MANUAL DE USO DE LA APLICACIÓN

EnCifra Box 2.0

Marzo de 2014

Objetivos de la Guía

El objetivo de este presente documento es el de servir como una guía fácil y completa de la utilización de la aplicación de consigna **EnCifra Box** como sencilla herramienta de cifrado utilizable en diferentes ámbitos, como pueden ser las carpetas en discos fijos de los equipos, las unidades móviles de almacenamiento, las memorias USB o SD, etc.

Así mismo, esta aplicación es compatible con el hecho de que la carpeta elegida forme parte de un sistema de sincronización de ficheros al estilo de Dropbox[1]. En este caso, el usuario debe tener ya instalado Dropbox y su carpeta sincronizada antes de utilizar la aplicación. Cómo se hace esa operación es muy sencilla, y aparece bien explicada en su página web.

Además de esa posibilidad, **EnCifra Box** permite cifrar el contenido de otras carpetas almacenadas en discos externos, sin importar si se conectan por USB o eSATA con el anfitrión, y que no necesariamente se compartan con el exterior.

Utilizar **EnCifra Box** permite preservar eficazmente la confidencialidad de los datos almacenados en los sistemas operativos **Windows XP**, **Windows 7** y **Windows 8** de Microsoft.

Motivación

Dropbox, al igual que otros ya disponibles y otros que habrán de llegar, es un servicio que permite a sus clientes almacenar ficheros de cualquier naturaleza en "*La Nube*" manteniéndolos sincronizados con los que guarda en su propio equipo, y todo ello de manera muy eficiente y sencilla.

Enviar ficheros a la nube implica perder el control sobre los mismos, no pudiendo nunca estar seguros de cuál será su destino final. Para no prescindir de las ventajas que esa nueva tecnología de deslocalización ofrece y, a la vez, poder estar seguros de que se preserva la confidencialidad de los datos desubicados, **es necesario recurrir al cifrado criptográfico de los mismos**. Los ficheros correctamente cifrados sólo los pueden abrir aquellos que tengan la clave de descifrado correcta.

La aplicación de consigna **EnCifra Box** se encarga de proteger la confidencialidad de los datos que se sincronizan con la nube cifrando, fichero a fichero, cada uno de ellos antes de que se salgan de su equipo. Una vez cifrados los ficheros en el repositorio local, será Dropbox, o cualquier otro servicio de sincronización, el que los lleve a la nube.

---

[1] Ver http://www.dropbox.com/ para más información.

Audiencia de este Documento

Esta aplicación está dirigida a todo tipo de personas e instituciones que deseen o precisen normativamente proteger la confidencialidad de los datos almacenados en un directorio a la vez que son sincronizados con repositorios externos no controlados.

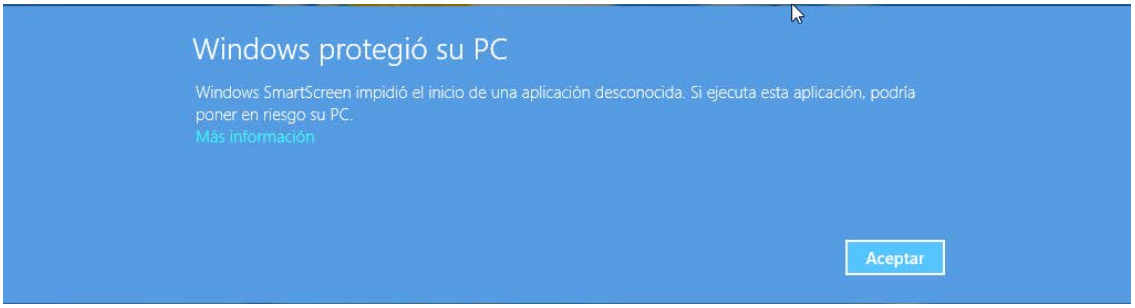
Instalador

El instalador que facilita la compañía EnCifra, una vez aceptadas las condiciones de uso, comprueba si ya hay instalaciones previas de la aplicación EnCifra Box en el equipo y, de no ser así, procede a la instalación de todos sus componentes para que, al final, todo funcione correctamente. Una vez terminado el proceso de instalación, se procede y muestra el proceso de instalación (montaje) de la carpeta vinculada a la nueva aplicación para comprobar que todo ha ido bien.

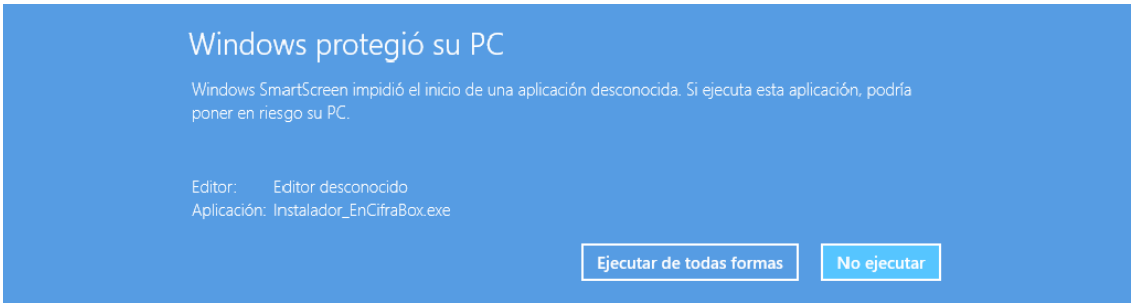
Como proceso de instalación que es, hay que tener en cuenta que **es necesario que el usuario sea administrador del sistema** para que Windows le permita instalar la aplicación.

