en la nube como DropBox ya que se necesita la cuenta del

usuario en el sistema para poder desencriptar los archivos, por lo que esto no servirá a la hora de bajárselos en otro equipo.

También nos encontramos herramientas gratuitas como AxCrypt (4) que permite encriptar ficheros independientemente. La aplicación encripta un fichero en base a una contraseña, a la hora de descriptar el contenido nos vuelve a preguntar la contraseña y si es correcta desencripta el fichero en una ruta temporal. Una vez que hemos dejado de hacer uso del fichero, la aplicación vuelve a encriptar este fichero temporal con las modificaciones que hayamos podido hacer modificando el fichero encriptado, de esta manera el funcionamiento es transparente para el usuario.

2.1.4- Ficheros comprimidos encriptados.

Compresores como WinRar (5) o 7Zip (6) permiten encriptar el contenido de los archivos encriptados mediante algoritmos como AES-256. Cuando se trabaja con algún archivo de los comprimidos, éste es descomprimido en una ruta temporal y es abierto con la aplicación correspondiente. Una vez terminada la edición se nos da la posibilidad de actualizar el fichero modificado dentro del archivo comprimido.
De nuevo el problema que aparece aquí es que no es un sistema adecuado para trabajar en la nube con aplicaciones como DropBox ya que cualquier cambio en alguno de los ficheros comprimidos implica la modificación del archivo comprimido, por lo que tendría que volver a ser subido de nuevo.

2.1.5- Encriptación independiente de ficheros mediante directorios o unidades virtuales espejo.

Este modo de encriptación es una mezcla de algunos de los anteriores modelos. Consiste en que se tiene un directorio o unidad virtual con el que se trabaja con los archivos desencriptados, mientras que en la carpeta de trabajo de la aplicación en la nube se almacenan los archivos encriptados a modo de espejo, es decir, cualquier cambio en los archivos de la carpeta desencriptada es automáticamente replicado y sincronizado en el directorio encriptado. El

contenido de ambos directorios siempre será el mismo sólo que uno lo tendrá de manera encriptada y el otro no.
Este sistema es el ideal para trabajar con servicios de alojamiento en la nube como DropBox ya que solamente los ficheros que realmente hayan sufrido alguna modificación son los que serán subidos a la nube, por lo que el volumen de datos que se envía a la nube se reduce considerablemente. Es por ello que este sistema de encriptación será el que se use para la aplicación que se va a implementar en este proyecto.
Aplicaciones que usen este sistema de encriptación las más conocidas son BoxCryptor (7) y Cloudfogger (8).

2.2- Análisis de riesgos

Durante el desarrollo del proyecto es posible que puedan surgir algunos problemas o imprevistos. Éstos principalmente serían de tipo técnico. Algunos de estos problemas podrían ser:

- Fallo en los algoritmos de encriptación que dejen la información irrecuperable.

- Problemas en los algoritmos de sincronización que dejasen los ficheros encriptados corruptos o que no se actualizarán éstos a la última modificación realizada sobre los archivos originales.

Se tendrá por lo tanto especial cuidado con dichos puntos y cualquier contingencia será reflejada correspondientemente en la planificación temporal.

2.3- Análisis de viabilidad

Este proyecto no requiere de una amplia inversión a nivel tecnológico, todo lo contrario, cualquier ordenador de hoy en día valdría para poder desarrollarlo.

En cuanto a la complejidad de su desarrollo tampoco es excesivo, por lo que los análisis preliminares indican que se trata de un proyecto viable tanto en tiempo como en recursos.

Por lo tanto se estima que este proyecto es viable teniendo un total de 64 días a partir de ahora para el desarrollo de la aplicación.

2.4- Presupuesto del proyecto

A continuación se recoge en una tabla los costes estimados del proyecto:

Concepto	Días	Precio
1 ordenador PC con monitor	-	600€
Sistema operativo Windows 8.1	-	119€
Microsoft Visual Studio .NET 2013 Premium	-	7.927€
Microsoft Office 2013 Professional	-	539€
Analista	20 días a 30€/hora	4.800€
Desarrollador	22 días a 20€/hora	3.520€
Testeador	3 días a 10€/hora	240€
Documentalista	19 días a 13€/hora	1.976€

Total: 19.721€

2.5- Análisis de requerimientos formales

Se necesita una aplicación que, dada una ruta local a la que llamaremos no encriptada-, sea capaz de encriptar automáticamente el contenido del directorio, incluidos sus subdirectorios, en otra carpeta –a la que llamaremos encriptada-, y que cualquier cambio producido en la carpeta no encriptada sea automáticamente y de forma transparente reflejado en la carpeta encriptada. Por lo tanto se necesita una aplicación que realice los siguientes puntos:

- La aplicación deberá encriptar el contenido de la carpeta no encriptada en otra carpeta encriptada, incluidos todos sus subdirectorios.

- La aplicación deberá ser capaz de enterarse qué ficheros de la carpeta no encriptada han sido modificados desde la última vez que se realizó la encriptación y procediendo por lo tanto a encriptar de nuevo estos ficheros. Esta comprobación deberá ser inmediata, de tal manera que un archivo de la carpeta no encriptada que acaba de ser modificado debe de ser encriptado en cuestión de segundos.

- La aplicación deberá de realizar la encriptación en un segundo plano de manera transparente para el usuario.

- La primera vez que se asigne una nueva dirección de carpeta encriptada (o una nueva de la carpeta no encriptada) la aplicación deberá proceder a encriptar todo el contenido de la carpeta no encriptada en la carpeta encriptada.

2.6- Definición de actores

- **Usuario**: será el encargado de interactuar con el sistema. Se encargará de indicar al sistema la ruta de la carpeta no encriptada y de la carpeta encriptada, y se encargará también de generar contenido en la carpeta no encriptada que luego será encriptado por el sistema.

- **Sistema**: se encargará de encriptar de manera automática todo el contenido de la carpeta no encriptada en la carpeta encriptada. Estará continuamente verificando si hay nuevos ficheros que encriptar en la carpeta no encriptada o si alguno de estos ha sufrido alguna modificación desde la última vez que se encriptaron.

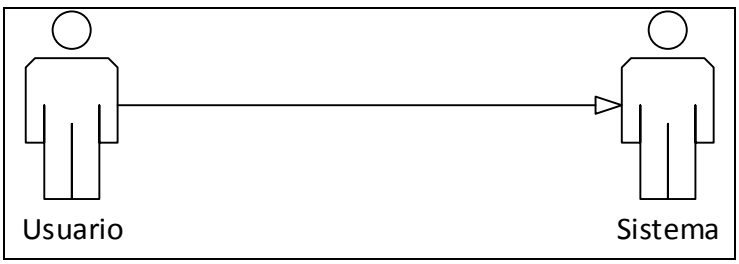


Figura 1: actores

2.7- Casos de uso

2.7.1- Casos de uso de usuario

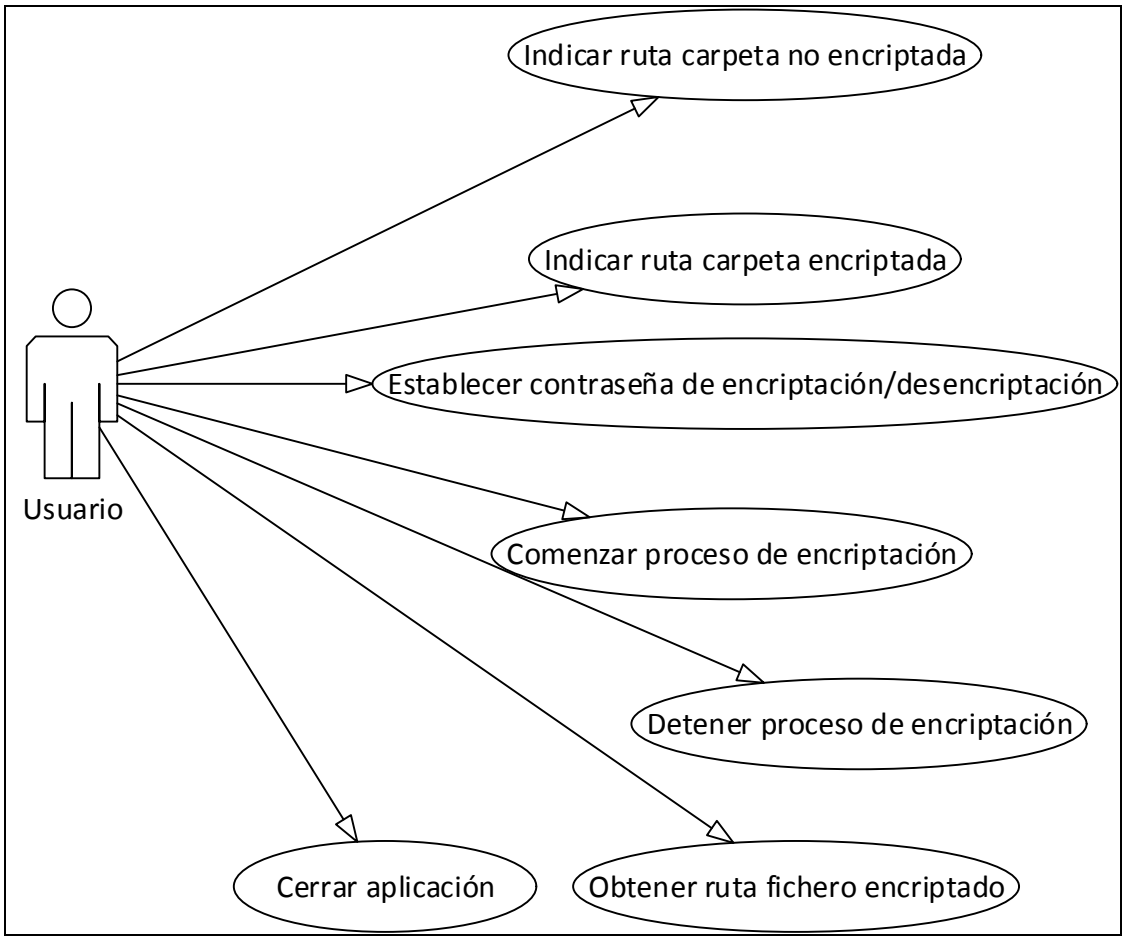


Figura 2: casos de uso de usuario

Caso de Uso 1 – Indicar ruta carpeta no encriptada
Resumen: el usuario establece la ruta de la carpeta no encriptada.
Actores: usuario
Casos de uso relacionados
Precondición
Postcondición: el sistema almacena la ruta de la carpeta no encriptada.
Proceso principal: 1- El usuario introduce la ruta de la carpeta no encriptada.
Excepciones
Observaciones

