CIF-KM: GESTIÓN DOCUMENTAL SEGURA

CIF-KM
MÁXIMA SEGURIDAD

- **Cifrado General:** Archivos almacenados cifrados en el servidor.
- **Cifrado Individual:** Acceso exclusivo a usuarios autorizados, por archivo y necesidad.
- **Uso sencillo**

CIF-KM tiene tres niveles de seguridad para garantizar que sólo los usuarios autorizados disponen de acceso a los archivos almacenados en la gestión documental.

El primer nivel de seguridad es el que proporciona CIF-KM por definición. Como gestión documental, aporta el acceso a la información a través de "Smartbox": fichas de información que reúnen una serie de datos y archivos para su consulta y gestión por un conjunto de usuarios autorizados.

Cada Smartbox incorpora su propio sistema de permisos que determina quienes pueden acceder a su contenido y sus facultades.

Sin embargo, hay ocasiones en las que es necesario disponer de una mayor seguridad que garantice que nadie ajeno al ciclo de vida de los archivos tiene acceso a ellos.

Los archivos sólo se obtienen a través de la aplicación, con permisos.

El Cifrado general evita la fuga de información mediante la copia de archivos en el servidor de CIF-KM.

CIFRADO GENERAL

El cifrado general se presenta como una opción de configuración de servidor de CIF-KM para mantener el repositorio de archivos cifrado, mediante cifrado automático con algoritmo AES de todos los archivos que llegan al servidor, de forma que estos sólo podrán ser visualizados a través de CIF-KM, de acuerdo con las reglas de acceso y permisos de cada uno.

Así, aunque una persona tenga acceso al servidor donde está alojado de CIF-KM, que siempre puede ocurrir, no podrá visualizar ningún archivo almacenado en dicho servidor si no utiliza la aplicación CIF-KM con los permisos adecuados en ella. Evitando de esta forma fugas mediante la copia de archivos.

Sin embargo, para el usuario de CIF-KM todo es transparente, ya que tanto el cifrado como el descifrado de los archivos se realiza de manera automática al cargar o descargar archivos desde la aplicación sin ninguna intervención del usuario.

CIFRADO INDIVIDUAL PARA ARCHIVOS CONFIDENCIALES

¿Qué ventajas tiene el cifrado individual?:

- Un usuario pueda tener en CIF-KM **archivos que sólo él puede descifrar.**
- Un grupo de personas puede colaborar con la **certeza** de que sólo ellas pueden **descifrar los archivos** que utilizan y que se ponen a su disposición.
- Dos o más personas puedan mantener correspondencia con correos electrónicos, avisos o notas de CIF-KM, con **hipervínculos a archivos confidenciales así encriptados**, con la más absoluta seguridad de que sólo ellas pueden visualizarlos, y ninguna persona más, aunque pueda acceder a sus carpetas de correo.

CIFRADO INDIVIDUAL PARA ARCHIVOS CONFIDENCIALES

¿Es un proceso sencillo para el usuario?:

Cifrar y descifrar es muy fácil para el usuario. CIF-KM sólo le pide que elija una palabra, o frase, secreta, que sólo él conozca y que no comunique a nadie.

Cada vez que cifre o descifre un archivo CIF-KM sólo le pedirá al usuario que introduzca la palabra secreta elegida y nada más. Así de sencillo y transparente.

Una vez que el usuario descarga el archivo cifrado CIF-KM lo abre utilizando la aplicación correspondiente (por ejemplo, Microsoft Word) y puede realizar cambios sobre él.

Tan pronto guarde los cambios CIF-KM se encargará de guardar de nuevo el archivo en el servidor, cifrándolo para todos los usuarios con acceso de forma automática y transparente. Siendo posible seguir consultando el historial de cambios de dicho archivo (siempre por usuarios autorizados).

El usuario puede realizar la operación de cifrado o descifrado en cualquier ordenador que tenga instalado el programa cliente de CIF-KM en el que se identifique con su nombre de usuario y contraseña.

¿Quién puede cifrar y descifrar archivos?:

Cualquier usuario que:

- Esté autorizado con la facultad para usar claves de cifrado (mediante configuración de CIF-KM).
- Tenga permisos para subir y/o modificar archivos en el correspondiente Smartbox donde está situado el archivo.
- Esté expresamente autorizado respecto del archivo concreto a descifrarlo, bien porque él lo haya cifrado o bien porque haya sido autorizado por otro usuario que ya estuviera previamente autorizado.

www.cifkm.com/cifrado

¿El sistema de cifrado es robusto y seguro?:

La seguridad es completa ya que depende de que alguien pueda conocer la palabra secreta que haya elegido el usuario, además de la contraseña y nombre de usuario que lo identifica dentro de CIF-KM.

