



sdb

safe digital box

?

▪ ¿Puedo estar tranquilo acerca de la información de mi empresa?

▪ ¿Donde puedo poner mis archivos cuando viajo?

▪ ¿Cómo hago llegar esta información confidencial a mis gerentes o clientes?

▪ Necesito un lugar donde depositar archivos al que solo yo y las personas que desee puedan acceder, sin importar donde se encuentren en ese momento.



Él ya tiene Safe Digital Box en su empresa!

¿Qué es Safe Digital Box?

Es un **Cofre Digital**, el cual permite el almacenamiento seguro de archivos confidenciales o críticos para usted o su empresa.

En los mismos podrá usted, sus empleados o clientes almacenar información relevante para su empresa en forma encriptada, y acceder a la misma desde cualquier lugar en el mundo con acceso a Internet a través de sus **Llaves Digitales**. Como también puede ser utilizado desde dentro de su empresa como medida de seguridad para acceder a los datos.

De esta manera, si usted necesita transportar información crítica y no desea que la misma se encuentre alojada en su notebook, pendrive etc., simplemente conéctese a su **Cofre Digital** en el momento que la necesite; utiliza la misma desde su llave digital y luego de utilizarla la elimina de forma completamente segura.

Cada Cofre tiene su correspondiente **Llave Digital** para acceder al mismo.

La misma se ejecuta sobre un pendrive usb y si esta fuera copiada o clonada, NO funcionará aunque sepan su usuario y contraseña.

En el supuesto caso de que esta fuese robada, podrá ser desactivada de forma inmediata, haciendo que sus datos permanezcan seguros.

En todos los casos, los archivos se almacenan y transfieren en forma encriptada utilizando *Advanced Encryption Standard (AES)*.

(AES ha sido adoptado como estándar de encriptación por el gobierno de los **Estados Unidos**)



¿Cómo funciona?

SDB se compone de 2 módulos: el **Servidor** y el **Cliente**.

- **El modulo Servidor:**

Inicialmente se instala el modulo Servidor en un equipo cuyo requisito es que utilice Windows como Sistema Operativo.

Posteriormente se crean los **Cofres Digitales**, los cuales son carpetas dentro del servidor que va a funcionar como repositorio de información y también se crean las **Llaves Digitales** para poder acceder a los mismos utilizando pendrives.

Usando el administrador de Cofres, se toma un usuario de la empresa, se le asigna un **Cofre** en el cual guardará sus archivos, se crea la **Llave Digital** (en ese momento se carga el software cliente al pendrive, se lee de este su ID único y se genera la clave randómica y única para encriptar y desencriptar).

Cada usuario puede tener 2 **Llaves Digitales** validas para acceder a su **Cofre Digital**, no existiendo otra manera de acceder y desencriptar los archivos ahí contenidos; en el caso de que pierda todas sus Llaves esos archivos no podrán ser desencriptados.

Una vez que el usuario envió o recibió información desde su **Cofre Digital**, no queda ningún vestigio de esta en ningún lado ya que las transferencias siempre se efectuaron desde su **Llave Digital**.