Caso de Uso 2 – Indicar ruta carpeta encriptada
Resumen: el usuario establece la ruta de la carpeta encriptada.
Actores: usuario
Casos de uso relacionados
Precondición
Postcondición: el sistema almacena la ruta de la carpeta encriptada.
Proceso principal: 1- El usuario introduce la ruta de la carpeta encriptada.
Excepciones
Observaciones

Caso de Uso 3 – Establecer contraseña de encriptación/desencriptación
Resumen: el usuario establece la contraseña de encriptación/desencriptación.
Actores: usuario
Casos de uso relacionados
Precondición
Postcondición: el sistema almacena la contraseña de encriptación/desencriptación.
Proceso principal: 1- El usuario introduce la contraseña de encriptación/desencriptación.
Excepciones
Observaciones

Caso de Uso 4 – Comenzar proceso de encriptación
Resumen: el usuario pulsa el botón de comenzar encriptación.
Actores: usuario
Casos de uso relacionados
Precondición: 1 - Las rutas de las carpetas encriptada y no encriptadas tienen que haber sido establecidas. 2 - El proceso de encriptación no debe de estar ejecutándose.

Postcondición: el sistema encripta el contenido de la carpeta no encriptada en la carpeta encriptada.
Proceso principal: 1- El usuario pulsa el botón de comenzar encriptación.
Excepciones
Observaciones

Caso de Uso 5 – Detener proceso de encriptación
Resumen: el usuario pulsa el botón de detener encriptación.
Actores: usuario
Casos de uso relacionados
Precondición: el proceso de encriptación debe de estar ejecutándose.
Postcondición: el sistema encripta el contenido de la carpeta no encriptada en la carpeta encriptada.
Proceso principal: 1- El usuario pulsa el botón de comenzar encriptación.
Excepciones
Observaciones

Caso de Uso 6 – Obtener ruta fichero encriptado
Resumen: el usuario selecciona un fichero de la carpeta no encriptada y la aplicación muestra la ruta del mismo fichero en la carpeta encriptada.
Actores: usuario
Casos de uso relacionados
Precondición
Postcondición: el sistema muestra la ruta del fichero encriptado.
Proceso principal: 1- El usuario pulsa el botón de buscar. 2- Le aparece un cuadro de diálogo para que seleccione un fichero perteneciente a la carpeta encriptada. El usuario lo selecciona y pulsa OK. 3- La ruta del fichero encriptado se muestra en una caja de texto.
Excepciones
Observaciones

Caso de Uso 7 – Cerrar aplicación
Resumen: el usuario pulsa el botón de cerrar aplicación.
Actores: usuario
Casos de uso relacionados
Precondición
Postcondición: el sistema termina el proceso de encriptación (si estaba en ejecución) y cierra la aplicación.
Proceso principal: 1- El usuario pulsa el botón de cerrar aplicación.
Excepciones
Observaciones

2.7.2- Casos de uso de Sistema

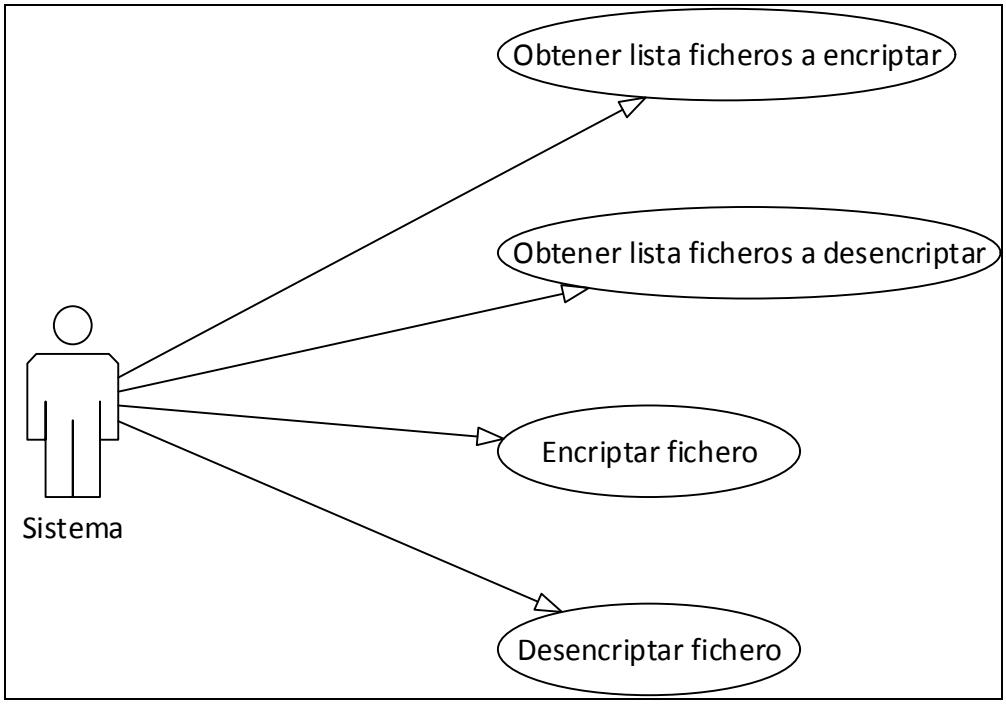


Figura 3: casos de uso de sistema

Caso de Uso 8 – Obtener lista de ficheros a encriptar
Resumen: el sistema devuelve una lista con los ficheros que deben de ser encriptados.
Actores: sistema.
Casos de uso relacionados
Precondición: el proceso de encriptación debe de estar en ejecución.
Postcondición: el sistema obtiene una lista de los ficheros a encriptar.
Proceso principal: 1- El sistema verifica fichero a fichero cuáles han sido modificados en la carpeta de no encriptados respecto de la carpeta encriptados guíandose por la fecha de modificación.. 2- El sistema devuelve una lista con esos ficheros que deben de ser encriptados.
Excepciones
Observaciones

Caso de Uso 9 – Obtener lista de ficheros a desencriptar
Resumen: el sistema devuelve una lista con los ficheros que deben de ser desencriptados.
Actores: sistema.
Casos de uso relacionados
Precondición: el proceso de encriptación debe de estar en ejecución.
Postcondición: el sistema obtiene una lista de los ficheros a desencriptar.
Proceso principal: 1- El sistema verifica fichero a fichero cuáles han sido modificados en la carpeta de encriptados respecto de la carpeta no encriptados guíandose por la fecha de modificación. 2- El sistema devuelve una lista con esos ficheros que deben de ser desencriptados.
Excepciones
Observaciones

Caso de Uso 10 – Encriptar fichero
Resumen: el sistema encripta un fichero en la carpeta encriptada.
Actores: sistema.
Casos de uso relacionados
Precondición: el proceso de encriptación debe de estar en ejecución.
Postcondición: el sistema graba un fichero encriptado en la carpeta encriptada.
Proceso principal: 1- El sistema encripta un fichero de la carpeta no encriptada y lo almacena en la carpeta encriptada.
Excepciones
Observaciones

Caso de Uso 11 – Desencriptar fichero
Resumen: el sistema desencripta un fichero en la carpeta encriptada.
Actores: sistema.
Casos de uso relacionados
Precondición: el proceso de encriptación debe de estar en ejecución.
Postcondición: el sistema graba un fichero desencriptado en la carpeta no encriptada.
Proceso principal: 1- El sistema desencripta un fichero de la carpeta encriptada y lo almacena en la carpeta no encriptada.
Excepciones
Observaciones Si la contraseña de desencriptación es incorrecta mostrará un mensaje de error y abortará el proceso de desencriptación.

