HARDkey MIO
Protege tu información

FAQs (¨PREGUNTAS FRECUENTES")

¿Qué beneficios obtengo instalando la HARDkey MIO Security Suite?
La Suite fue desarrollada para ayudarlo a proteger información sensible y confidencial, utilizando un método de seguridad basado en "Dos Factores": "algo que tengo" (su llave HARDkey) y "algo que conozco" el PIN su acceso.

¿Puedo instalar la Suite en más de una computadora?
Si, la licencia de la Suite es en definitiva su llave HARDkey y puede utilizarla en los equipos que desee.

¿Puedo instalar y desinstalar la Suite sin generan inconvenientes?
Si, por supuesto. La Suite no compromete para nada todo lo que contenga su computadora.

¿Cuáles son las mejores opciones para elegir mi PIN?
El PIN debería ser siempre una combinación de números y letras, FACIL DE TIPEAR y RECORDAR, pues esto es importante para la comodidad del esquema, y poder utilizar en forma ÁGIL todos los módulos que le solicitaran el ingreso de su PIN en cada opción importante a nivel seguridad para su información.

¿Qué sucede si alguien encuentra mi llave HARDkey y quiere acceder a mi información?
Si alguien encuentra su llave HARDkey no va a poder utilizarla porque no conoce el PIN de la misma, y luego de una serie de intentos con el PIN incorrecto la llave se bloquea.

¿Cómo puedo protegerme por si se daña o extravía mi llave HARDkey?
La Suite dentro de "Configurar opciones" posee una serie de medidas de seguridad y prevención para estos casos. Una de ellas es permitir hacer un "back up" del contenido de su HARDkey a un archivo "fuertemente cifrado". Este archivo puede ser recuperado en otra llave conociendo la "password " que se utilizó para generarlo. Actualice este "back up" cada vez que haga un cambio, guárdelo en un lugar seguro para utilizarlo cuando lo necesite o para recuperarlo en otra llave HARDkey para obtener un duplicado.
NOTA: La Nueva Suite HARDkey MIO viene con 2 llaves, pudiendo utilizarlas para dos usuarios distintos o una como **Master** y la otra como **Back Up**, y guardar el duplicado en un lugar seguro para cualquier eventualidad.

¿Cómo desbloqueo mi llave HARDkey?
Dentro de "Configurar opciones" se debe definir la cantidad de intentos fallidos de ingreso del PIN deseo permitir antes de que se "bloquee" la llave. Por defecto está seteado en 10, pero se puede elegir entre 3 y 10. Además se deben configurar tres "Preguntas Secretas" que se deberán responder para poder "desbloquear" la llave en caso de haberla "bloqueado" por error o uso no autorizado.

¿Qué sucede si un día me olvido mi llave y necesito utilizar la Suite?
Dentro de cada módulo, en el menú "Archivo" se puede habilitar la generación "automática" de un "archivo imagen" para utilizarlo en estas situaciones. Si se habilita esta opción, recordando sólo el PIN de su llave, podrá usar la Suite en "modo de emergencia" por medio de este archivo.

HARDkey
Protege tu información

FAQ del DISCO CIFRADO

¿Qué tipo de información puedo guardar en mi Disco Cifrado?
La Suite permite almacenar todo tipo de información, archivos e incluso programas en su Disco Cifrado, como por ejemplo documentos Office, imágenes, música, fotos, videos, balances, fuentes de programas, etc.

¿Mi información está realmente segura en un Disco Cifrado?
Toda la información almacenada en un Disco Cifrado está "fuertemente encriptada o cifrada" (esto es totalmente transparente para el usuario) por una implementación certificada del algoritmo de encriptación AES de 256 bits. Está "matemáticamente" comprobado que con la tecnología actual es imposible acceder a la información almacenada en su Disco Cifrado.

¿Cuántos Discos Cifrados puedo crear con mi llave HARDkey de la Suite?
La Suite permite generar y mantener configurados 4 Discos Cifrados, en una misma computadora o en distintas. Si desea tener más discos, podrá hacerlo y acceder "manualmente" cada vez que lo desee por medio de la opción "Inspeccionar discos".

¿De qué tamaño pueden ser los Discos Cifrados que puedo crear con la Suite?
La Suite permite generar Discos Cifrados desde 10 Mega Bytes hasta 1000 Giga Bytes. Igualmente es recomendable crear discos de a lo sumo 60 Giga bytes, para poder manipularlos mejor en procesos de "back up", o copias de seguridad que se quieran realizar de la información protegida en ellos.