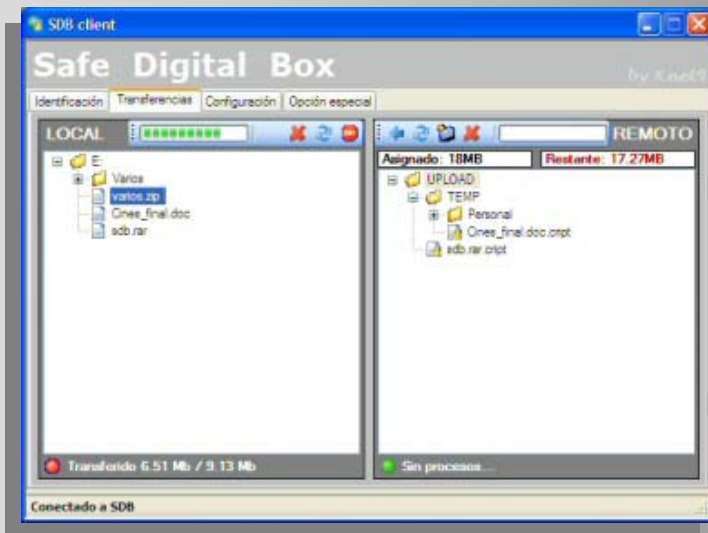
- **El modulo Cliente:**

La aplicación cliente se conecta al servidor ejecutándose desde la **Llave Digital** (pendrive con software de acceso). El mismo contiene un administrador de archivos para poder ver que hay en el **Cofre Digital** y que hay en la **Llave Digital**.

Este es el encargado de hacer la encriptación y upload así como el download y desencriptación de los archivos.

Una vez conectado al Cofre Digital

Pantalla correspondiente al administrador de archivos donde se ve el contenido de la **Llave Digital** (Local) así como del **Cofre Digital** (Remoto).



Si el usuario lo desea puede desde el administrador de archivos borrar contenidos en el Cofre o en la **Llave Digital**, así como también crear carpetas en su **Cofre Digital**.

Para el caso de la información contenida en el Cofre, también tiene disponible las acciones de copiar, cortar y pegar, pudiendo de esta forma manejar libremente la organización de la misma.

También use su Llave Digital como encriptador portátil de archivos!

Con el solo uso del botón derecho del mouse sobre un archivo ubicado en la **Llave Digital**, será capas de encriptar o desencriptar dicho archivo. Podrá utilizar la clave que ya posee su Llave para esta acción o asignarle usted una clave, que deberá recordar, para el encriptado y desencriptado del mismo.

Llaves “hijas”

Cada **Llave Digital** puede tener otras Llaves “hijas”, a las cuales la Llave “padre” puede darles permisos de lectura escritura o solo lectura sobre su **Cofre**, así como generar un archivo de Log de las acciones efectuadas por las mismas. También podrá desactivarlas en el momento que desee.

Opción especial

Esta es una opción para casos extremos en los cuales se necesite borrar toda la información contenida en la Llave, realizándolo de forma totalmente segura y que no permita recuperación posterior por ningún medio.

Dicha opción “auto-destruirá” la misma dejándola como un simple pendrive sin información.

Esta operación **no es reversible** por lo que el usuario que la ejecute deberá poseer otra Llave para poder acceder a la información que tenga en su **Cofre Digital**.

Seguridad

La seguridad de los datos es la esencia de este Sistema, como estos se guardan en forma encriptada y solo se pueden desencriptar (descifrar) en base a la clave contenida en la llave digital, aunque el computador que contiene los cofres fuese vulnerado, no existe forma de acceder a los datos sin las Llaves Digitales.

Como ya fue mencionado, si bien las llaves tienen un identificador único y no es posible clonaras, si alguna de ellas fuera robada, tampoco podrán acceder a los datos ya que necesitan saber usuario y contraseña para poder ingresar; además esa Llave puede ser desactivada inmediatamente.

Cuando el usuario borra datos de la **Llave Digital** utilizando el programa cliente, estos archivos son irrecuperables ya que borra y luego sobrescribe donde estuvieron los archivos. Esto hace imposible la recuperación de la información borrada.

Todas las transferencias a través de Internet en el caso de que lo este usando fuera de la empresa, o en la red local si lo esta usando dentro de la empresa, se realizan en forma encriptada.

Para ello utiliza *Advanced Encryption Standard (AES)*, también conocido como *Rijndael*, el cual es un esquema de cifrado por bloque adoptado como un estándar de encriptación por el gobierno de los **Estados Unidos**.

Además tiene la opción de utilizar HashMD5 *Message-Digest Algorithm 5*, Algoritmo para verificar que el archivo cuando llega es exactamente igual que cuando salió, asegurando que no fue alterado durante la transmisión en Internet o en la red local. Si un solo BIT es cambiado del archivo, una vez que termina la transmisión avisará al usuario que el archivo fue modificado.

www.SafeDigitalBox.com