2.8- Diagramas de secuencia

2.8.1- Establecer ruta de carpeta no encriptada

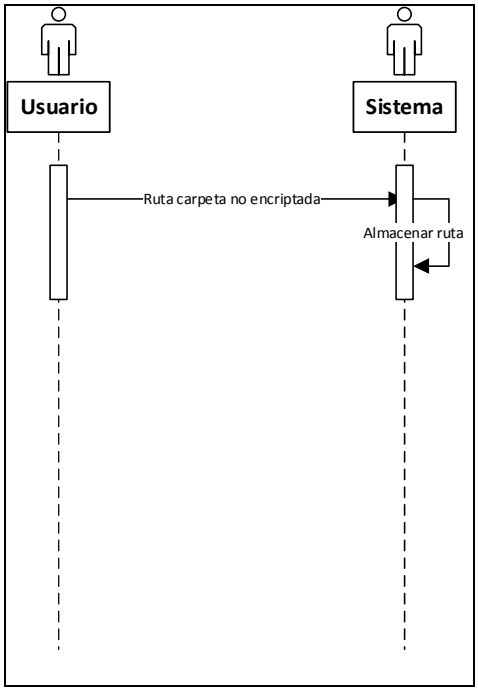


Figura 4: establecer ruta de carpeta no encriptada

2.8.2- Establecer ruta de carpeta encriptada

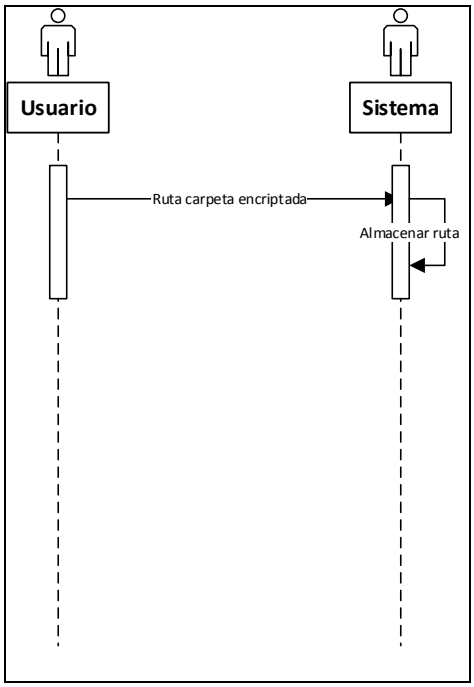


Figura 5: establecer ruta de carpeta encriptada

2.8.3- Establecer contraseña de encriptación/desencriptación

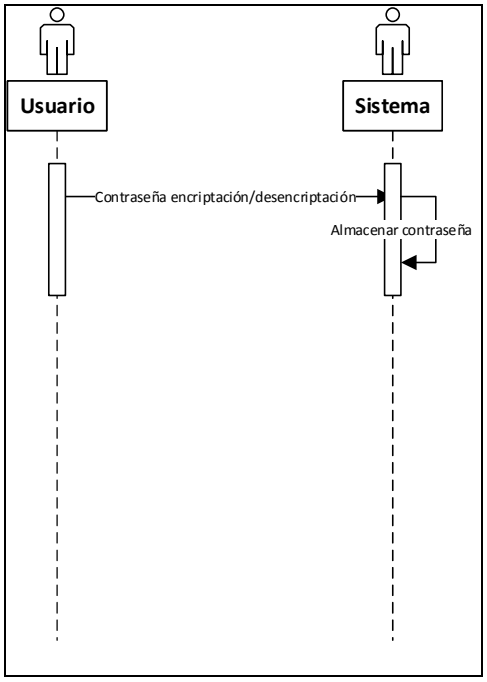


Figura 6: establecer contraseña de encriptación

2.8.4- Comenzar proceso de encriptación

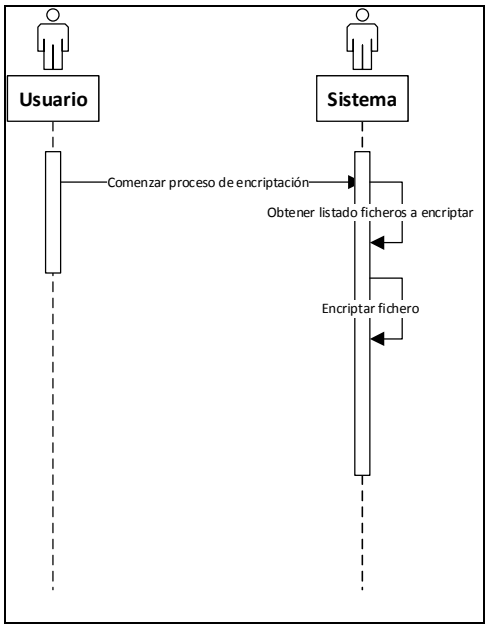


Figura 7: comenzar proceso de encriptación

2.8.5- Detener proceso de encriptación

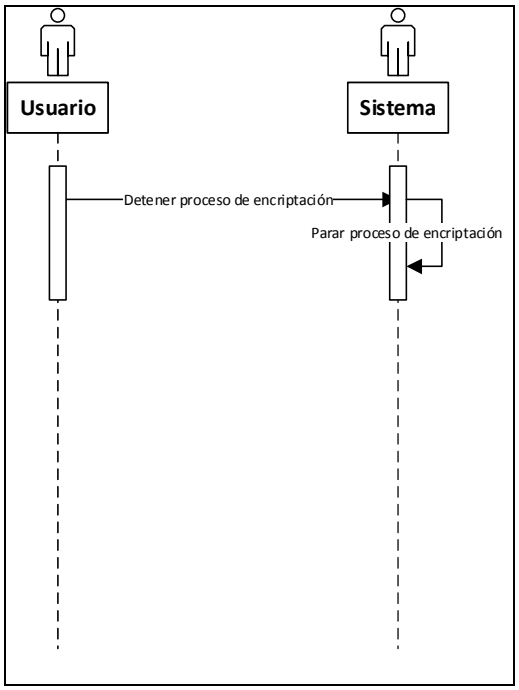


Figura 8: detener proceso de encriptación

2.8.6- Cargar fichero de configuración

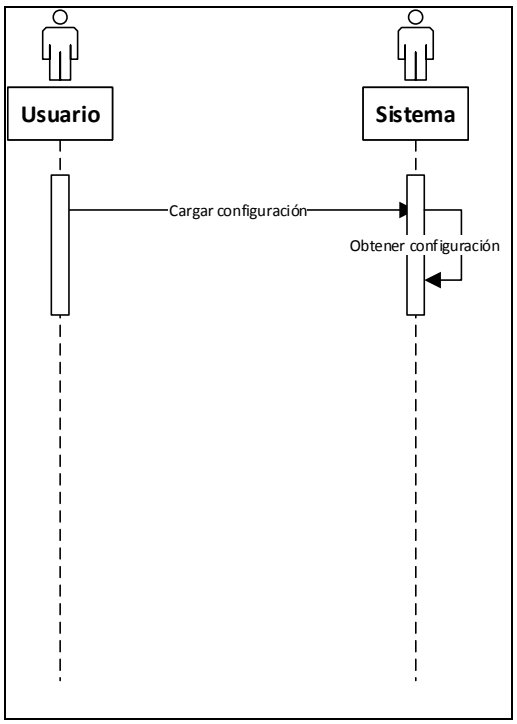


Figura 9: cargar fichero de configuración

2.8.7- Grabar fichero de configuración

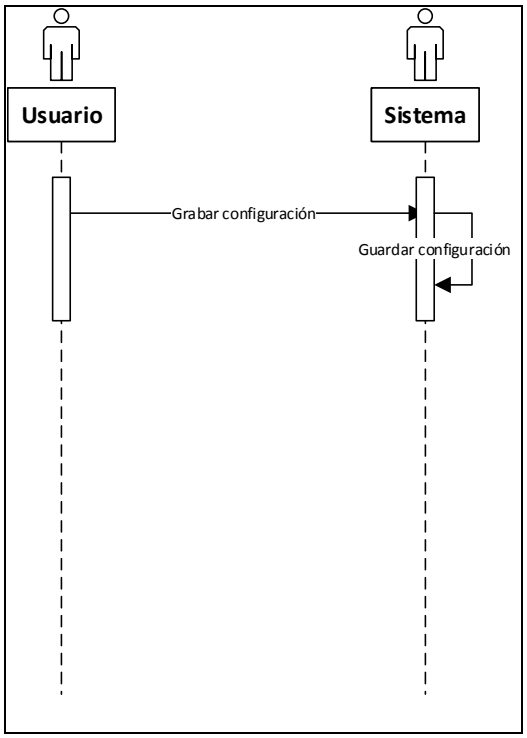


Figura 10: grabar fichero de configuración

2.8.8- Sincronizar directorios

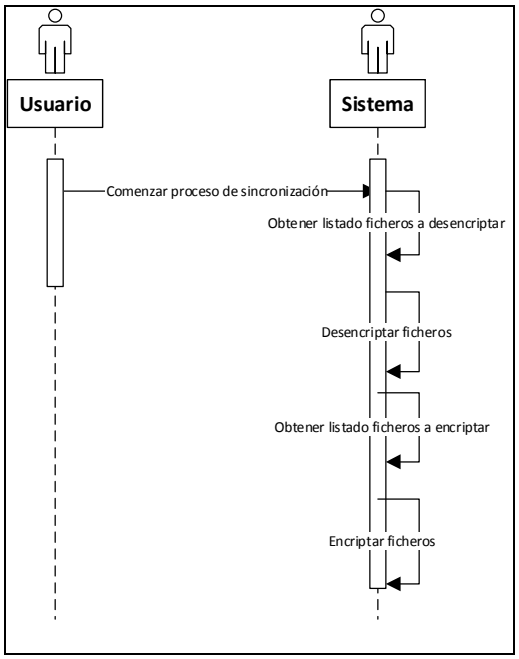


Figura 11: sincronizar directorios

2.8.9- Buscar ruta de fichero no encriptado

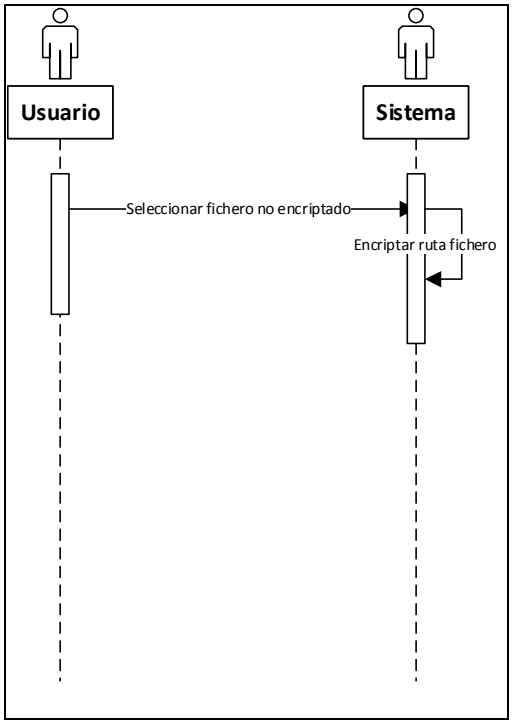


Figura 12: buscar ruta de fichero no encriptado

2.9- Diseño del interfaz

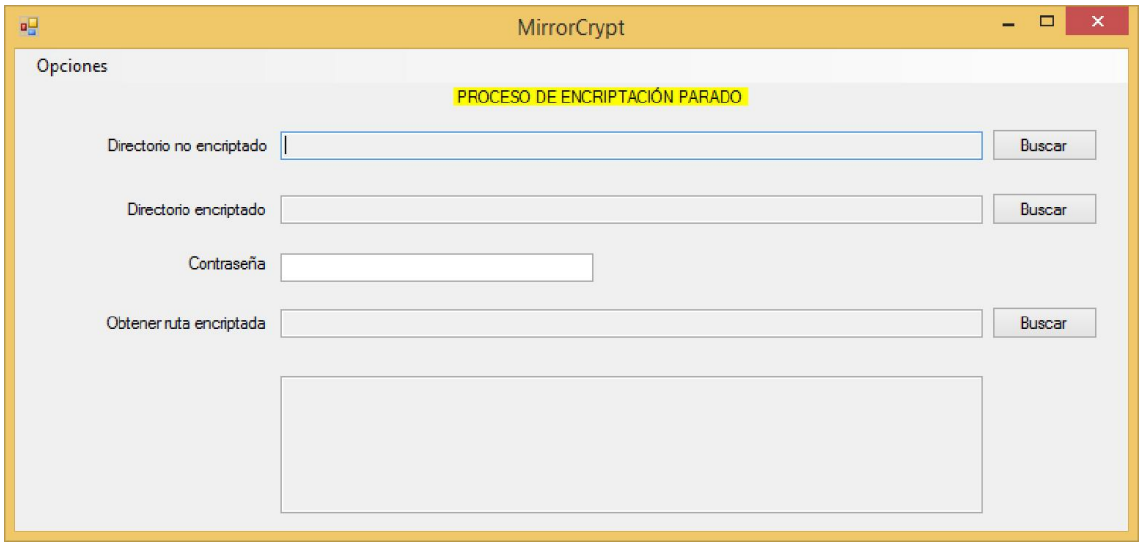


Figura 13: diseño del interfaz principal

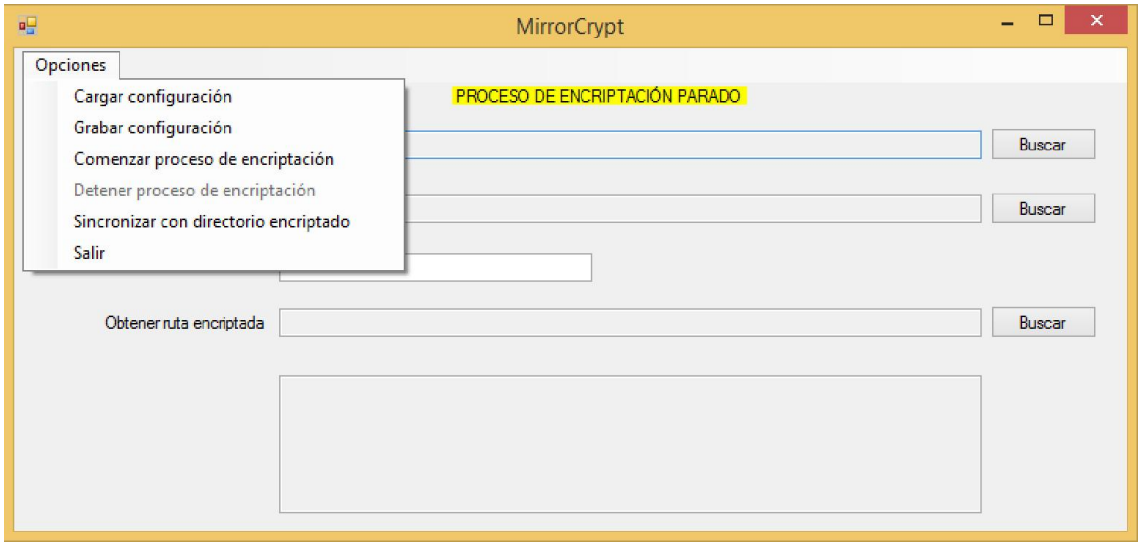


Figura 14: diseño del menú con las opciones principales

2.10- Información técnica de la implementación.

En este punto se va a comentar desde un punto de vista técnico la implementación llevada a cabo.

2.10.1- Algoritmo de encriptación

La aplicación hace uso del algorimo Rijndael, más conocido como AES, en su versión de 256 bits. Este es hoy en día el estándar de encriptación usado tanto por la mayoría de las aplicaciones software como por hardware.

2.10.2- Algoritmo de compresión

La aplicación hace uso del algoritmo Gzip para la compresión de archivos. Se trata de un algoritmo muy usado en aplicaciones software que ofrece un buen equilibrio entre ratio y velocidad de compresión.

2.10.3- Funcionamiento del proceso de encriptación automático

Cuando el proceso de encriptación está activado cualquier cambio que se haga sobre cualquier fichero o directorio de la carpeta no encriptada será automáticamente sincronizado en él. Esto incluye:

- La creación de un directorio o fichero.
- La modificación del contenido de un fichero.
- El borrado de un fichero o directorio.
- El renombrado de un fichero o directorio.
- Copiar o mover un fichero o directorio.

Cuando el proceso de encriptación está áctivo la aplicación funciona como un servicio que está constantemente mirando si se realiza alguna modificación en la carpeta no encriptada, tanto en su raíz como en cualquiera de sus subdirectorios. En el momento que se encuentra alguno de los cambios que se ha enumerado arriba la aplicación automáticamente realiza la misma operación de manera encriptada. Por ejemplo, para la creación:

- Si se trata de fichero:

- Si se trata de un fichero, primero lo comprime en la carpeta temporal del usuario con el nombre original usando el algoritmo GZip. Esto es así porque el fichero encriptado ocupa más espacio que el fichero original, por lo que primero comprime el original intentando que el fichero encriptado ocupe menos o al menos lo mismo ya que éste, debido al contenido que tiene, no es bueno para ser comprimido debido al bajo de ratio de compresión que se obtiene.
- Después se procede a su encriptación en la carpeta encriptada en un nuevo fichero cuyo nombre está encriptado para que no se dé ninguna pista sobre su posible contenido. Por lo tanto, tanto el contenido del fichero como el nombre son encriptados con el algoritmo AES-256.
- Por último el fichero original comprimido es borrado del directorio temporal quedándose sólo el fichero encriptado.

- Si se trata de un directorio

- Crea directamente el directorio en la carpeta encriptada con el nombre encriptado.

2.10.4- Funcionamiento del sistema de sincronización

Una vez que todo el contenido de la carpeta local de un servicio como DropBox o Google Drive ha sido encriptado mediante el sistema de encriptación automático expuesto anteriormente, queda otro paso, y es como realizar la sincronización cuando vayamos a otro equipo.

