Kripta

Manual de usuario

Cifrado guiado de memorias USB y particiones, con recuperación de la contraseña a través del Help Desk de la empresa.



Versión 1.2 · Windows · macOS · Linux

Noviembre de 2026

Índice

1 Qué es Kripta — para qué sirve, qué necesitas

2 Primer inicio — configuración de la empresa y componentes

3 La ventana principal — indicadores, avisos, icono

4 Cifrar una unidad — el asistente en 4 pasos

5 Dividir un disco en particiones — área cifrada y área libre

6 Usar una unidad cifrada — desbloquear, abrir, bloquear

7 Cambiar la contraseña

8 He olvidado la contraseña — recuperación con el Help Desk

9 Ajustes — idioma, configuración, actualizaciones

10 Usar la unidad en otros ordenadores

11 Mensajes y solución de problemas

12 Preguntas frecuentes

A Apéndice para TI — paquetes, configuración firmada, idiomas

Convenciones

Los textos que aparecen en pantalla (botones, títulos, opciones) se escriben así: **Cifrar una unidad**. Las capturas proceden de la versión para macOS: en Windows y Linux la ventana es idéntica, solo cambian los nombres de los dispositivos (por ejemplo `E:` o `/dev/sdb1` en lugar de `/dev/disk4s1`).

1 Qué es Kripta

Kripta protege los datos de tus **memorias USB** y de las **particiones** de discos externos con cifrado AES-256. Tras el cifrado, el contenido de la unidad solo puede leerlo quien conoce la contraseña: si pierdes la memoria, nadie más puede abrirla.

Cifrado guiado
Cuatro pasos: elige la unidad, elige la contraseña, confirma y espera.

Desbloqueo automático
Al conectar una unidad cifrada, Kripta te pide la contraseña al momento y la abre.

Funciona en todas partes
La misma memoria se abre en Windows, macOS y Linux (formato estándar VeraCrypt).

Instalación autónoma
Kripta instala y actualiza VeraCrypt por sí solo; la configuración de la empresa se importa desde un archivo.

Nueve idiomas
Italiano, inglés, francés, español, alemán, ruso, árabe, chino y japonés, más los que añadas tú.

Recuperación con el Help Desk
Si olvidas la contraseña, el Help Desk puede ayudarte a definir una nueva sin perder datos.

Qué necesitas

- **Kripta** instalado en el ordenador. En el primer inicio Kripta instala por sí solo **VeraCrypt**, el motor de cifrado (en macOS también **FUSE-T**), si falta: capítulo 2.
- El **archivo de configuración firmado** (`.kripta-config`) recibido del Help Desk, si TI no ha configurado ya el ordenador.
- La **conexión a la red de la empresa** (o VPN) cuando cifras una unidad nueva: la clave de recuperación se envía al Help Desk de inmediato. Para desbloquear una unidad ya cifrada no hace falta la red.
- Las **credenciales de administrador** del ordenador, cuando el sistema las pide (ver recuadro).

> **Solicitudes de autorización**
> Para leer y escribir directamente en la unidad, instalar componentes y guardar la configuración, Kripta necesita permisos de administrador. En **Windows** aparece la ventana de Control de cuentas de usuario al iniciar. En **macOS** y **Linux** aparece el mensaje «Kripta necesita la autorización de un administrador para completar la operación». Si TI ha instalado el servicio del sistema de Kripta, estas solicitudes no aparecen.

Cómo funciona la recuperación, en resumen

Durante el cifrado Kripta genera una **clave de recuperación** de 48 cifras, la protege y la envía al archivo del Help Desk. No tienes que verla ni guardarla. Solo los operadores del Help Desk pueden consultarla, tras verificar tu identidad, y cada consulta queda registrada.

2 Primer inicio

En el primer inicio Kripta comprueba dos cosas: si está conectado con el Help Desk de tu empresa y si VeraCrypt está en el ordenador. Si falta algo, en la parte superior de la ventana aparece un aviso con un botón para solucionarlo. Puedes hacerlo todo tú.

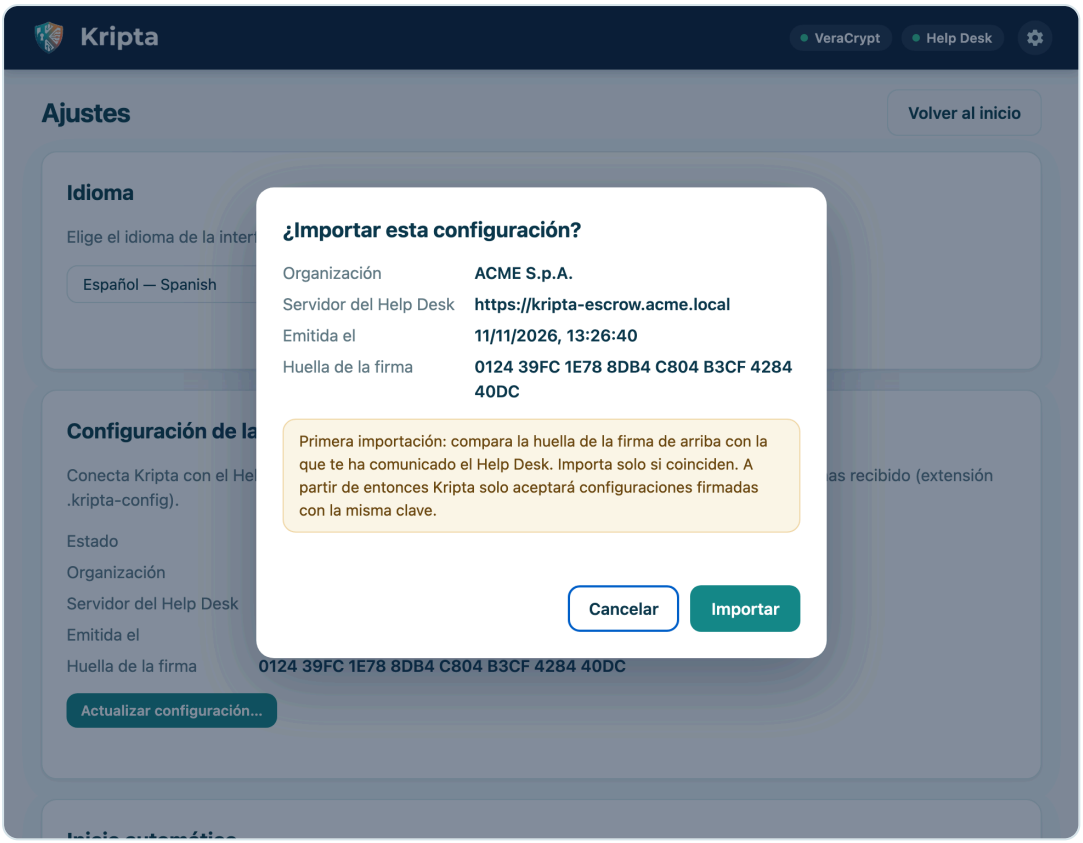


Primer inicio: configuración por importar y VeraCrypt por instalar.

Importar la configuración de la empresa

La configuración indica a Kripta a qué archivo del Help Desk enviar las claves de recuperación. El Help Desk te la entrega como archivo con extensión `.kripta-config`, firmado digitalmente: nadie puede modificarlo sin que Kripta lo detecte.

1. Guarda en el ordenador el archivo recibido (por correo, desde el portal de la empresa o en una memoria).
2. Pulsa **Importar configuración** en el aviso, o abre **Ajustes** (el engranaje arriba a la derecha) y pulsa **Importar configuración firmada…**.
3. Elige el archivo. Kripta verifica su firma y muestra organización, servidor del Help Desk, fecha de emisión y **huella de la firma**.
4. En la primera importación **compara la huella** con la que te ha comunicado el Help Desk (por teléfono, en la intranet…). Si coincide, pulsa **Importar**.
5. Confirma la solicitud de autorización del sistema. Aparece **Configuración importada** y el indicador **Help Desk** se pone verde.

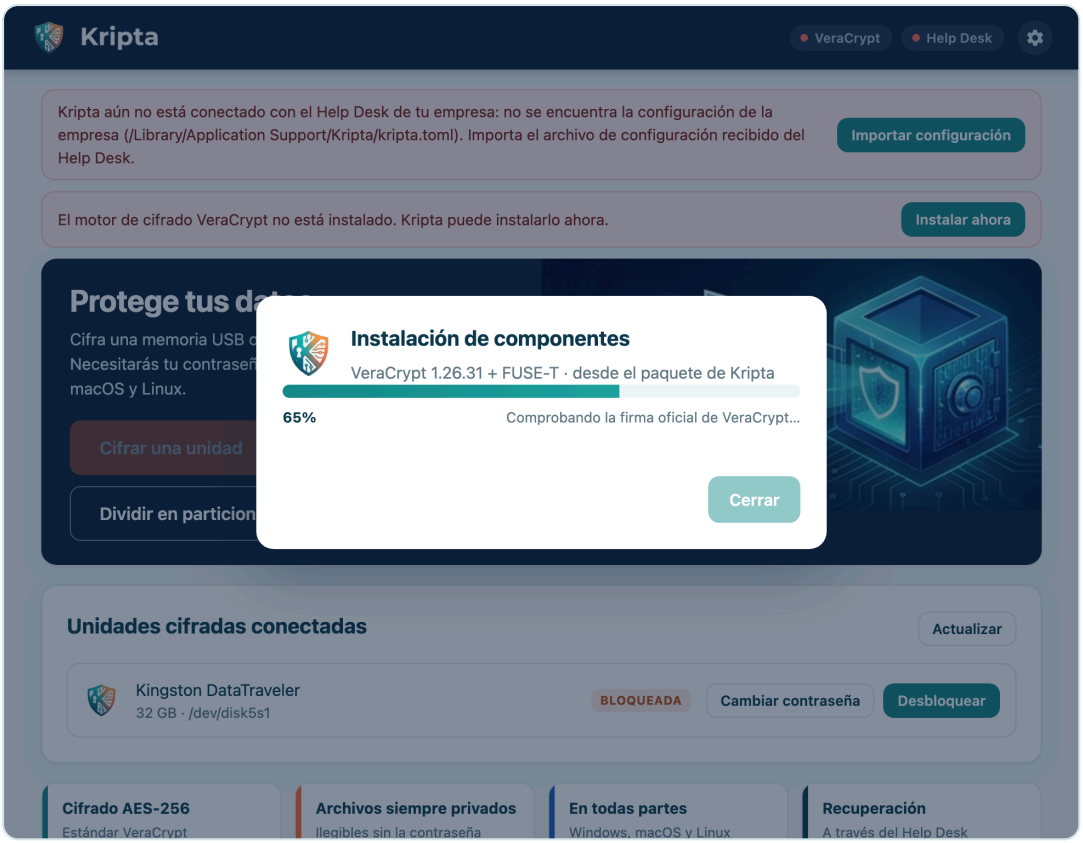


Confirmación de la importación con la huella de la firma.