Si se trata de un **usuario de Windows 8** al ejecutar el instalador deberá seguir los siguientes pasos:

1. Al aparecer la siguiente ventana (SmartScreen[2]), deberá hacer click en "**Más información**".



2. A continuación, haga click en "**Ejecutar de todas formas**".



---

[2] Windows 8 cuenta con un filtro de seguridad llamado Smartscreen el cual se activa cuando se intenta ejecutar una aplicación desconocida; es decir, sin estar firmada por Microsoft como es el caso de EnCifra Box 2.0.

En el proceso de instalación se comprueba si existe una instalación previa de la librería Dokan[3] en el sistema y, en caso de no existir, ofrece la oportunidad de instalarla, cosa que habrá de aceptarse ya que es un componente esencial de la aplicación **EnCifra Box**.

A continuación, el instalador solicita que el usuario seleccione (1) **la carpeta** que tiene sincronizada mediante Dropbox[4] u otra cualquiera, (2) **la contraseña de cifrado** que se utilizará para proteger los ficheros contenidos en ella y (3) la nueva **unidad lógica de disco** en la que queremos que aparezca nuestro directorio con los datos en claro.

Se recomienda encarecidamente asegurarse de que **la unidad de disco en la que vamos a montar los datos en claro no esté ocupada por otro medio**, ni se use habitualmente para ello, ya que podría dar problemas en montajes posteriores.

Una vez configurada la aplicación, se termina el proceso ofreciéndonos la posibilidad de ejecutar la aplicación **EnCifra Box** directamente.

---

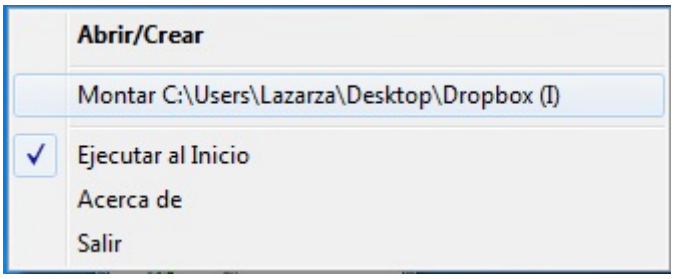
3 Dokan son una serie de bibliotecas que son necesarias para el correcto funcionamiento de la aplicación en el montado de unidades virtuales en el espacio del usuario.

4 También se pueden elegir carpetas que se quieran mantener cifradas y no necesariamente deben estar sincronizadas con el exterior a través de Dropbox.

Funcionalidad y Recomendaciones

EnCifra Box se puede utilizar desde la línea de comandos en un terminal o **a través de un icono**[5] que aparecerá en la barra de notificaciones, a la derecha en la "Barra de Tareas" del escritorio de Windows. Dada su sencillez, se recomienda utilizar la segunda opción, la del icono.

Si se hace doble click sobre el icono que representa **una llave blanca**, se abrirán las opciones disponibles:



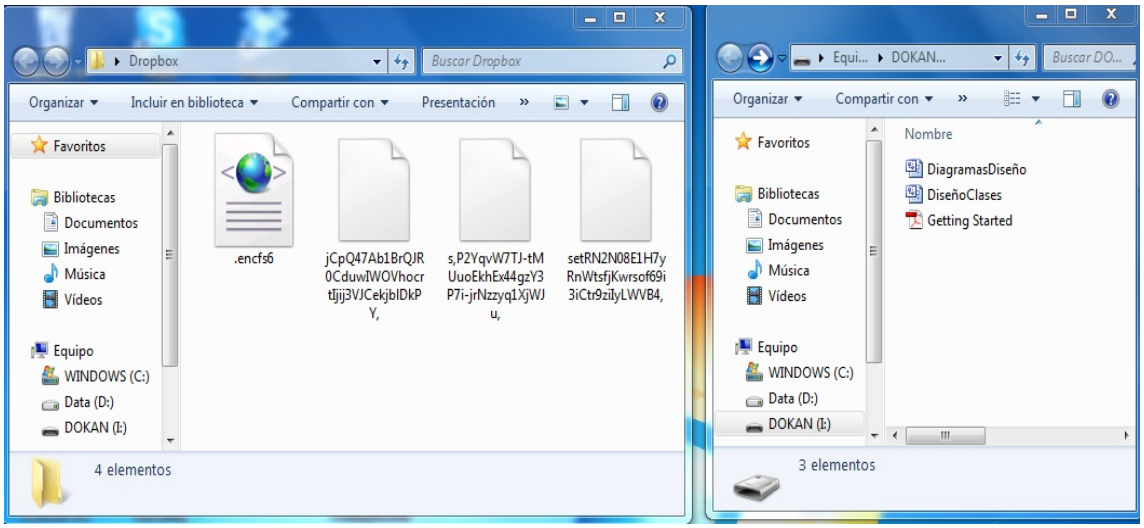
- La funcionalidad principal es la de "***Abrir/Crear***" contendores cifrados y se procede del mismo modo que ya se ha hecho durante la instalación. **Es**