¿Cómo puedo realizar una copia de seguridad del contenido mi Disco Cifrado?
Se puede hacer fácilmente un back up de la información protegida en cada Disco Cifrado copiando el archivo generado en al PATH elegido al crearlo a otro equipo o servidor de backup. De esta forma si se daña el disco fijo de la computadora donde está el Disco Cifrado bastará con instalar la Suite y copiar el archivo de respaldo en otra computadora para poder acceder a su información con su llave HARDkey.

¿Si envío a reparar mi computadora pueden ver mi información o perderla?
Nadie puede acceder a su información sin usted no entrega su llave HARDkey y comenta su PIN. Sólo perdería su información si formatean todo su disco, de ser esto necesario pida que antes hagan una copia del "archivo" de su Disco Cifrado.

¿Cuánto puede demorar la creación de un Disco Cifrado?
El tiempo de generación de cada Disco Cifrado varía en función del tamaño del mismo y de las características del hardware y software instalado en su computadora. En promedio se puede decir que el proceso de "cifrado y generación" demora entre 10 y 20 minutos cada 10 Giga Bytes.

¿Se puede modificar el tamaño de mi Disco Cifrado que estoy utilizando?
Si, para hacerlo deberá hacer una "Copia de respaldo" del contenido de su Disco Cifrado, crear uno nuevo con el tamaño que desee y recuperar el "respaldo".

HARDkey
Protege tu información

FAQ del CORREO SEGURO (CS)

¿Cómo utilizo el CORREO SEGURO?
Es muy fácil de instalar y utilizar. Hay que definir los datos personales y de la cuenta de correo a utilizar y luego enviar "invitaciones" por medio de un Email a otras personas que tengan el CORREO SEGURO para armar la base de contactos. En el momento de la configuración inicial se genera un par de claves (una pública y otra privada) que se utilizan para el cifrado de los correos.

¿Qué tipo de servidores de correo soporta el CORREO SEGURO?
Se puede utilizar con cualquier servidor de correo, y tiene configuraciones predefinidas para Outlook, Thunderbird, Gmail y Hotmail. También se puede guardar el correo en un archivo "cifrado" para enviarlo al destinatario por medio de cualquier dispositivo de almacenamiento.

¿Cómo se recibe un CORREO SEGURO?
Se recibe un Email con un archivo adjunto "cifrado", y se puede leer con sólo hacer doble click sobre ese archivo, teniendo su llave HARDkey y tipeando el PIN correcto para habilitar el descifrado del Email.

¿Puedo leer y enviar CORREOS SEGUROS dese distintas PCs?
Si, sólo hace falta instalar la aplicación en cada PC que se desee utilizar usar la llave HARDkey de habilitación correspondiente, no existe limitación para la instalación de la aplicación, ya que la "licencia" es la llave HARDkey de habilitación, y solo el que la posee puede utilizarla.

¿Puedo enviar archivos adjuntos en un CORREO SEGURO?
Si, se puede adjuntar todo tipo de archivos y al enviarlo se cifra junto con el texto del email. Hay que tener en cuenta que si se envían archivos muy grandes va a demorar el cifrado y descifrado en forma proporcional al tamaño de los archivos.

¿Se puede enviar un CORREO SEGURO a más de un destinatario a la vez?
Efectivamente, se puede elegir todos los destinatarios que se quiera de la lista de contactos que se tiene. Incluso al recibir un correo se puede responder, responder a todos, o reenviar.

¿Se tiene acceso a los CORREOS SEGUROS enviados históricamente de alguna forma?
Los correos se guardan cifrados en la "bandeja de enviados" como cualquier otro Email. Para poder abrirlos para releerlos o reenviarlos, para poder abrirlos sólo hay que hacer doble click sobre el archivo que tiene cada CORREO SEGURO enviado, teniendo su llave HARDkey y tipeando el PIN correcto para habilitar el descifrado del Email.

NOTA IMPORTANTE:
Siempre hay una "solución de compromiso entre seguridad y comodidad" y hay que buscar un equilibro entre estos extremos. . Si bien existe la opción de habilitar la generación de un "Archivo Imagen" de la llave en la PC para usarlo en "modo emergencia" al no tener acceso a su llave HARDkey, no es recomendable porque disminuye el nivel de seguridad de la suite. Lo ideal es hacer un back up de su llave HARDkey en otra llave y guardarla en un lugar seguro.