> **Si la huella no coincide, no importes**
>
> El archivo podría no proceder de tu empresa. Cancela y contacta con el Help Desk. Tras la primera importación Kripta solo acepta actualizaciones firmadas con la misma clave: un archivo falso se rechaza automáticamente.

Instalar VeraCrypt

Kripta ya contiene el instalador oficial de VeraCrypt (y de FUSE-T para macOS). Pulsa **Instalar ahora** en el aviso y confirma la solicitud de autorización: Kripta verifica la firma oficial de los instaladores y los instala sin más preguntas.

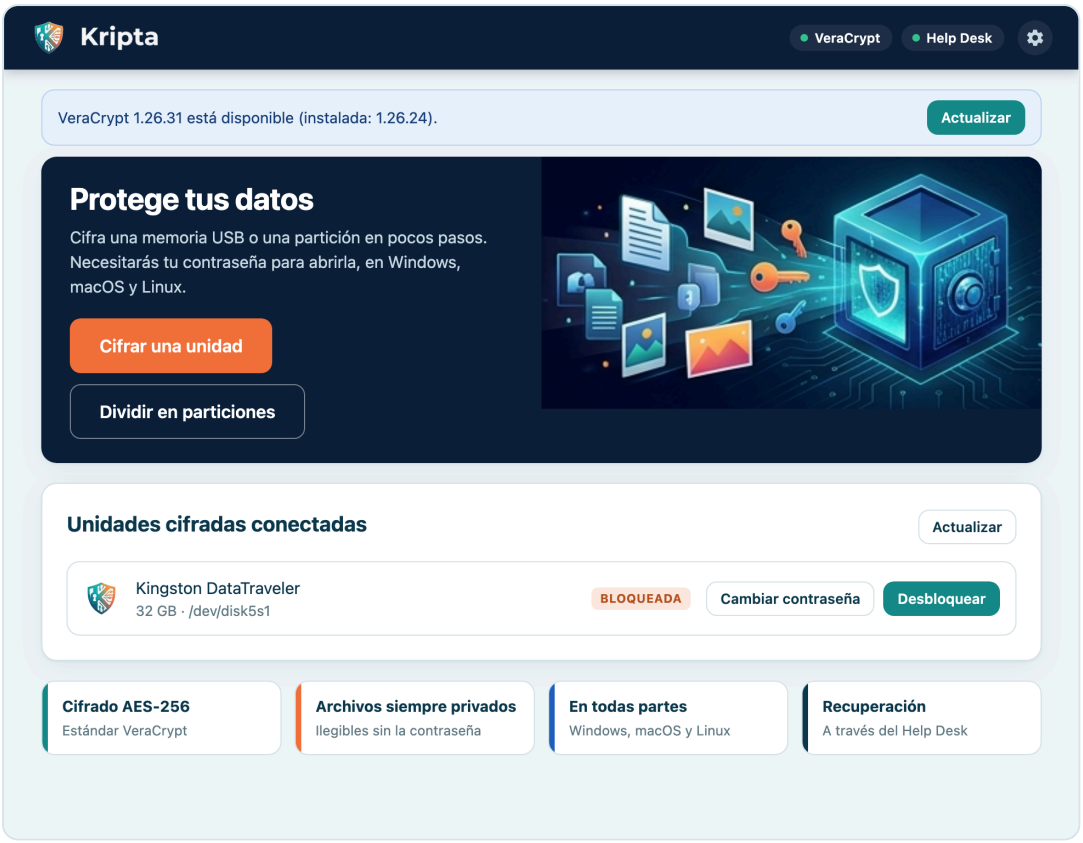


Instalación de componentes con verificación de la firma oficial.

Al terminar aparece **Instalación completada**. En Windows puede pedirse reiniciar el ordenador.

Actualizaciones de VeraCrypt

En cada inicio (y luego una vez al día) Kripta comprueba si hay una versión más reciente de VeraCrypt. Si la hay, aparece un aviso azul con el botón **Actualizar**. La nueva versión se descarga del sitio oficial y solo se instala si la firma de los desarrolladores de VeraCrypt es válida.

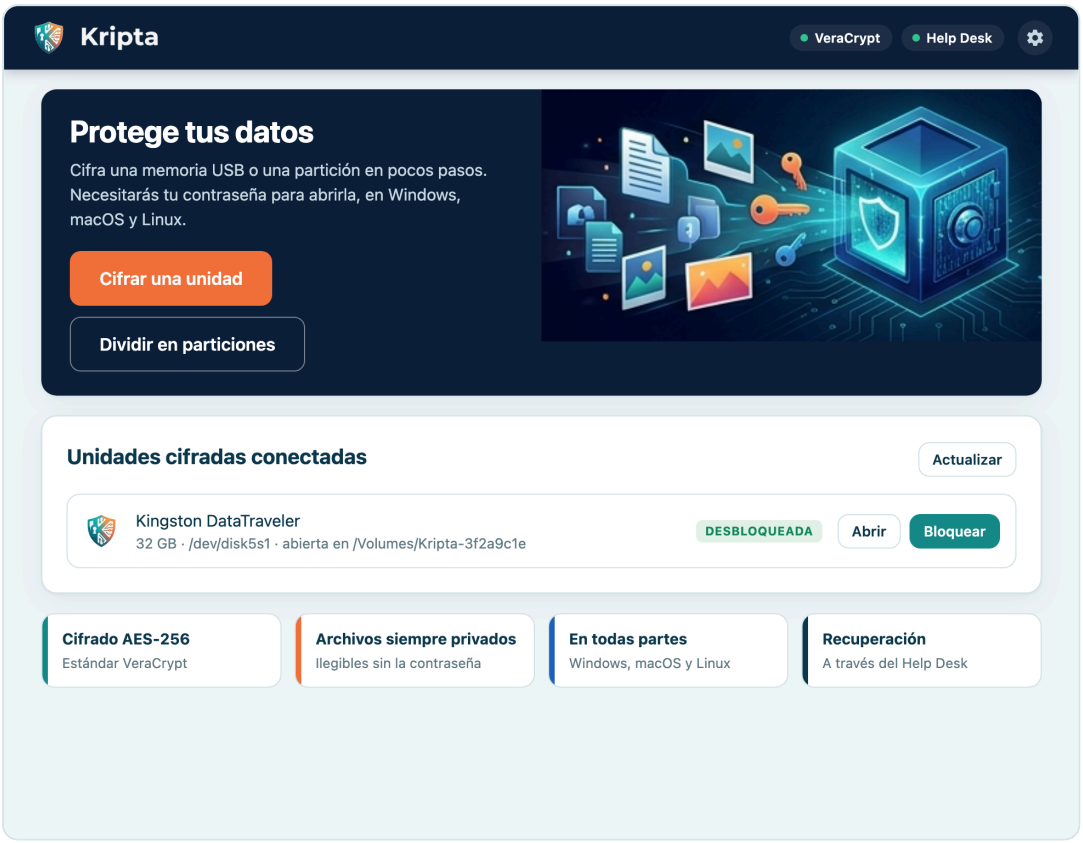


Actualización de VeraCrypt disponible.

> **Antes de actualizar**
>
> Bloquea todas las unidades cifradas abiertas: Kripta no actualiza VeraCrypt mientras haya una unidad desbloqueada. Puedes desactivar la comprobación automática en Ajustes (capítulo 9).

3 La ventana principal

Al abrirse, Kripta muestra la pantalla de inicio. Desde aquí puedes cifrar una unidad nueva y gestionar las unidades cifradas conectadas al ordenador.

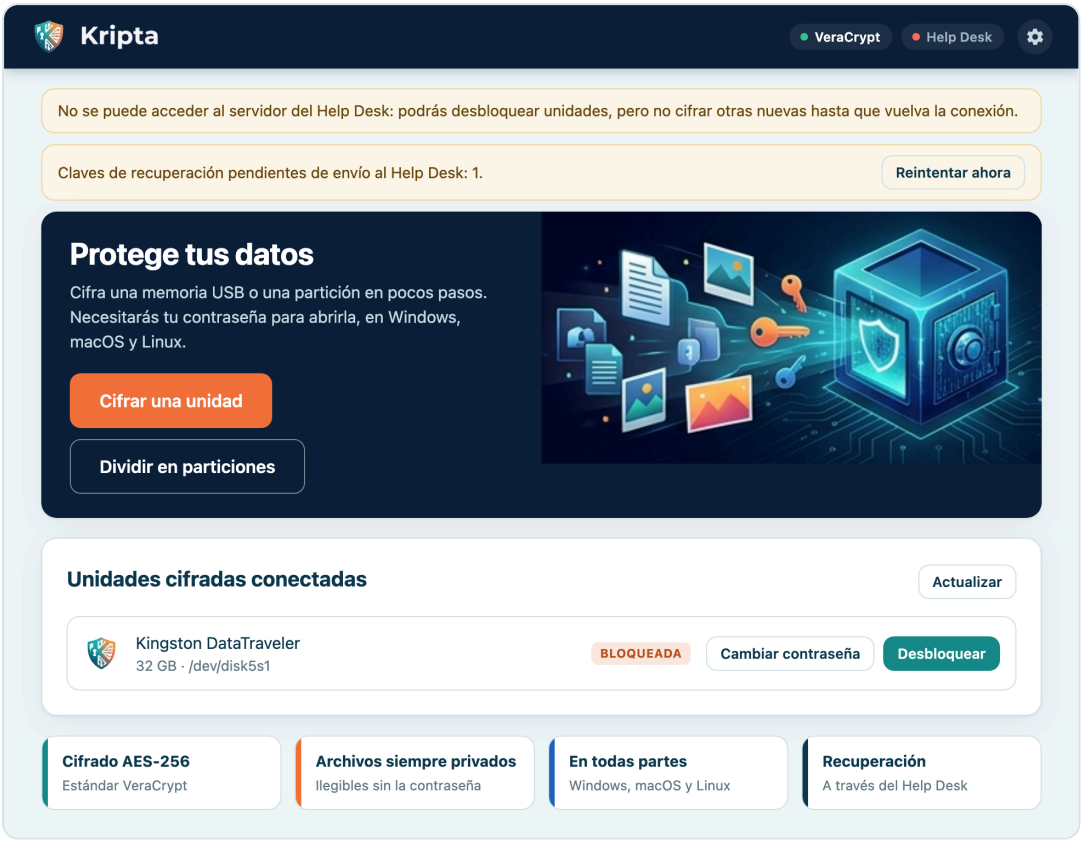


Pantalla de inicio con una unidad cifrada conectada y desbloqueada.