En otro equipo automáticamente el contenido encriptado alojado en un servicio como DropBox o Google Drive es automáticamente bajado a la carpeta local de la máquina. Por lo tanto ahora el proceso que queda pendiente es el de realizar la desencriptación de ese contenido en otra carpeta de la máquina para que se pueda trabajar con el proceso de encriptación automático.

Sin embargo esto no es tan sencillo como desencriptar el contenido sin más ya que pueden ocurrir que la carpeta desencriptada ya tuviese contenido de una desencriptación anterior por lo que puede darse alguno de los siguientes casos:

a) El fichero en la carpeta destino tiene una fecha de modificación posterior a la del fichero encriptado.
b) Existe un fichero o directorio que no existe en la carpeta encriptada.

El sistema de sincronización se guía por la fecha de modificación de los ficheros para saber qué ficheros debe sincronizar. Éste sólo actualiza los ficheros o carpetas que tengan una fecha de modificación en la carpeta encriptada posterior a la de la carpeta no encriptada.

Para los casos expuestos anteriormente el funcionamiento sería el siguiente:

a) En el caso de que el fichero destino tenga una fecha de modificación posterior –entendiéndose por lo tanto que la modificación fue realizada sin que el sistema de encriptación automático estuviese activo-, el sistema de encriptación, como medida de seguridad, conserva esta versión del archivo sin sobrescribirlo con la versión encriptada. En este caso será responsabilidad del usuario actualizar la versión encriptada con la nueva versión activando la opción de encriptación automática y produciendo algún cambio en el fichero original para que el sistema lo detecte y vuelva a encriptarlo.
b) Este caso plantea un problema. No sabemos si el fichero o carpeta existen porque son nuevos –y fueron creados sin que el sistema de encriptación automática estuviese activo- o no existen en la carpeta encriptada porque se borraron en el otro equipo cuando el sistema de encriptación automática estaba activo. En este caso la aplicación opta por la segunda posibilidad y entiende que si un fichero o carpeta existen en el fichero no encriptado y no existen en el encriptado es porque fueron borrados en el otro equipo, por lo que la aplicación borrará esos archivos. Por ello es siempre muy importante cuando se trabaje con los archivos que el proceso de encriptación automática esté activo.

2.10.5- Estructura de clases

A continuación se van a explicar las clases usadas en la implementación de la aplicación:

- FileCompresor.cs: se encarga de la compresión de los archivos mediante algoritmo GZip.
- FileWatcher.cs: se encarga de monitorizar si se ha producido algún cambio en el directorio no encriptado para reproducirlo inmediatamente en el directorio encriptado. Este proceso corre en su propio hilo de ejecución.

- RecorrerDirectorio.cs: se encarga de realizar la sincronización entre el directorio no encriptado y el encriptado cuando vamos a otro equipo.
- RijndaelFileEncription: se encarga de encriptar con el algoritmo AES 256 el contenido de los ficheros de la carpeta no encriptada.
- RijndaelManagedEncription: se encarga de encriptar con el algoritmo AES 256 los nombres de los ficheros.
- Main.cs: contiene el formulario principal.

2.10.6- Dificultades técnicas durante la implementación

- El mayor problema que se tuvo en la implementación fue el manejo del componente FileSystemWatcher ya que éste producía comportamientos extraños como eventos que se llamaban dos veces seguidos o eventos que se perdían (o no eran disparados). Conseguir que funcionase correctamente llevó mucho tiempo y sin duda alguna ha supuesto el grueso de la implementación.

- Otro de los problemas que se encontró durante la implementación de la aplicación fue que el FileSystemWatcher usado para la monitorización de los cambios producidos en la carpeta no encriptada corre en su propio hilo de ejecución, por lo tanto cuando está activo la aplicación tiene dos hilos de ejecución:
    - El hilo principal bajo el que corre el formulario.
    - El hilo bajo el que corre el FileSystemWatcher.