Todo el proceso se realiza por el programa cliente de CIF-KM en el ordenador de trabajo. El servidor de CIF-KM no interviene en los procesos de cifrado y descifrado, sólo recibe y guarda los archivos y claves cifradas.

El acceso se controla individualmente por archivo, incluso dentro del mismo Smartbox, con listas de acceso seguras e independientes para un mejor control de la visibilidad de documentación sensible.

CIF-KM utiliza tecnologías estándar para cifrado mediante claves asimétricas RSA y algoritmo AES Rijndale de 256bits.

GESTIÓN DOCUMENTAL SEGURA

CIF-KM

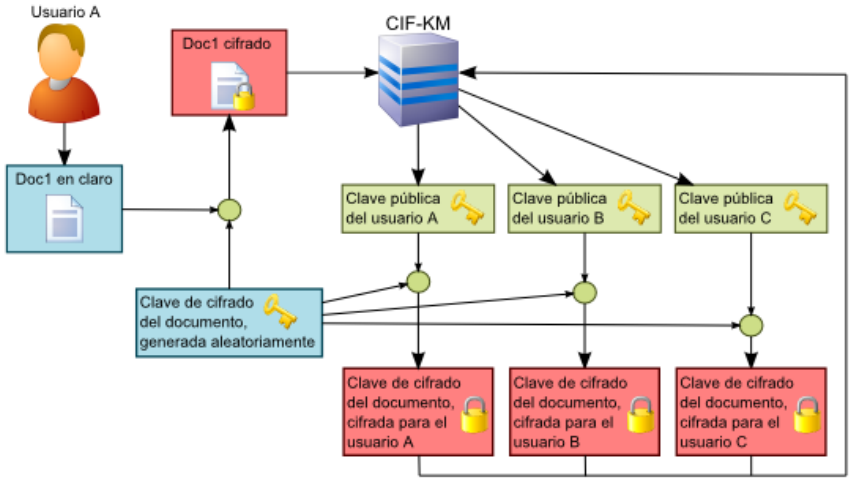
CIFRADO INDIVIDUAL PARA ARCHIVOS CONFIDENCIALES

Funcionamiento:

Para cada usuario autorizado a usar cifrado se generan dos claves aleatorias RSA asimétricas:

- **Clave pública** que permitirá cifrar información para este usuario.
- **Clave privada** con la que este usuario podrá acceder a sus contenidos cifrados.

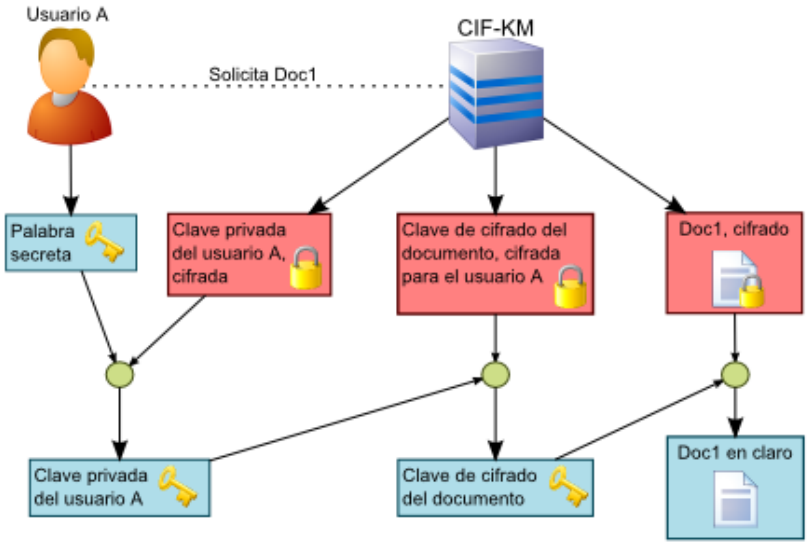
Se solicita al usuario una palabra secreta con la que se cifra mediante AES la clave privada, y se envían al servidor.



Cuando se ordena el cifrado de un archivo, **el programa cliente del usuario** que lo hace **genera una clave aleatoria con la que se cifra el archivo usando algoritmo AES, y dicha clave aleatoria se cifra a su vez con la clave pública de cada usuario** que esté autorizado a acceder a dicho archivo.

CIF-KM SEGURO

EL SERVIDOR NUNCA TIENE ACCESO A LA INFORMACIÓN EN CLARO.



El programa cliente de CIF-KM envía al servidor el archivo cifrado y todas las claves cifradas (el servidor nunca tendrá acceso a la información en claro).

Para acceder a un archivo cifrado el programa cliente solicita al servidor el archivo cifrado, la clave de descifrado de este archivo para este usuario y la clave privada del usuario.

El usuario confirma su acceso introduciendo en el programa cliente su palabra secreta, con la que se descifra la clave de cifrado del archivo y luego este, mostrando el archivo al usuario para que pueda trabajar con él.