Elemento	Para qué sirve
VeraCrypt	Punto **verde**: el motor de cifrado está instalado. **Rojo**: no lo está (capítulo 2). Al pasar el ratón ves la versión.
Help Desk	Verde: el archivo de claves está accesible. Rojo: no lo está (sin red, VPN apagada, falta la configuración).
Engranaje	Abre **Ajustes**: idioma, configuración de la empresa, componentes (capítulo 9).
Cifrar una unidad	Inicia el asistente (capítulo 4). Está desactivado si Kripta no está configurado o falta VeraCrypt.
Dividir en particiones	Divide una memoria USB o un disco externo en varias particiones (capítulo 5).
Unidades cifradas conectadas	Las unidades Kripta conectadas, con el estado **Bloqueada** o **Desbloqueada** y sus botones.

Avisos

En la parte superior de la ventana pueden aparecer recuadros de color con un botón para resolver el problema:



Servidor del Help Desk inaccesible y una clave de recuperación pendiente de envío.

- **Servidor del Help Desk inaccesible:** puedes seguir desbloqueando unidades, pero no cifrar otras nuevas.
- **Claves de recuperación pendientes de envío:** Kripta reintenta solo; pulsa **Reintentar ahora** cuando vuelvas a estar conectado. **Mantén Kripta abierto hasta que desaparezca el aviso.**
- **Kripta aún no está conectado con el Help Desk / VeraCrypt no está instalado / VeraCrypt … está disponible:** ver capítulo 2.

El icono de Kripta: barra de menús y área de notificación

Kripta trabaja en segundo plano para detectar cuándo conectas una unidad cifrada, y se controla desde un icono con el emblema:

Sistema	Dónde está el icono	Conviene saber
macOS	En la **barra de menús** arriba a la derecha. Kripta **no aparece en el Dock**.	En los MacBook con muesca, si la barra está llena los iconos sobrantes quedan ocultos: quita los que no uses o arrástralos manteniendo pulsado ⌘.
Windows	En el **área de notificación** abajo a la derecha, junto al reloj.	Si está entre los iconos ocultos, haz clic en la flecha ^ y arrastra el emblema a la barra.

Sistema	Dónde está el icono	Conviene saber
Linux	En el **área de notificación** del panel.	En GNOME «puro» (Fedora, Debian) se necesita la extensión **AppIndicator and KStatusNotifierItem Support**.

El menú del icono contiene **Abrir Kripta**, **Cifrar una unidad…**, **Dividir en particiones…**, **Bloquear todas las unidades**, **Ajustes…** y **Salir de Kripta**. Las opciones siguen el idioma elegido.

> **Cerrar la ventana no cierra Kripta**
> Kripta sigue activo en la barra de menús o el área de notificación. Para volver a abrir la ventana usa **Abrir Kripta**, o inicia Kripta de nuevo: se mostrará la ventana ya activa.

Inicio automático

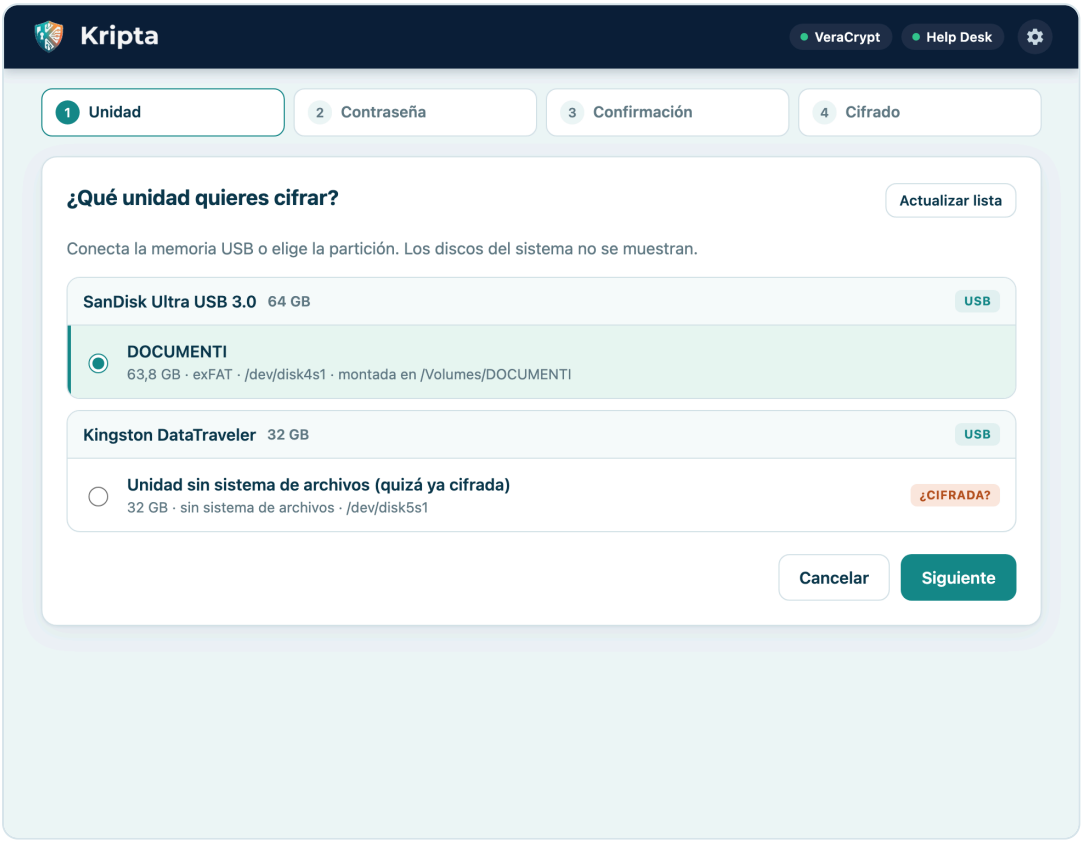
Tras la instalación, Kripta **se inicia solo cada vez que inicias sesión**, sin abrir la ventana, y permanece siempre a la escucha: en cuanto conectas una unidad cifrada te pide la contraseña. Puedes desactivarlo en **Configuración › Inicio automático** (capítulo 9). **Salir de Kripta** lo cierra hasta el próximo inicio de sesión.

4 Cifrar una unidad

> **El cifrado borra todo el contenido de la unidad.**
> Antes de empezar, copia en otro lugar los archivos que quieras conservar. Tras el cifrado podrás volver a copiarlos en la unidad protegida.

Conecta la memoria, comprueba que el indicador **Help Desk** está en verde y pulsa **Cifrar una unidad**.

Paso 1 — Unidad

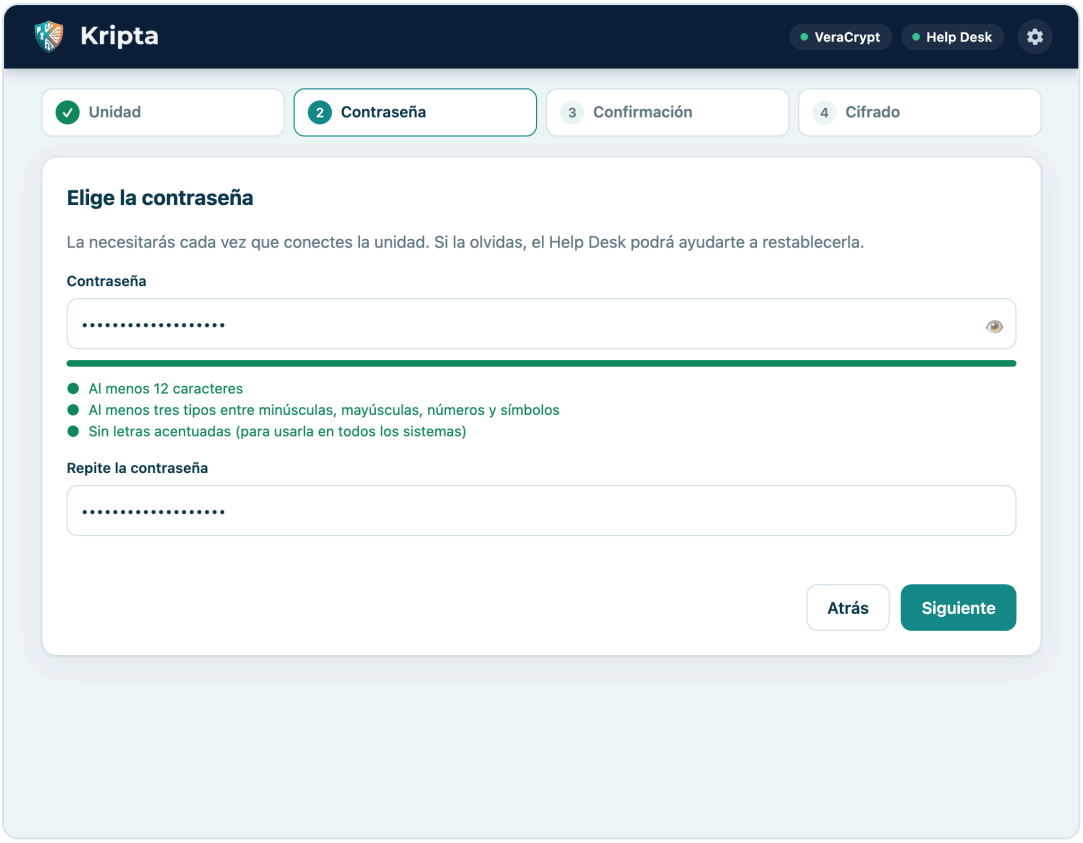


Elección de la unidad que se va a cifrar.