  Esto supone un problema y es que el hilo del FileSystemWatcher no puede acceder directamente al formulario para mostrar o cambiar algún valor puesto que éste está ejecutándose en otro hilo de ejecución.Llevó un tiempo encontrar la solución mediante el uso del método Invoke del formulario ya que la programación multithreading es casi algo nuevo para mí y obliga a cambiar radicalmente la manera de pensar para una persona que ha trabajado toda su vida en programación tradicional singlethreading.

2.10.6- Limitaciones

Como se ha podido ver, la aplicación hace uso del objeto FileSystemWatcher de .NET para la monitorización de las actividades en el directorio no encriptado. Este objeto tiene alguna limitación que se pasa a comentar a continuación, por lo que la aplicación también presenta la misma limitación:

- Cortar/pegar en la carpeta no encriptada no encripta el contenido de ésta: según menciona Microsoft en su página web[1]:

"The operating system and FileSystemWatcher object interpret a cut-and-paste action or a move action as a rename action for a folder and its contents. If you cut and paste a folder with files into a folder being watched, the FileSystemWatcher object reports only the folder as new, but not its contents because they are essentially only renamed."

Lo que viene a decir que cuando se realiza una operación de cortar/pegar de un directorio en la carpeta encriptada sólo salta un evento de creación del directorio principal, sin saltar ningún evento para sus ficheros y subdirectorios. Debido a ello la aplicación no puede procesar éstos y por lo tanto no son encriptados. Por lo tanto úsese siempre la opción copiar/pegar para mover contenido a la carpeta no encriptada.

2.10.7- Requerimientos técnicos

La aplicación ha sido desarrollada con un Visual Studio 2013 por lo que se ha usado la última versión del .Net Framework disponible, la 4.51. Por ello es necesario tener esta versión instalada para poder ejecutar la aplicación.

Esta versión puede descargarse gratuitamente en la siguiente página:

http://www.microsoft.com/es-es/download/details.aspx?id=40779

[1] http://msdn.microsoft.com/en-us/library/system.io.filesystemwatcher.aspx

2.10.8- Casos de tests

A continuación se muestran los testeos realizados con la aplicación, todos pasados exitosamente:

- Tests de proceso de encriptación automático

Número de test	Descripción	Resultado esperado
001	Crear un fichero en la carpeta no encriptada.	Se creará un fichero nuevo encriptado en la carpeta encriptada.
002	Crear un directorio en la carpeta no encriptada.	Se creará un directorio nuevo encriptado en la carpeta encriptada.
003	Modificar el contenido de un fichero de la carpeta no encriptada.	Se volverá a encriptar el fichero en la carpeta encriptada.
004	Renombrar el nombre de fichero.	Se renombrará el nombre del fichero encriptado.
005	Renombrar el nombre de un directorio.	Se renombrará el nombre del directorio encriptado.
006	Copiar una carpeta con ficheros y subdirectorios a la carpeta no encriptada.	Creará la misma estructura en la carpeta encriptada con los nombres de los ficheros y directorios encriptados, así como su contenido.
007	Borrar un directorio de la carpeta no encriptada.	Borra el directorio encriptado correspondiente de la carpeta encriptada.

008	Borrar un fichero de la carpeta no encriptada.	Borra el fichero encriptado correspondiente de la carpeta encriptada.

- Tests de proceso de sincronización

Número de test	Descripción	Resultado esperado
001	Sincronizar estando la carpeta no encriptada vacía.	Se desencriptarán los archivos de la carpeta encriptada en la no encriptada con la misma estructura.
002	Sincronizar teniendo la carpeta no encriptada archivos con fecha anterior a los de la carpeta encriptada.	Se desencriptarán los archivos de la carpeta encriptada con fecha posterior a los de la carpeta no encriptada machacando éstos.
003	Sincronizar teniendo la carpeta no encriptada algunos archivos con fecha posterior a los de la carpeta encriptada.	Se desencriptarán los archivos de la carpeta encriptada con fecha posterior a los de la encriptada y se encriptarán los archivos de la carpeta no encriptada con fecha posterior machacando los de la carpeta encriptada.
004	Sincronizar teniendo la carpeta encriptada algún fichero que no se encuentra en la carpeta encriptada.	Se desencriptarán los archivos de la carpeta encriptada con fecha posterior a los de la encriptada y los archivos no existentes en la carpeta encriptada serán eliminados.

3. Conclusiones

Desarrollar esta aplicación ha sido un reto importante ya que he tenido que trabajar con tecnologías con las cuales nunca antes había trabajado como el FileSystemWatcher de Microsoft usado para la monitorización de los cambios en el directorio no encriptado.

También ha sido interesante ir viendo el desarrollo e implementación de la solución, de partir de una idea más o menos vaga de lo que se pretendía que hiciera el sistema hasta la implementación en una solución efectiva y funcional.

En resumen, la implementación de este proyecto me ha permitido aprender:

- El uso de tecnologías como el FileSystemWatcher y el Microsoft Visual Studio 2013.
- Aprender cómo se puede acceder a los controles del formulario desde un hilo de ejecución diferente a aquel en el que se está ejecutando el formulario.
- Administrar los tiempos en base a las estimaciones realizadas.
- Introducirme en un campo tan interesante de la seguridad informática como es la encriptación de información.
- Ser capaz de manejar las adversidades técnicas surgidas durante el desarrollo del proyecto.

Los objetivos previstos al comienzo de este proyecto han sido resueltos satisfactoriamente. Se ha conseguido crear una aplicación que automáticamente es capaz de replicar cualquier modificación realizada en un directorio en otro de manera encriptada y además comprimiento el archivo original para que el tamaño del fichero encriptado sea más óptimo. Además se ha conseguido el que al ir a otro equipo el contenido de la carpeta encriptada pueda ser sincronizado con la carpeta no encriptada del equipo, desencriptando el contenido de la carpeta encriptada en la carpeta no encriptada, manteniendo los archivos originales

modificados con posterioridad a las fechas de sus correspondientes ficheros encriptados.

Por lo general las estimaciones se han ido cumpliendo aunque alguna vez se ha tenido que realizar alguna modificación, principalmente debido a los problemas técnicos encontrados en el desarrollo de la aplicación que han ocasionado que la fase de desarrollo se alargase más de lo previsto.

Respecto a posibles mejoras y futuras líneas de trabajo sería posible trabajar en desarrollar un sistema de sincronización más complejo del usado actualmente. Ahora mismo el sistema usado para la sincronización de los ficheros entre la carpea encriptada y la no encriptada se guía por la fecha de modificación de los ficheros. Esto acarrea una seria de problemas como por ejemplo no saber si cuando un archivo existe en la carpeta no encriptada pero no aparece en la carpeta encriptada si se debe a que el fichero original fue eliminado en otro equipo o si se trata de un nuevo fichero creado sin que el sistema de encriptación automático estuviese activo.

También acarrea el problema de que cuando los ficheros encriptados son desencriptados en la carpeta no encriptada obtienen una fecha de modificación posterior a la de los ficheros encriptados, pues evidentemente se realiza en un momento posterior. Si posteriormente queremos lanzar un proceso que actualice en la carpeta encriptada los archivos no encriptados que tienen una fecha de modificación posterior -por si se hubieran modificado ficheros sin que el sistema de encriptación estuviese activo-, nos encontramos con el problema de que todos los ficheros desencriptados volverían a ser encriptados porque su fecha de modificación es posterior, lo cual es evidentemente un fallo de optimización.

En este punto se recomienda una posible línea de trabajo sobre este aspecto que podrían ayudar a resolver alguno de estos problemas:

- En lugar de guiarse por la fecha de modificación del fichero guiarse por su checksum, por ejemplo usando un algoritmo CRC-32. Es decir, que independientemente de la fecha, lo que se busque realmente es si el

fichero ha sufrido alguna variación en su contenido comparando el contenido de ambos ficheros, el original y el encriptado (que evidentemente debería de ser desencriptado y descomprimido antes en alguna ruta temporal para poderlo comparar). Aunque esto haría que el proceso de sincronización tardase bastante más al tener que realizar este proceso fichero a fichero (habría que hacer pruebas de rendimiento para ver si el tiempo empleado entra dentro de lo que consideraría aceptable) sería un modo eficaz de saber realmente qué ficheros deberían ser desencriptados y cuáles deberían de volver a ser encriptados.

4. Glosario

- **GZip**: se trata de un formato de compresión de archivos mediante el algoritmo Deflate
- **LHA**: se trata de un algoritmo de compresión de archivos sin pérdida de información basado en el algoritmo LZSS.
- **AES**: también conocido como Rijndael, es un estándar de cifrado de información muy usado en la actualidad.

5. Bibliografía

1. TrueCrypt - Free Open-Source On-The-Fly Disk Encryption Software for Windows 7/Vista/XP, Mac OS X and Linux [Internet]. [cited 2014 Apr 8]. Available from: http://www.truecrypt.org/

2. DiskCryptor wiki [Internet]. [cited 2014 Apr 10]. Available from: https://diskcryptor.net/wiki/Main_Page

3. encfs - www [Internet]. [cited 2014 Apr 10]. Available from: http://www.arg0.net/encfs

4. Axantum Software AB | AxCrypt | File Encryption Software [Internet]. [cited 2014 Apr 10]. Available from: http://www.axantum.com/axcrypt/

5. WinRAR archiver, a powerful tool to process RAR and ZIP files [Internet]. [cited 2014 Apr 10]. Available from: http://www.rarlab.com/

6. 7-Zip [Internet]. [cited 2014 Apr 10]. Available from: http://www.7-zip.org/

7. Boxcryptor | Encryption for cloud storage | Window, Mac, Android, iOS | boxcryptor.com [Internet]. [cited 2014 Apr 10]. Available from: https://www.boxcryptor.com/

8. Cloudfogger - Free File Encryption for Dropbox and the Cloud [Internet]. [cited 2014 Apr 10]. Available from: https://www.cloudfogger.com/en/

6. Anexos

6.1- Manual de usuario

6.1.1- Selección de carpetas y contraseña

En la pantalla de la aplicación seleccione la ruta del directorio no encriptado pulsando en el botón de buscar. Este directorio será con el que trabajemos normalmente.