[5] El icono es uno de los pequeños elementos que aparecen en la barra de herramientas del menú de Windows en la parte inferior derecha de la pantalla

importante que el directorio que contendrá los ficheros cifrados[6], haya sido creado previamente y que **no esté abierto**, ya que en caso contrario no proseguirá el proceso.

- También tenemos la opción de "***Montar***" un volumen previamente creado, y así tener acceso en claro a los ficheros cifrados por la aplicación y que son los que realmente se almacenan en el disco. Es en éste volumen donde el usuario debe trabajar con los ficheros protegidos. En contrapunto de esta posibilidad es que, si tenemos algún volumen montado, aparecerá la opción de "***desmontar***".
- Con la operación "***Ejecutar al inicio***" podemos decir que la aplicación arranque automáticamente en el momento de poner en marcha el equipo y arrancar el sistema operativo.
- Por último, la operación "***Salir***" provoca en cierre de la aplicación.

Cuando la aplicación de consigna **EnCifra Box** no se está ejecutando, en el equipo o medio de almacenamiento extraíble sólo queda la carpeta con todos los ficheros cifrados bajo el control de una contraseña que no está en el equipo y que (sólo) conoce el usuario. En ese directorio origen la información está cifrada y los nombres de los ficheros resultan del todo ininteligibles.



A la izquierda de la imagen se muestra la carpeta cifrada, que es la que permanece en el equipo, mientras que a la derecha se encuentra la carpeta del volumen montado con la información descifrada, que sin Consigna no existirá.

Condiciones de uso y Precauciones

Es conveniente saber que, para compartir carpetas cifradas entre distintos usuarios, ya sea a través de sistemas de sincronización de ficheros en La Nube, como a través de unidades comunes de almacenamiento en una red local, todos **los usuarios deberán**

---

[6] En nuestro caso será el directorio Dropbox.

tener correctamente instalada la aplicación EnCifra Box y **utilizar exactamente la misma contraseña** que se estableció a la hora de crear la carpeta que se comparte.

En caso de necesitarlo, se pueden transferir o intercambiar ficheros cifrados entre carpetas cifradas gestionadas por **EnCifra Box siempre y cuando ambas carpetas fuesen creadas con la misma contraseña**.

En el caso de que las unidades cifradas se sincronicen con la Nube a través de aplicaciones como Dropbox, **no es conveniente editar o utilizar los ficheros de la unidad virtual (en claro) con aplicaciones que generen ficheros temporales** ya que eso sobrecarga el sistema de cifrado y descifrado al vuelo y, sobre todo, afecta al sistema de sincronización encargado de subir o recibir cambios desde las versiones almacenadas en la Nube.

Dado que el único elemento secreto de todo el sistema es la contraseña que haya elegido el usuario a la hora de crear la consigna cifrada, **la protección de la confidencialidad de los datos nunca será mayor que la de dicha contraseña**. Cualquiera que conozca esa contraseña podrá tener acceso a los ficheros de los datos. Proteger el secreto e integridad de esa contraseña equivale a proteger esas cualidades de los ficheros almacenados utilizando la aplicación **EnCifra Box**.

Aunque el directorio origen tenga su contenido cifrado, el usuario debe saber que cualquier otra persona con acceso a dicho directorio puede ver cuántos documentos contiene, qué permisos tienen esos documentos, cuál su tamaño aproximado y cuando fue la última vez que se accedió a ellos o fueron modificados. Aunque estas informaciones no desvelan el contenido de los ficheros, si pueden dar información colateral de lo que para el usuario significan.

Debe tenerse en cuenta, además, que **no es conveniente colocar en las carpetas cifradas, ficheros que sean necesarios a la hora de arrancar el sistema operativo** ya que no estarán disponibles por no estar en ejecución la aplicación, y no poder estar montada la correspondiente unidad virtual. Esa imposibilidad de acceso puede causar inestabilidades y errores a ciertas aplicaciones.

Además de todo lo dicho, cabe destacar que la aplicación de consigna **EnCifra Box es una demostración de concepto**, por lo que no se asegura un funcionamiento perfecto en cualesquiera circunstancias y no se recomienda su uso en un ámbito empresarial en el que se trabaje con documentos de importancia destacable. En cualquier caso, una política muy saludable cuando se trabaja con medios de almacenamiento, estén cifrados o no, es **tener una eficaz y disciplinada política de salvaguardias**[7].

[7] Ver, por ejemplo, http://en.wikipedia.org/wiki/Backup