1. Kripta muestra los dispositivos conectados, primero los extraíbles. Los **discos del sistema nunca se muestran**.
2. Comprueba bien la **capacidad y el nombre** para asegurarte de elegir la unidad correcta.
3. Si la memoria no aparece, vuelve a conectarla y pulsa **Actualizar lista**.
4. Selecciona la unidad y pulsa **Siguiente**.

> **Etiqueta «¿Cifrada?»**
> Indica una unidad sin sistema de archivos reconocible: probablemente ya está cifrada. Si la cifras de nuevo, perderás su contenido actual.

Paso 2 — Contraseña

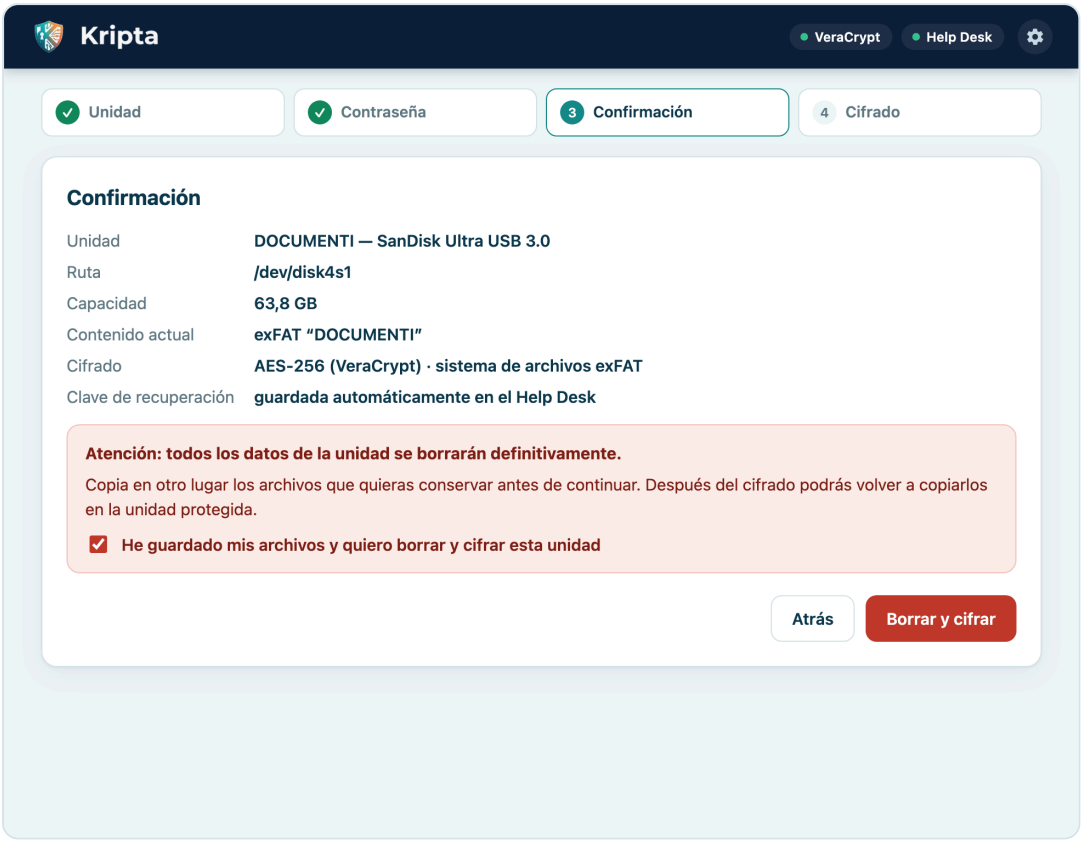


Las reglas se ponen en verde a medida que se cumplen.

La contraseña debe tener **al menos 12 caracteres**, **al menos tres tipos** entre minúsculas, mayúsculas, números y símbolos, y **ninguna letra acentuada** (á, ñ, ü…), que otros sistemas podrían teclear de forma distinta. La barra de color indica la robustez; el botón 👁 muestra la contraseña. Repítela en el segundo campo y pulsa **Siguiente**.

> **Consejo**
> Una frase de varias palabras unidas por símbolos y números (por ejemplo `Tren-Lago-Verde-47`) es segura y fácil de recordar. No uses la contraseña de tu cuenta de la empresa.

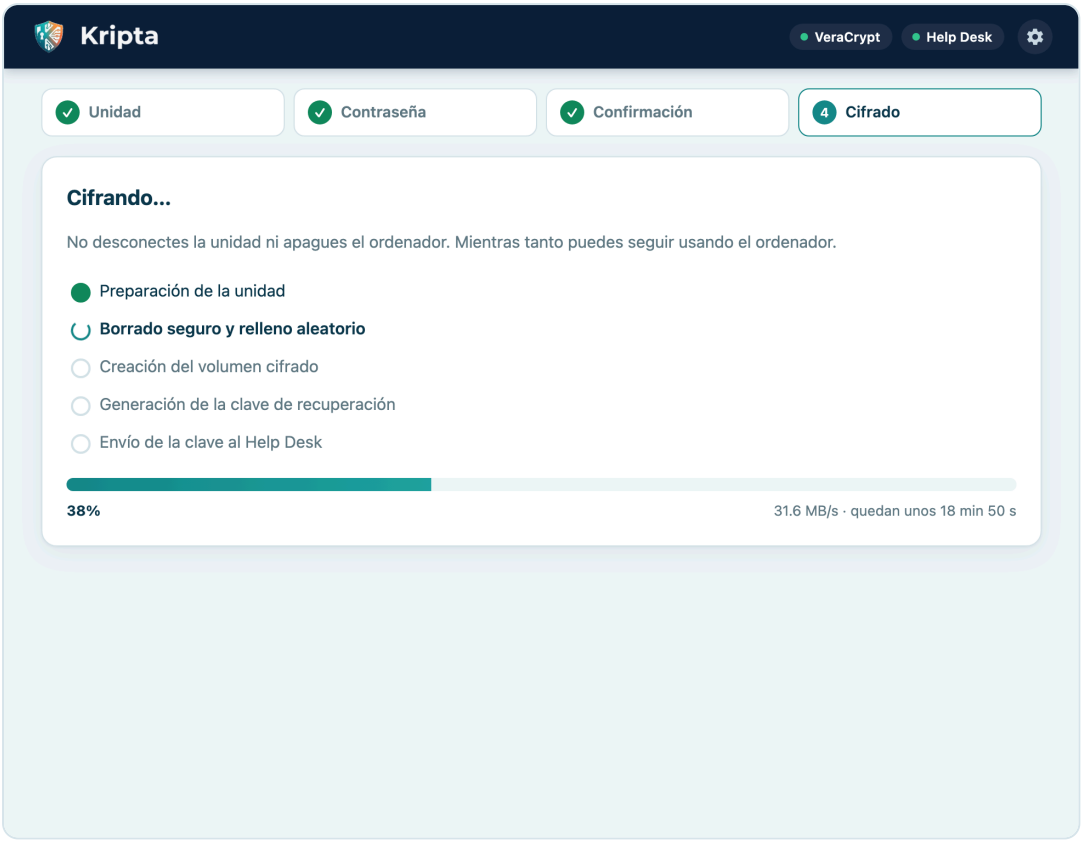
Paso 3 — Confirmación



Resumen y confirmación del borrado.

Revisa el resumen, marca **He guardado mis archivos y quiero borrar y cifrar esta unidad** y pulsa **Borrar y cifrar**. El sistema puede pedirte autorización de administrador.

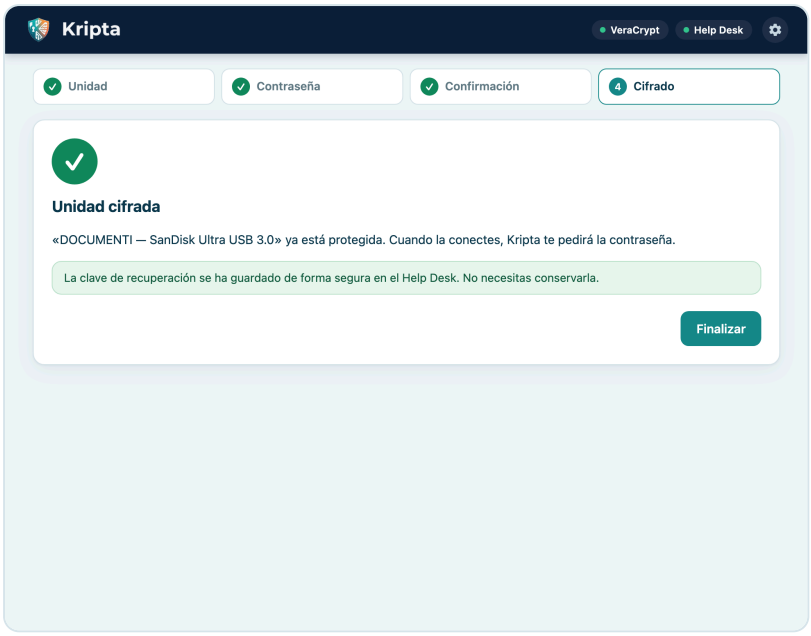
Paso 4 — Cifrado



Progreso con velocidad y tiempo restante.

Kripta prepara la unidad, la sobrescribe por completo con datos aleatorios (la fase más larga), crea el volumen cifrado exFAT, genera la clave de recuperación y la envía al Help Desk.

> **Durante el cifrado**
> No desconectes la unidad ni apagues o suspendas el ordenador. Una memoria de 64 GB tarda aproximadamente entre 15 minutos y una hora.



Cifrado completado.

Si aparece **la clave de recuperación aún no se ha enviado**, la unidad está cifrada y se puede usar igualmente: mantén Kripta abierto y conectado, enviará la clave lo antes posible. Si el cifrado falla, el mensaje explica el motivo (capítulo 11).