A continuación seleccione la ruta del directorio encriptado. En este directorio se duplicará como en un espejo todo lo que hagamos sobre el directorio no encriptado, sólo que lo hará de manera encriptada. Así si creamos un archivo, lo creará de manera encriptada. Si copiamos una carpeta con subcarpetas y ficheros creará exactamente la misma estructura de manera encriptada, encriptando también los nombres de los ficheros para que no pueda saberse el contenido.

Por último introduzca la contraseña de encriptación/desencriptación. Esta contraseña será usada para encriptar los ficheros de la carpeta no encriptada y será usada también para desencriptarlos cuando se seleccione la opción de sincronización. A la hora de sincronizar los ficheros si la contraseña de encriptación es incorrecta no podrá desencriptarlos.

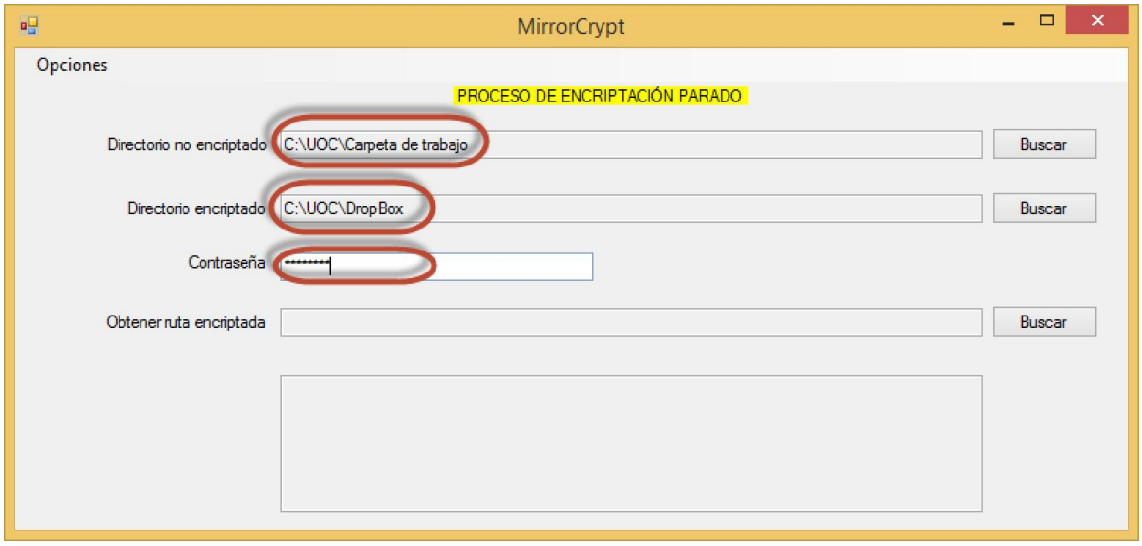


Figura 15 Selección de carpetas y contraseña

6.1.2- Grabación de la configuración

Para no tener que introducir cada vez las carpetas de trabajo se puede grabar dicha configuración. Para ello en el menú Opciones seleccione "Grabar configuración".

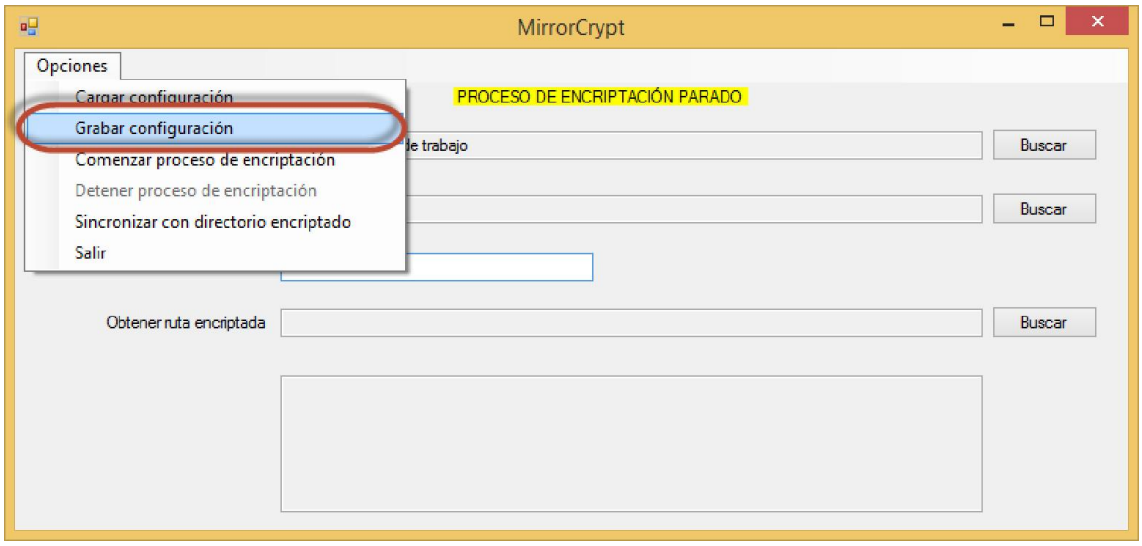


Figura 16 Grabar configuración

Aparecerá una ventana en la que se nos pedirá seleccionar la ruta donde grabar el fichero de configuración. Introduzca el nombre y grabe la configuración.

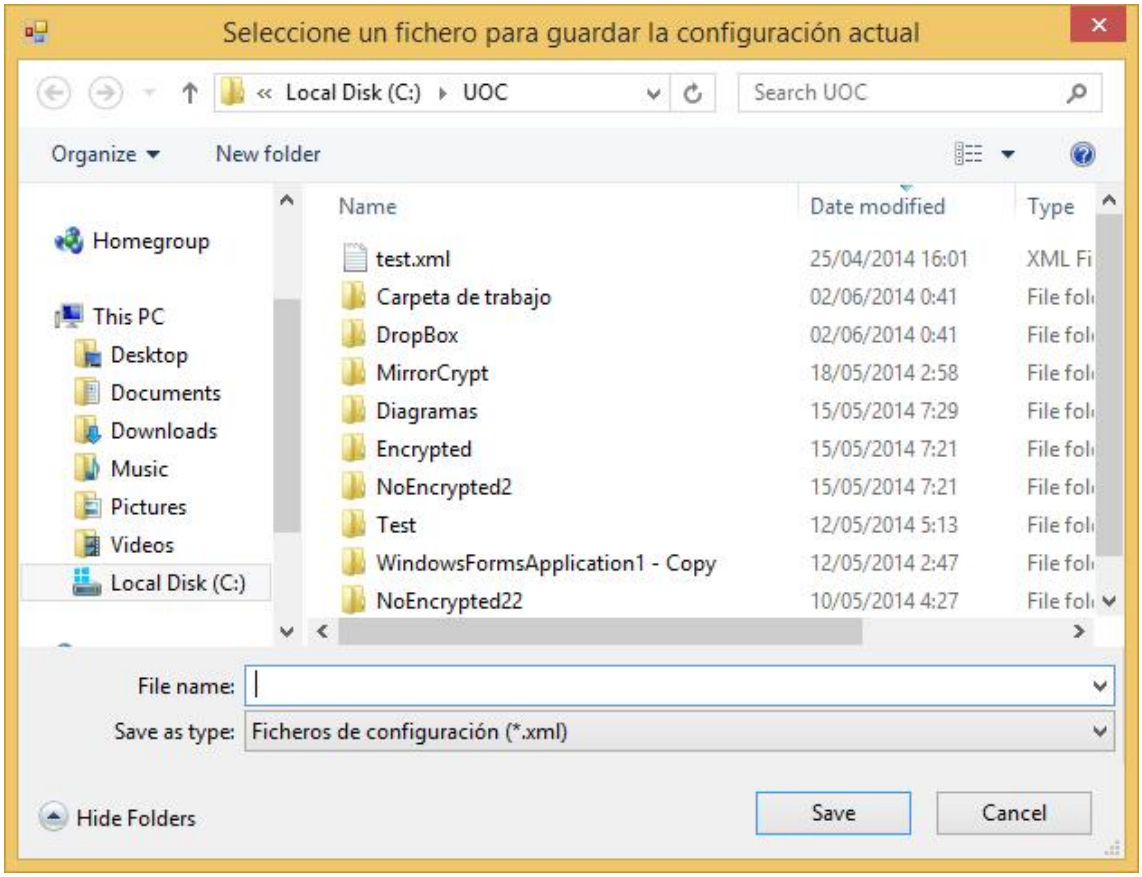


Figura 17 Selección de fichero para guardar la configuración

6.1.3- Carga de la configuración

Si tenemos una configuración guardada no hará falta que tengamos que introducir cada vez los directorios de trabajo. Para cargar una configuración seleccione en el menú Opciones “Cargar configuración”.

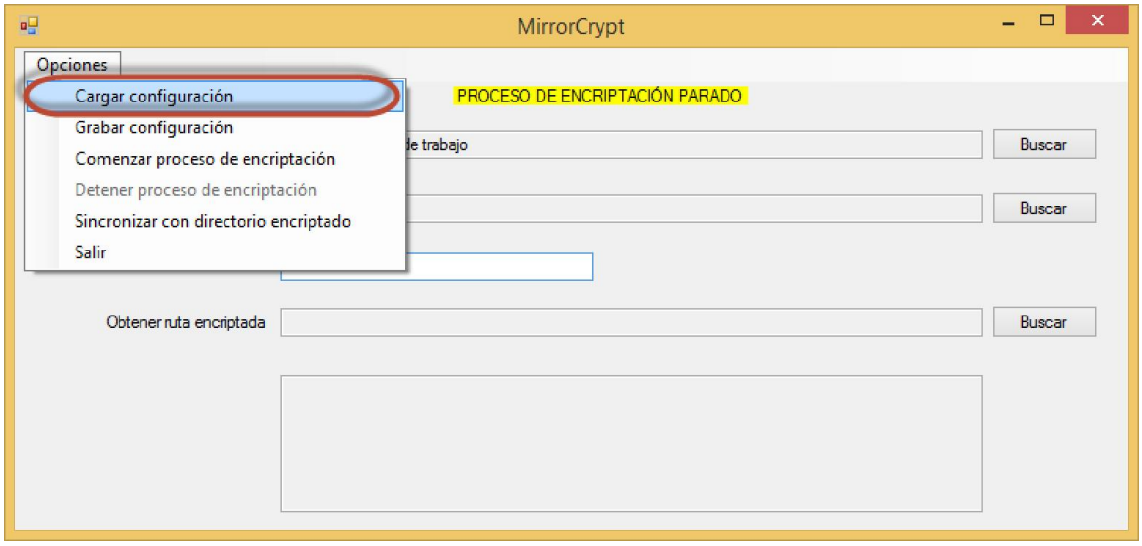


Figura 18 Cargar la configuración

Aparecerá una ventana para que seleccionemos un fichero de configuración. Seleccionamos uno y lo abrimos.