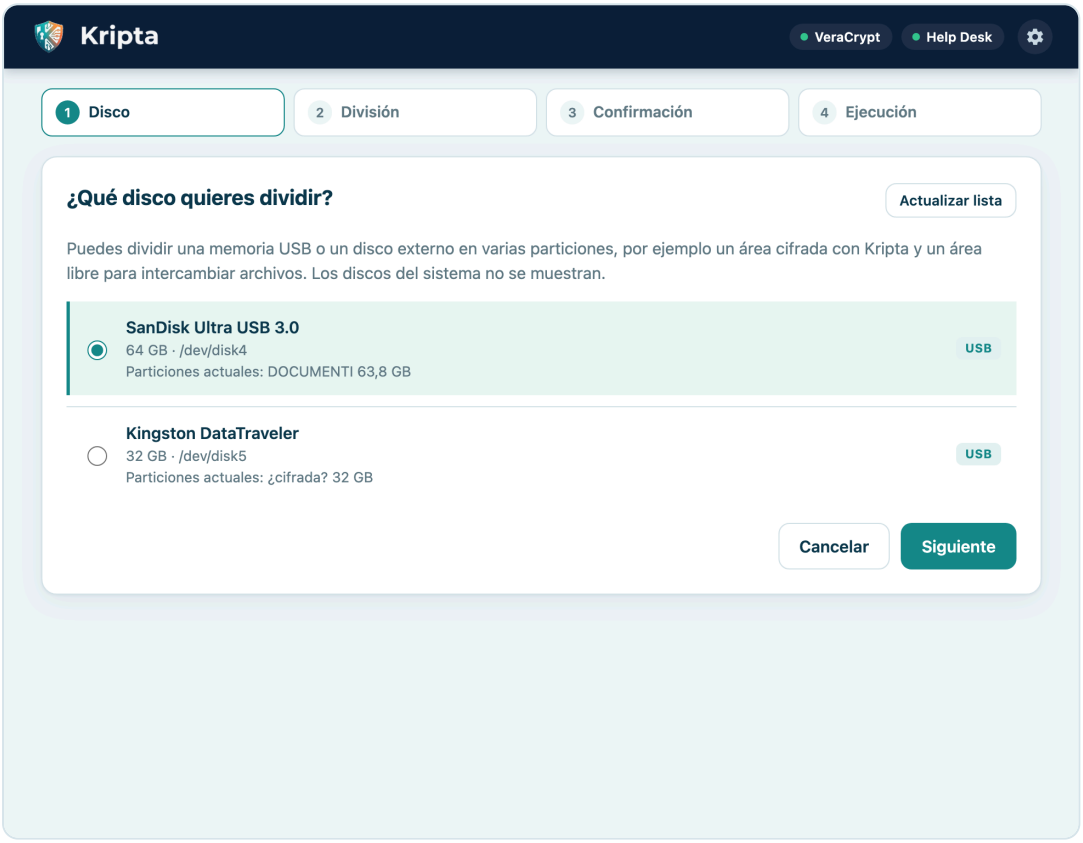
5 Dividir un disco en particiones

Con **Dividir en particiones** divides una memoria USB o un disco externo en varias partes independientes, cada una con su nombre y su sistema de archivos. El uso típico es un **área cifrada** para los datos confidenciales y un **área libre** para intercambiar archivos con ordenadores sin Kripta.

La división borra todo el disco

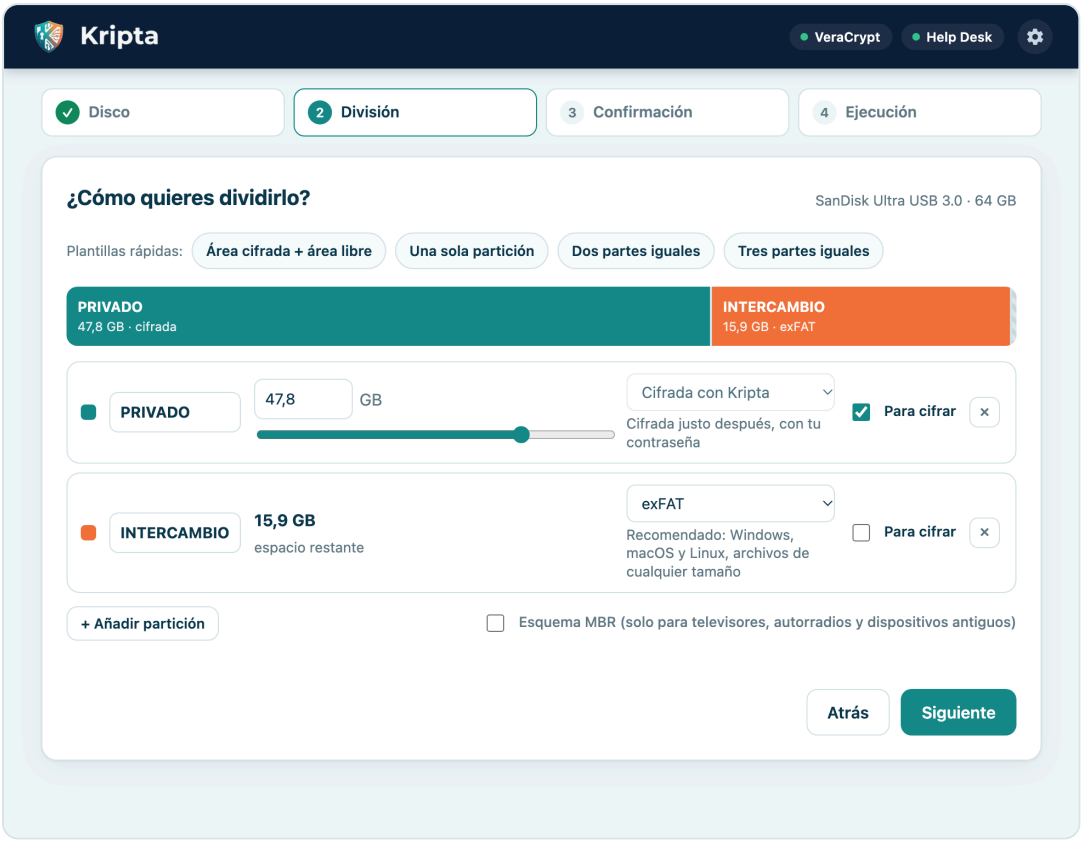
, incluidas las particiones existentes y las unidades ya cifradas. Guarda en otro lugar los archivos que quieras conservar.

Paso 1 — Disco



Elección del disco, con sus particiones actuales.

Paso 2 — División



La barra de color muestra la división en proporción.

Plantilla	Resultado
Área cifrada + área libre	Tres cuartos del disco para cifrar y el resto libre en exFAT. Es la plantilla propuesta al principio.
Una sola partición	Todo el disco en una única partición.
Dos / Tres partes iguales	El disco dividido en partes del mismo tamaño.

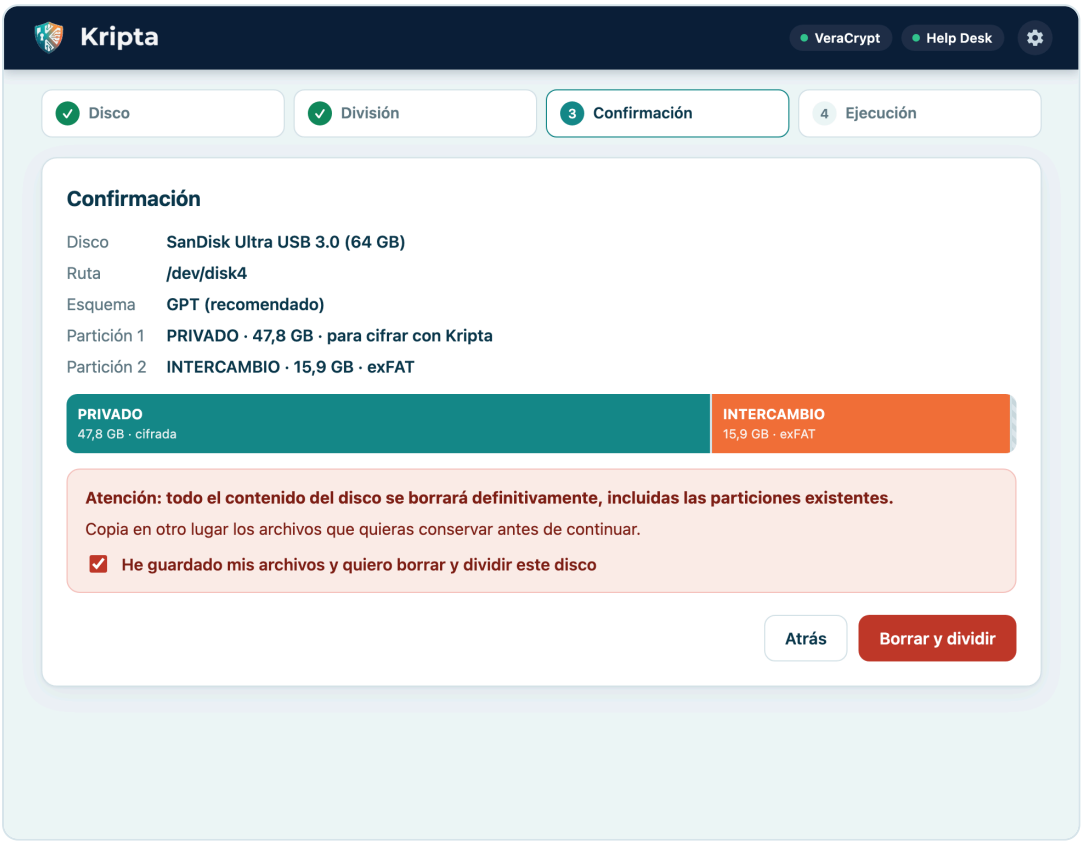
Para cada partición defines el **nombre** (hasta 11 caracteres: letras, números, `_` y `-`), el **tamaño** (la última ocupa el espacio restante), el **sistema de archivos** y **Para cifrar**. **+ Añadir partición** añade otra (hasta 8).