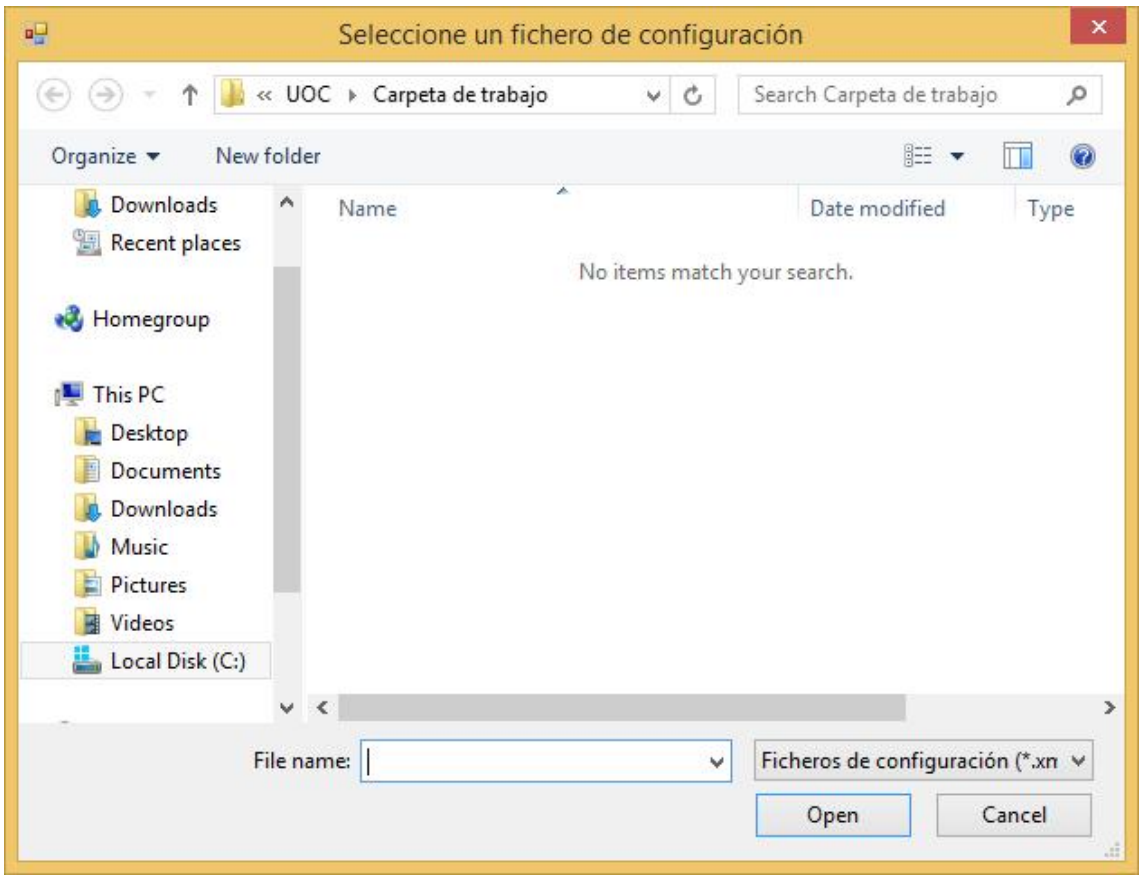


Figura 19 Selección de fichero de configuración para cargarlo

6.1.4- Comenzar proceso de encriptación

Para que comience el proceso de encriptación automático y que por lo tanto todo lo que realicemos en el directorio no encriptado se replique automáticamente de manera encriptada en el directorio encriptado se debe activar el proceso de encriptación.

Para ello iremos al menú Opciones y seleccionaremos “Comenzar proceso de encriptación”, desde este momento cualquier cambio que hagamos en el directorio no encriptado se replicará de manera encriptada en el directorio encriptado.

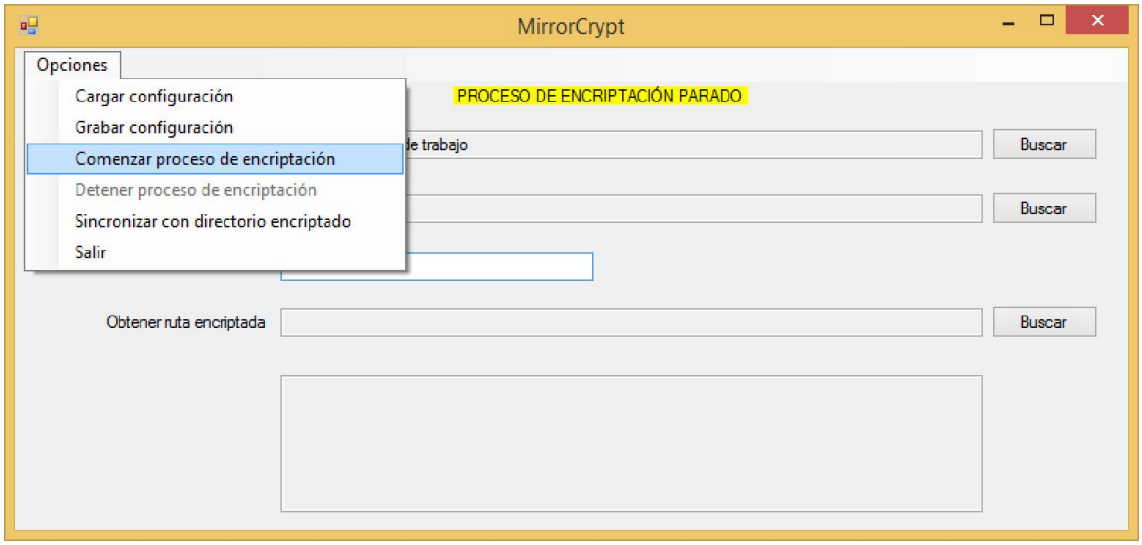


Figura 20 Comenzar proceso de encriptación

Como se puede ver en la siguiente imagen, automáticamente al crear el fichero ReadMe.txt en la carpeta no encriptada se ha creado el mismo fichero con el contenido y el nombre encriptados en la carpeta encriptada. Cualquier modificación del fichero original, tanto en su nombre como en su contenido, será automáticamente replicado en el fichero encriptado.

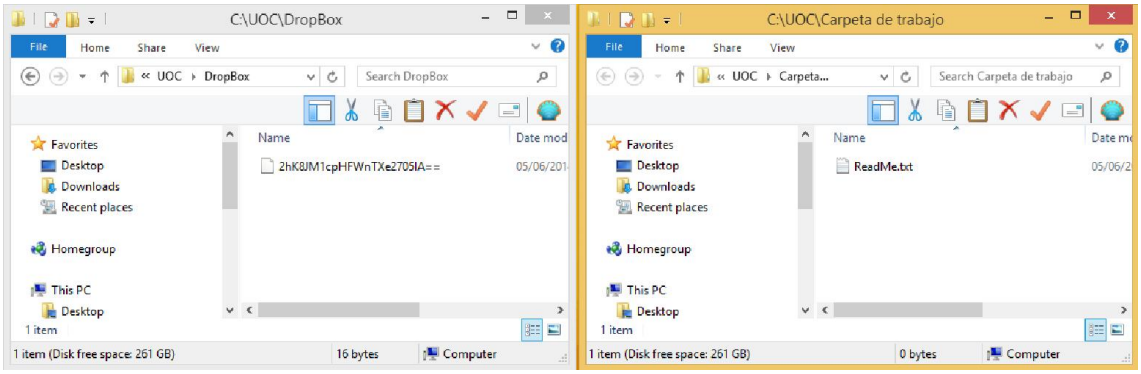


Figura 21 El fichero ReadMe.txt es automáticamente encriptado en la carpeta encriptada

6.1.5- Detener proceso de encriptación

Si por cualquier razón quisiéramos detener el proceso de encriptación automático bastará con seleccionar en el menú Opciones "Detener proceso de encriptación", desde ese momento el sistema automático de encriptación quedará parado.

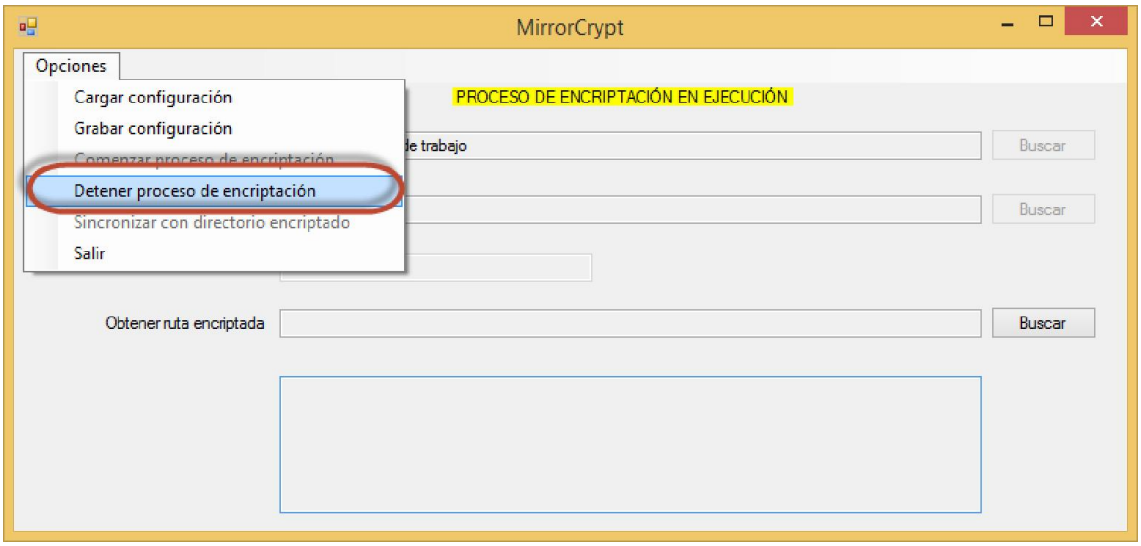


Figura 22 Detener proceso de encriptación

6.1.6- Sincronizar con directorio encriptado

Cuando vayamos a otro equipo y se descarge el contenido encriptado en la carpeta de trabajo de un servicio como DropBox deberemos primero de desencriptarlo a una carpeta local de trabajo para poder trabajar con él. Para ello

habiendo introducido la ruta de los dos directorios, encriptado y no encriptado, y la contraseña de encriptación/desencriptación seleccionamos en el menú Opciones “Sincronizar con directorio encriptado”. Al hacerlo automáticamente veremos que se comienza a crear en el directorio no encriptado la misma estructura de directorios y ficheros encriptados que existe en la carpeta encriptada pero en este caso de manera desencriptada, pudiendo acceder por lo tanto a los contenidos originales. Es importante que la contraseña de desencriptación sea correcta o sino la aplicación no será capaz de desencriptar los ficheros.

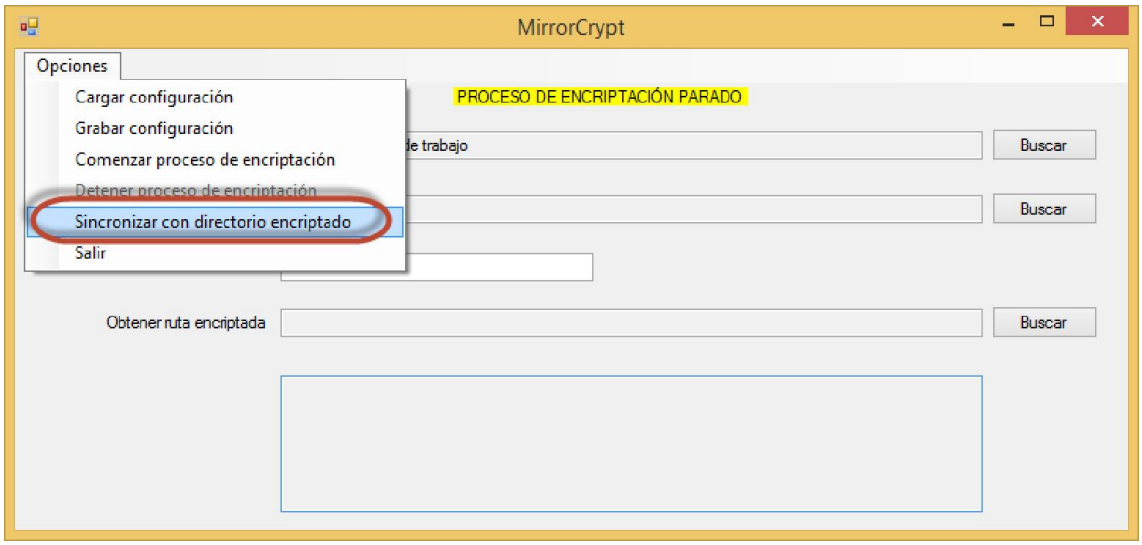


Figura 23 Sincronizar con directorio encriptado

Esta opción debe de ser usada cada vez que cambiemos de equipo y queramos sincronizar los contenidos. Lo que hará este proceso es desencriptar los ficheros encriptados en el directorio no encriptado. Como medida de seguridad los ficheros con una fecha de modificación posterior a la del fichero encriptado no son sobrescritos ya que se entiende que han sido modificados posteriormente sin que estuviese activo el sistema de encriptación automática. En este caso es el usuario quien tendrá que sincronizar manualmente las nuevas versiones de estos ficheros con la del directorio encriptado activando la opción del proceso de encriptación automático y realizando alguna modificación en esos ficheros para que automáticamente, ya con el sistema activo de encriptación, la aplicación los encripte automáticamente sobreescribiendo los ficheros encriptados con fecha anterior.

Es importante destacar en este punto que lo que prima es el contenido del directorio encriptado. Por lo tanto si la aplicación se encuentra a la hora de sincronizar con un fichero o directorio en la carpeta encriptada que no existe en la carpeta no encriptada lo borrará ya que entenderá que se trata de un fichero o directorio que en el otro equipo fue borrado con el sistema de encriptación automática activo, y que por lo tanto a la hora de sincronizar en otro equipo debe de ser eliminado.

Si la clave de desencriptación aportada no es correcta no se podrán desencriptar los archivos y el siguiente mensaje de error será mostrado:

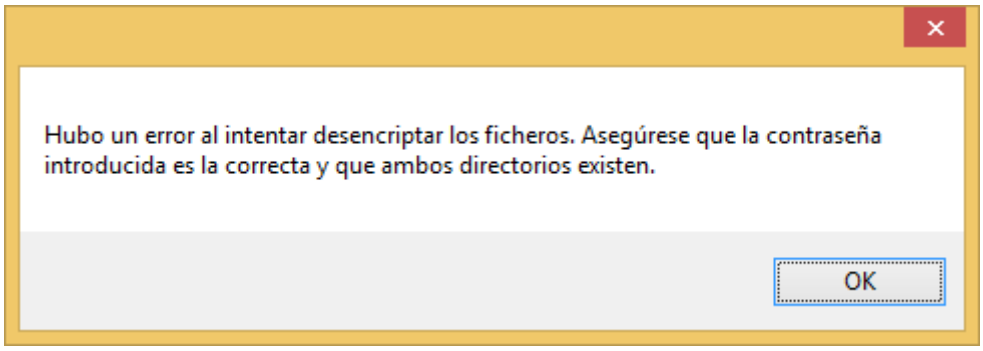


Figura 24 Mensaje de error en caso de que la contraseña de desencriptación sea inválida

6.1.7- Obtener ruta encriptada

Esta opción nos permite averiguar el nombre encriptado y la ruta completa encriptada de un fichero. Para ello tras pulsar el botón de Buscar aparecerá una ventana en la que se mostrará el contenido de la carpeta no encriptada. Tras seleccionar alguno de los ficheros de esta carpeta, o subcarpetas, mostrará la ruta de la carpeta encriptada donde se encuentra dicho fichero.

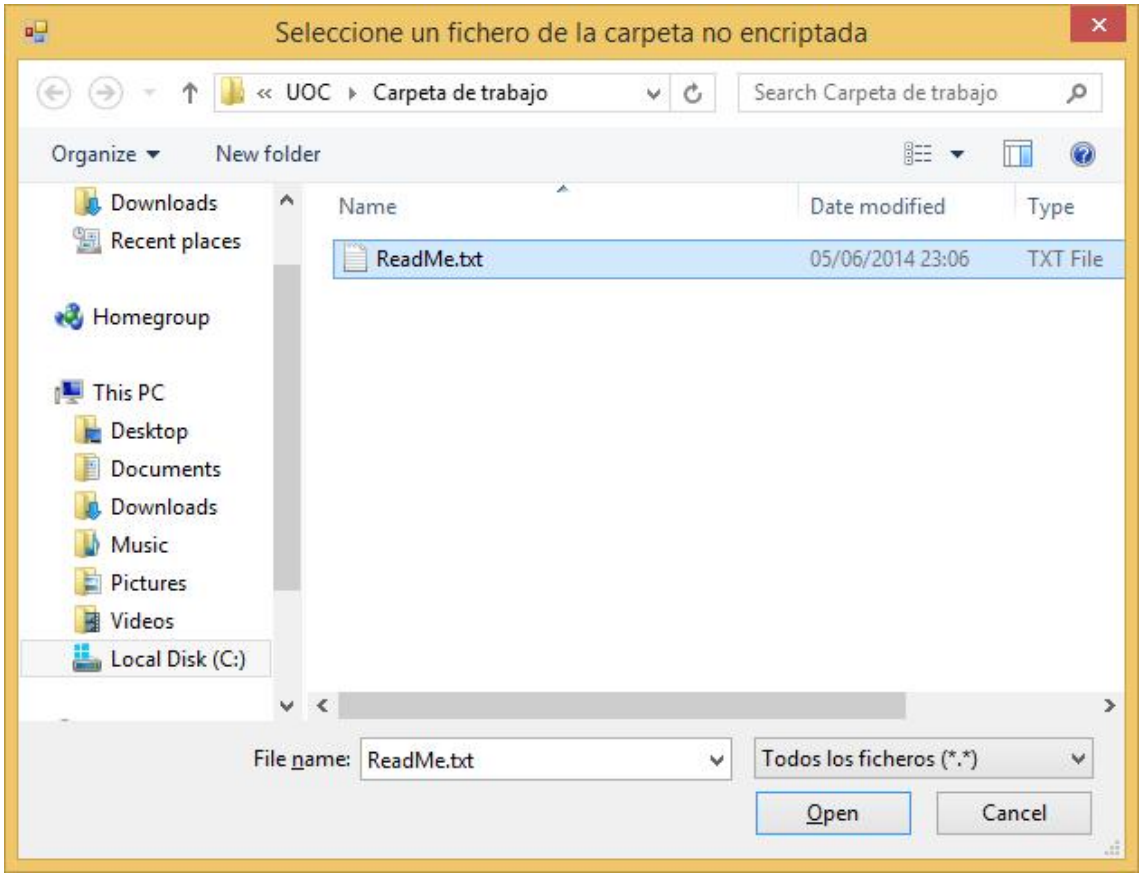


Figura 25 Selección de fichero no encriptado para ver la ruta del encriptado

Figura 26 Se muestra la ruta del fichero no encriptado y la de su correspondiente en la carpeta encriptada