Sistema de archivos	Se abre en	Notas
exFAT (recomendado)	Windows, macOS, Linux	Sin límite práctico en el tamaño de los archivos.
FAT32	Casi cualquier dispositivo	Archivos de hasta 4 GB; en Windows, particiones de hasta 32 GB.
NTFS	Windows; macOS solo lectura	En Linux requiere `ntfs-3g`.
APFS, **Mac OS Plus**	Solo Mac	Disponibles solo desde un Mac.

Sistema de archivos	Se abre en	Notas
ext4	Solo Linux	Disponible solo desde Linux.

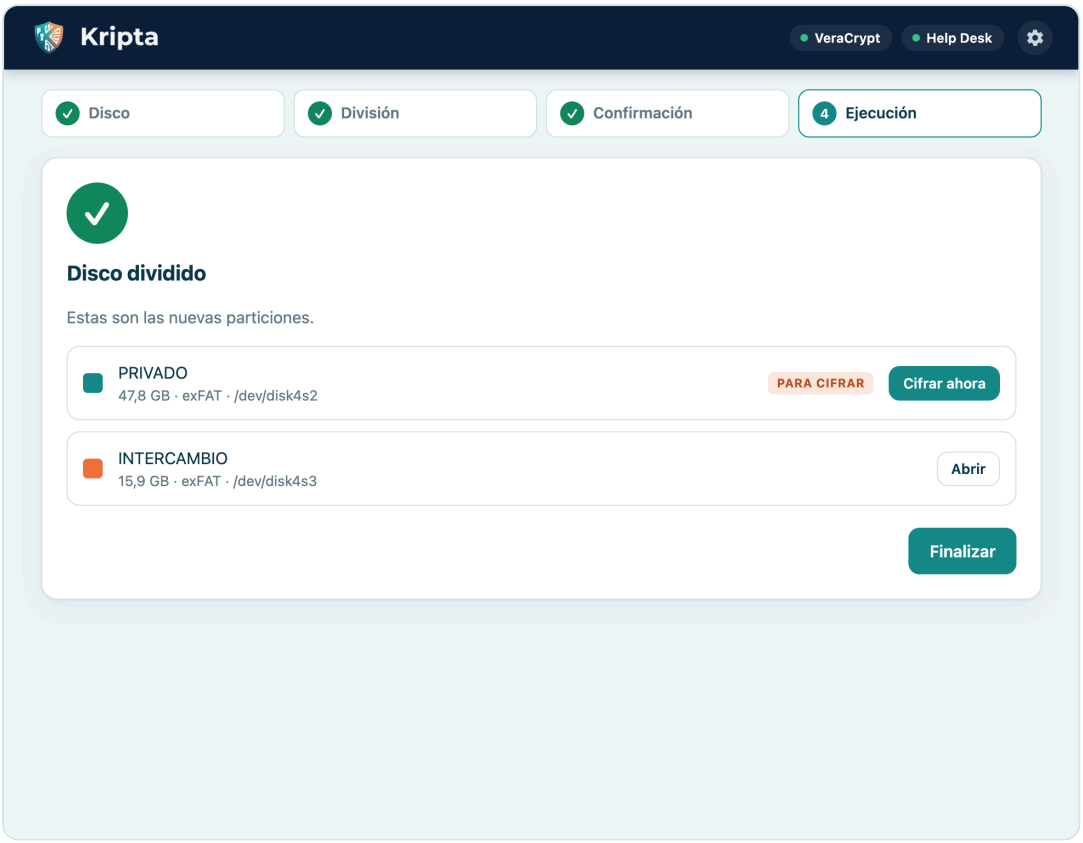
> **Esquema MBR**
> Actívalo solo si la memoria debe funcionar con televisores, autorradios u ordenadores muy antiguos: como máximo 4 particiones y 2 TB.

Paso 3 — Confirmación y paso 4 — Ejecución



Resumen antes del borrado.

Marca la casilla de confirmación y pulsa **Borrar y dividir**. Normalmente basta menos de un minuto.



Particiones creadas: el área para cifrar tiene el botón «Cifrar ahora».

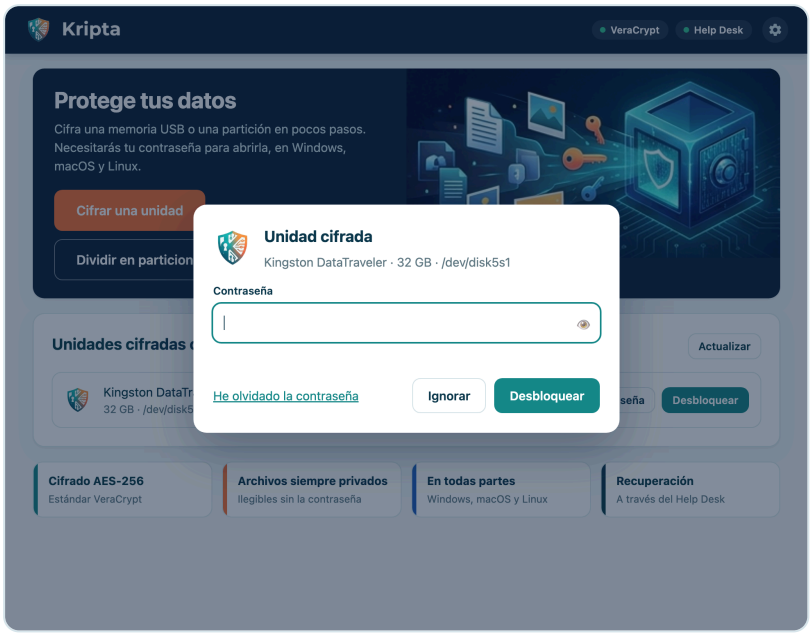
Junto a las particiones para cifrar pulsa **Cifrar ahora**: el cifrado (capítulo 4) comienza con la partición ya seleccionada.

> **Hasta que la cifres, el área «para cifrar» no está protegida**
> No copies en ella archivos confidenciales antes de terminar el cifrado.

6 Usar una unidad cifrada

Desbloquear

Cuando conectas una unidad cifrada con Kripta en ejecución, aparece automáticamente la solicitud de la contraseña.



Solicitud de la contraseña al conectar la unidad.

1. Escribe la contraseña y pulsa **Desbloquear** (o Intro).
2. La unidad se abre como un disco normal en el Explorador de archivos, el Finder o el gestor de archivos de Linux.
3. Con **Ignorar** la desbloqueas más tarde desde la ventana principal.

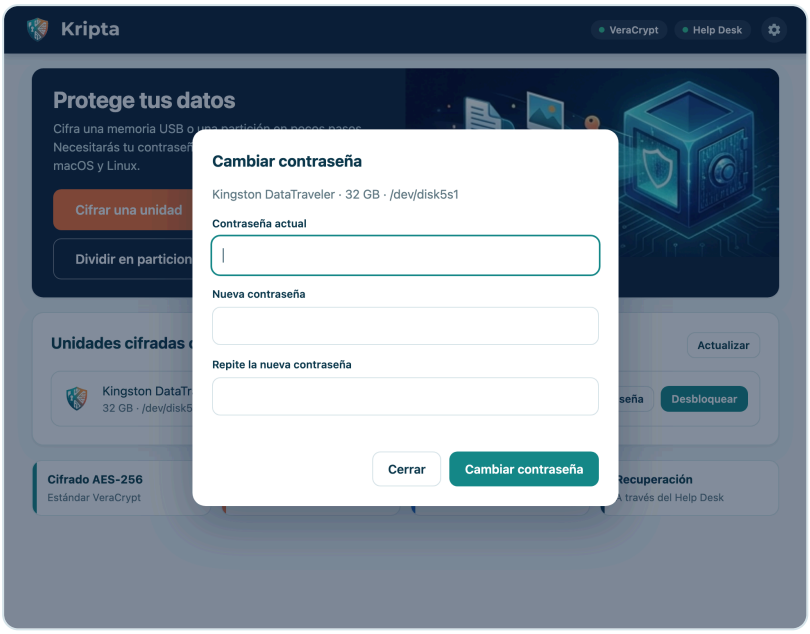
Trabajar con los archivos y bloquear

Con la unidad desbloqueada usas los archivos con normalidad: todo lo que escribes se cifra de forma transparente. Cuando termines, cierra los archivos abiertos, pulsa **Bloquear** y desconecta la unidad.

> **No desconectes una unidad desbloqueada sin bloquearla**
> Podrías perder los archivos que estabas copiando.

7 Cambiar la contraseña

Puedes cambiar la contraseña cuando quieras, si conoces la actual. Los datos de la unidad no se tocan.



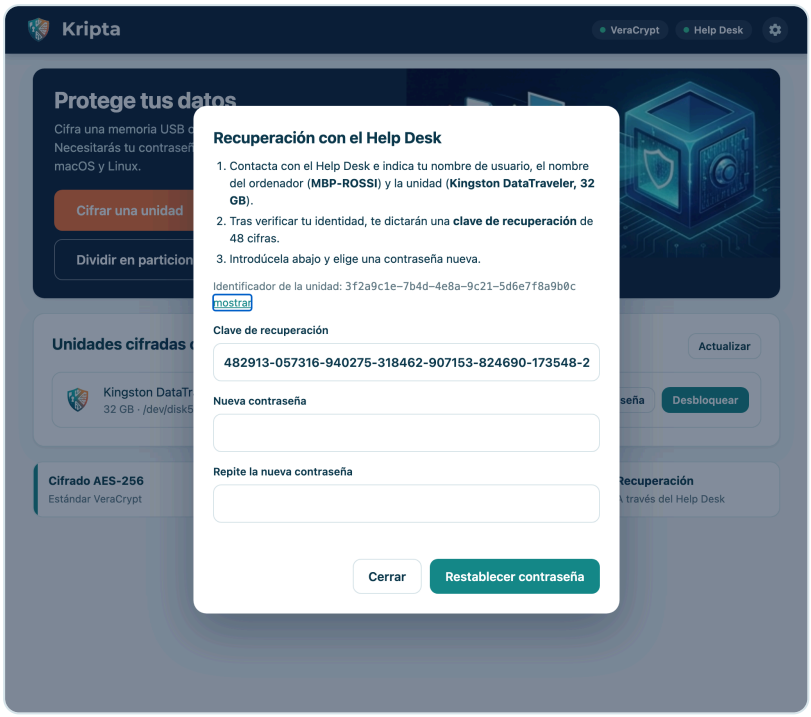
Ventana Cambiar contraseña.

1. Si la unidad está desbloqueada, pulsa antes **Bloquear**.
2. Pulsa **Cambiar contraseña** junto a la unidad.
3. Introduce la contraseña actual y dos veces la nueva (mismas reglas que en el capítulo 4), y confirma.

> **¿Y la clave de recuperación?**
> Sigue siendo válida: el Help Desk podrá ayudarte también tras un cambio de contraseña.

8 He olvidado la contraseña

El Help Desk puede darte la clave de recuperación de la unidad: con ella defines una contraseña nueva y recuperas todos tus archivos.



Recuperación con el Help Desk.

1. En la solicitud de contraseña elige **He olvidado la contraseña**.
2. La ventana muestra el nombre del ordenador y de la unidad; con **mostrar** aparece también el identificador de la unidad.
3. **Contacta con el Help Desk** y comunica estos datos. Tras verificar tu identidad, te dictarán la **clave de 48 cifras**.
4. Escríbela en el campo **Clave de recuperación**, elige una contraseña nueva y pulsa **Restablecer contraseña**.

Una clave, un solo uso

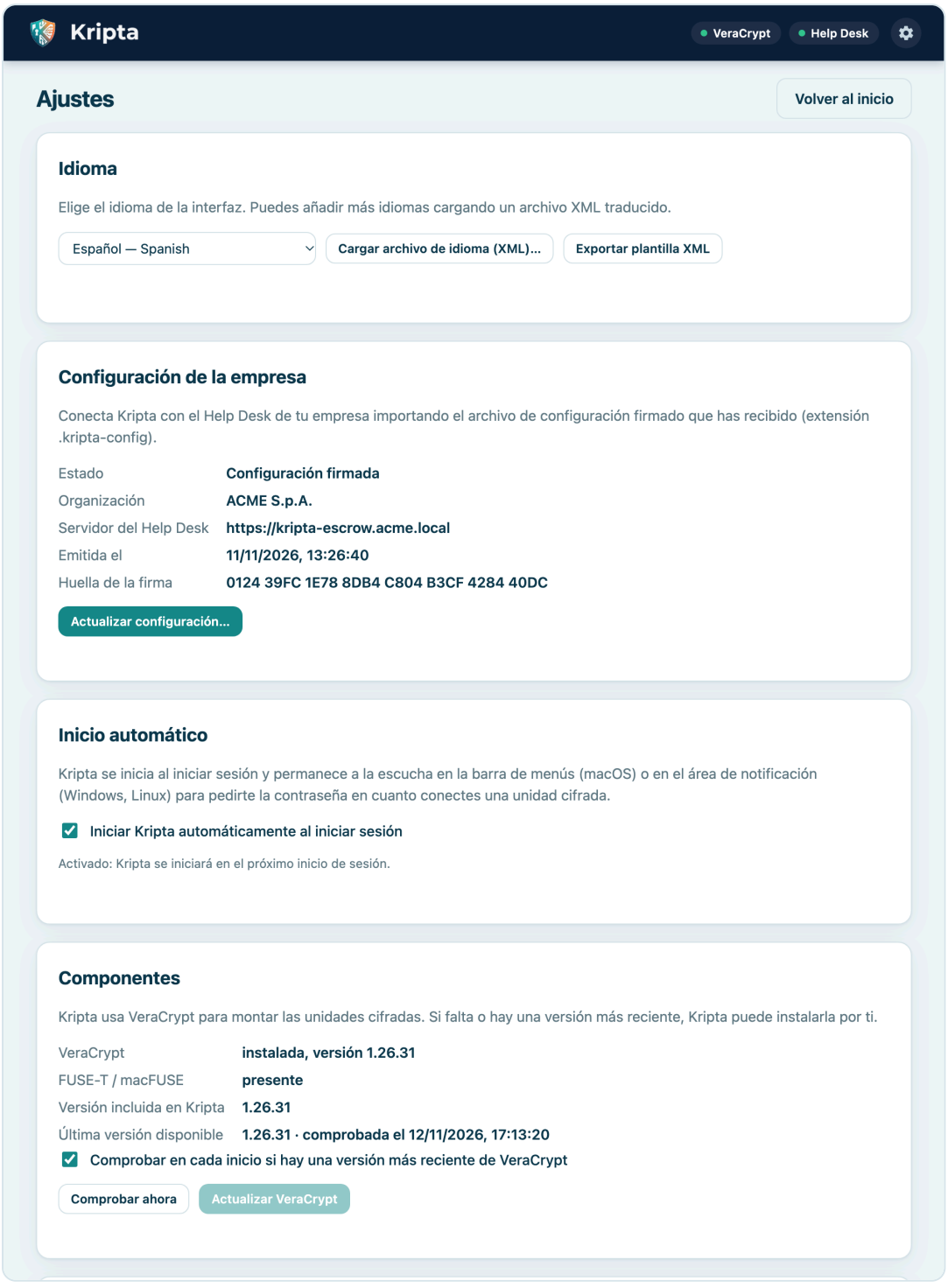
Tras cada recuperación Kripta genera una clave nueva y la envía al Help Desk.

Cuidado con las estafas

El Help Desk nunca te pedirá tu contraseña. Eres tú quien contacta con el Help Desk, no al revés.

9 Ajustes

Se abren con el engranaje arriba a la derecha o con **Ajustes…** en el menú del icono.



Ajustes: idioma, configuración de la empresa, componentes, información.

Idioma

Elige el idioma en la lista: la interfaz, el menú del icono y las solicitudes de autorización cambian al instante. Con **Automático** Kripta usa el idioma del sistema. Idiomas incluidos:

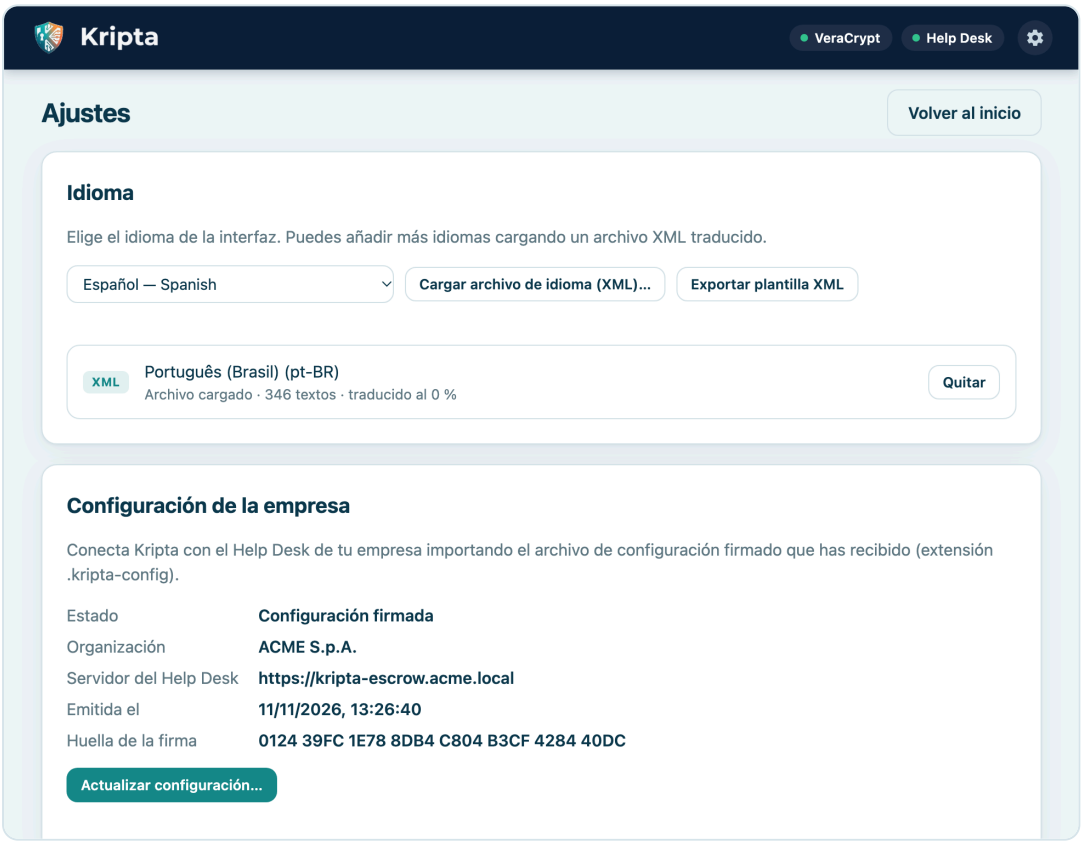
Italiano English Français Español Deutsch Русский العربية 中文 日本語

Añadir un idioma

Las traducciones son simples archivos **XML**, uno por idioma. Para añadir uno:

1. Pulsa **Exportar plantilla XML**: el archivo del idioma actual se guarda en la carpeta Descargas.
2. Traduce el texto de cada elemento `<string>` sin cambiar los atributos `id` ni los marcadores `{1}`, `{2}`.
3. Al principio del archivo define `code` (por ejemplo `pt` o `pt-BR`), `name`, `english-name` y `dir` (`rtl` para los idiomas que se escriben de derecha a izquierda).
4. Pulsa **Cargar archivo de idioma (XML)…** y elige el archivo: el idioma aparece en la lista con el porcentaje de textos traducidos. Los textos que faltan se muestran en inglés.

```
<kripta-language format="1" code="pt" name="Português" english-name="Portuguese" dir="ltr">
  <string id="home.title">Proteja os seus dados</string>
  …
</kripta-language>
```



Un idioma cargado desde un archivo XML, con el botón Quitar.

Cargar un archivo con el mismo código que un idioma incluido lo sustituye (útil para corregir un término); **Quitar** restablece el original. Los archivos de los nueve idiomas incluidos están junto a este manual, en la carpeta `lang`.

Configuración de la empresa

Muestra organización, servidor del Help Desk, fecha y huella de la configuración instalada. **Actualizar configuración…** importa un archivo nuevo recibido del Help Desk (capítulo 2).

Componentes

Muestra la versión de VeraCrypt instalada, la incluida en Kripta y la última disponible. **Comprobar ahora** comprueba al momento, **Instalar** / **Actualizar VeraCrypt** inicia la instalación. La casilla **Comprobar en cada inicio…** activa o desactiva la comprobación automática.

Inicio automático

La casilla **Iniciar Kripta automáticamente al iniciar sesión** está activada de forma predeterminada. Debajo se indica si el inicio automático está registrado en el sistema. Si la desactivas, Kripta no detecta las unidades cifradas hasta que lo abras.

10 Usar la unidad en otros ordenadores

Las unidades cifradas por Kripta usan el formato estándar de **VeraCrypt** con el sistema de archivos **exFAT**: se abren en Windows, macOS y Linux.

Ordenador	Qué ocurre al conectar la unidad
Con Kripta configurado	Aparece la solicitud de la contraseña: todo es automático.
Con Kripta instalado pero **sin configuración de la empresa** (por ejemplo en casa)	La solicitud de la contraseña aparece igualmente y la unidad se desbloquea. Si falta VeraCrypt, Kripta ofrece **Instalar ahora**. Sin configuración no puedes cifrar unidades nuevas ni recuperar contraseñas.
Solo con VeraCrypt	Abre VeraCrypt, elige una ranura libre, **Seleccionar dispositivo**, elige la partición de la memoria, luego **Montar** e introduce la contraseña.
Sin Kripta ni VeraCrypt	No aparece ninguna solicitud: los sistemas operativos no inician programas desde las memorias USB. El sistema podría proponerte **formatear** la unidad: **recházalo siempre**. Instala Kripta (desde el sitio de la empresa) y vuelve a conectar la unidad.

Permisos de administrador

Para abrir una unidad cifrada en cualquier ordenador se necesitan permisos de administrador, porque VeraCrypt usa un controlador del sistema. En un ordenador del que no tengas las credenciales, la unidad no se puede abrir.

Área libre para intercambio

Si usas a menudo ordenadores sin Kripta, divide la memoria con la plantilla **Área cifrada + área libre** (capítulo 5): en el área libre puedes copiar también el instalador de Kripta.

11 Mensajes y solución de problemas

Mensaje o situación	Qué hacer
Kripta aún no está conectado con el Help Desk de tu empresa	Importa el archivo `.kripta-config` recibido del Help Desk (capítulo 2).
La firma del paquete no es válida	El archivo se ha modificado o está dañado: pídelo de nuevo al Help Desk.
El paquete está firmado con una clave distinta / no aprobada	El archivo no procede de tu empresa. No lo uses y contacta con el Help Desk.
La configuración la gestiona TI y no puede sustituirse	El ordenador está configurado de forma centralizada: no hay que importar nada.
El motor de cifrado VeraCrypt no está instalado	Pulsa **Instalar ahora**. Si no hay botón, contacta con el Help Desk.
La firma oficial de VeraCrypt no es válida / el archivo no coincide con la versión firmada	La descarga se ha alterado o está incompleta: la instalación se ha cancelado. Inténtalo más tarde.
Bloquea todas las unidades cifradas antes de actualizar VeraCrypt	Pulsa **Bloquear** en las unidades abiertas y repite la actualización.
Reinicia el ordenador para completar la actualización (Windows)	Guarda tu trabajo y reinicia.
No se puede acceder al servidor del Help Desk. El cifrado no se ha iniciado.	Conéctate a la red de la empresa o a la VPN y vuelve a intentarlo. Los datos de la unidad no se han tocado.
Claves de recuperación pendientes de envío	Conéctate a la red y pulsa **Reintentar ahora**. Mantén Kripta abierto hasta que desaparezca el aviso.
No hay ninguna unidad disponible	Vuelve a conectar la memoria (prueba otro puerto USB) y pulsa **Actualizar lista**.
Autorización de administrador cancelada / Tiempo agotado	Repite la operación y confirma la solicitud del sistema.
No se puede desmontar / bloquear el volumen	Cierra los documentos y ventanas abiertos desde la unidad y vuelve a intentarlo.
Contraseña incorrecta	Comprueba Bloq Mayús y la distribución del teclado. Si no la recuerdas, consulta el capítulo 8.
Clave de recuperación incorrecta	Vuelve a comprobar las cifras con el operador: se necesita la clave **más reciente**.
El disco contiene una unidad Kripta desbloqueada	Bloquéala en la pantalla de inicio y repite la división.

Mensaje o situación	Qué hacer
El sistema no ha detectado las nuevas particiones	Desconecta y vuelve a conectar la unidad.
El archivo de idioma no es un XML válido / elemento no permitido	Corrige el archivo indicado en el mensaje: solo se admiten elementos `<string>` con texto sin formato.
La ventana de desbloqueo no aparece al conectar la unidad	Comprueba que Kripta esté en ejecución (icono en la barra) y usa **Desbloquear** desde la ventana principal.

12 Preguntas frecuentes

¿Puedo cifrar una memoria que ya contiene archivos sin perderlos?

No. El cifrado borra la unidad. Copia los archivos en otro lugar, cifra la unidad y luego vuelve a copiarlos.

¿Puedo cifrar el disco interno de mi ordenador?

No. Kripta está pensado para memorias y discos externos; los discos del sistema no se muestran.

¿Puede el Help Desk leer mis archivos?

El Help Desk solo guarda la clave de recuperación y solo puede consultarla a petición tuya, con registro de cada acceso.

¿Tengo que anotar la clave de recuperación?

No. Nunca la ves y no tienes que guardarla: está archivada en el Help Desk.

¿Kripta instala programas en mi ordenador?

Solo VeraCrypt (y FUSE-T en macOS), tras tu confirmación y solo si la firma oficial de los desarrolladores es válida.

¿Puedo usar la memoria en el ordenador de casa?

Sí, instalando Kripta o VeraCrypt (capítulo 10). Respeta siempre las normas de la empresa sobre el uso de los datos fuera de la oficina.

No está el idioma que necesito. ¿Qué puedo hacer?

Puedes traducir la plantilla XML y cargarla desde Ajustes (capítulo 9), o pedir a TI que distribuya una.

¿Por qué no puedo usar letras acentuadas en la contraseña?

Windows, macOS y Linux pueden codificarlas de forma distinta: la misma contraseña tecleada en otro sistema podría no reconocerse.

¿Cuánto espacio ocupa el cifrado?

Muy poco: unos cientos de kilobytes para las cabeceras del volumen.

A Apéndice para TI

Paquetes

Sistema	Paquete	Notas
Windows 10/11 (x64)	`Kripta_1.2.0_x64-setup.exe`	Contiene los MSI oficiales de VeraCrypt (x64 y ARM64). La aplicación se inicia con permisos de administrador.
macOS 11+	`Kripta_1.2.0_universal.dmg`	Contiene VeraCrypt (versiones FUSE-T y macFUSE) y FUSE-T, que no requiere extensiones del kernel.
Debian / Ubuntu	`Kripta_1.2.0_amd64.deb`	Contiene VeraCrypt para Ubuntu 22.04/24.04 y Debian 12/13; para otras versiones Kripta descarga el paquete verificado.
Fedora / RHEL	`Kripta-1.2.0-1.x86_64.rpm`	Contiene VeraCrypt para Fedora 44; instalar también `exfatprogs`.
Otras distribuciones	`Kripta_1.2.0_amd64.AppImage`	Ejecutable portátil.

Configuración firmada

En el servidor escrow, una sola vez, generar la clave de firma; después firmar la configuración del cliente (plantilla en `deploy/client/kripta.toml.example`):

```
kripta-escrow keygen-sign            # clave privada (guardar sin conexión) + pública + huella
kripta-escrow sign-config client.toml firma.key "ACME S.A." acme.kripta-config
```

Distribuir `acme.kripta-config` a los usuarios y publicar la **huella** en un canal fiable (intranet, teléfono del Help Desk). Kripta guarda la configuración en la ubicación del sistema (`%ProgramData%\Kripta`, `/Library/Application Support/Kripta`, `/etc/kripta`) mediante el proceso con privilegios, junto con la clave del firmante: las actualizaciones posteriores deben llevar la misma firma. Para no depender de que el usuario compruebe la huella, compilar Kripta con `KRIPTA_PROVISIONING_KEYS=<clave pública>`: solo se aceptarán esas claves. Una configuración copiada a mano por TI (sin firma) no puede sustituirse con un paquete.

Instalación y actualización de VeraCrypt

- Los instaladores incluidos se preparan con `scripts/fetch-veracrypt.py` al compilar.
- Antes de instalar, el proceso con privilegios verifica la firma OpenPGP de la lista SHA-256 oficial con la clave IDRIX integrada (huella `5069 A233 D55A 0EEB 174A 5FC3 821A CD02 680D 16DE`) y el hash del archivo.
- Opciones en `kripta.toml`: `veracrypt_update_check = false` desactiva la comprobación de actualizaciones; `veracrypt_release_api = "https://espejo.interno/…"` usa un espejo interno con

el mismo formato que la API de GitHub.

Idiomas

Los archivos XML de los idiomas están en `app/ui/lang/` (incluidos en la aplicación) y en `docs/manuale/lang/`. Los idiomas cargados por los usuarios se guardan en la carpeta de datos del usuario (`languages/`). Para distribuir un idioma nuevo a todos, añadir el archivo en `app/ui/lang/` y su código en la lista de `app/ui/i18n.js`.

Componentes opcionales

- **Inicio al iniciar sesión** en la barra de menús / área de notificación (`kripta --background`): **automático**. Kripta lo registra en cada inicio (macOS: `~/Library/LaunchAgents/com.kripta.agent.plist`, reiniciado si termina de forma anómala; Windows: tarea programada «Kripta» al iniciar sesión con privilegios máximos, creada también por el instalador y eliminada al desinstalar; Linux: `/etc/xdg/autostart/kripta.desktop` de los paquetes .deb/.rpm, `~/.config/autostart/kripta.desktop` para AppImage). Se desactiva en la Configuración.
- **Asistente con privilegios** como servicio (sin solicitudes de contraseña): `deploy/macos/com.kripta.helper.plist`, `deploy/linux/kripta-helper.service`.