

OBSKURA

SEGURIDAD INVISIBLE PARA TUS DATOS

MANUAL DE INSTRUCCIONES

VERSIÓN 0.3.0

MACOS · WINDOWS · LINUX

OCTUBRE DE 2026

MANUAL DE INSTRUCCIONES

ÍNDICE

01	Bienvenido a Obskura	Qué hace, bases de datos y cajas fuertes	03
02	Instalación y primer inicio	macOS, Windows, Linux · la clave de acceso · la interfaz	04
03	Contraseñas y archivos de clave	Credenciales, Argon2id, elección del cifrado	05
04	Bases de datos de contraseñas	Crear, desbloquear, organizar las entradas	07
05	Gestionar las entradas	Generador, campos, adjuntos, historial	08
06	Herramientas de la base de datos	Búsqueda, copia segura, menú de la base de datos	09
07	Cajas fuertes de archivos	Crear una caja fuerte y cifrar archivos	10
08	Trabajar con los archivos	Abrir, modificar, exportar	11
09	Servidores remotos	SFTP, WebDAV, SMB, FTP/FTPS	12
10	Varios dispositivos en tiempo real	Sincronización en tiempo real, notificaciones	14
11	Clave de acceso y dispositivos	Archivos complementarios, ID y rutas de cada dispositivo	15
12	Copia de seguridad automática	Segundo destino, copias fechadas, por dispositivo	17
13	Importar y exportar	Gestores en línea, CSV de KeePass y otros	18
14	Idiomas	Idioma automático, archivos XML, nuevas traducciones	20
15	Bloqueo y ajustes	Bloqueo automático, portapapeles, tema, nombre del dispositivo	23
16	Atajos y criptografía	Atajos de teclado y detalles técnicos	24
17	Buenas prácticas y problemas	Copias de seguridad, preguntas frecuentes	25

CONVENCIONES

Los nombres de botones y menús van en **negrita**. Las combinaciones de teclas se escriben así: `Ctrl/⌘` + `L`, donde `Ctrl` vale para Windows y Linux y `⌘` para macOS. Los nombres de archivo y extensiones van en `letra fija`. Las capturas muestran la interfaz en el idioma de este manual.

INTRODUCCIÓN

01 BIENVENIDO A OBSKURA

Obskura protege contraseñas y archivos con cifrado de nivel militar. Sin cuentas ni servicios de terceros: tus datos se quedan donde tú decidas, en el ordenador o en tu servidor.

Cada base de datos y cada caja fuerte es un archivo o una carpeta normales. Puedes guardarlos en el disco del ordenador, en una memoria USB, en una carpeta sincronizada como Dropbox, OneDrive o iCloud Drive, o directamente en tu propio servidor SFTP, WebDAV, SMB o FTP, y tener tantos como quieras: uno personal, uno de trabajo, uno compartido con la familia. Varios ordenadores pueden usarlos a la vez y ven los cambios de los demás en tiempo real, aunque lleguen a ellos por rutas distintas.

BASE DE DATOS DE CONTRASEÑAS

Un único archivo `.obk`, inspirado en KeePass. Contiene entradas con nombre de usuario, contraseña, dirección, notas, campos personalizados, adjuntos e historial de cambios, organizadas en grupos.

CAJA FUERTE DE ARCHIVOS

Una carpeta, inspirada en Cryptomator. Arrastras dentro documentos, fotos y archivos comprimidos: cada archivo se cifra por separado, incluidos los nombres y la estructura de carpetas.

CÓMO FUNCIONA LA PROTECCIÓN

Al crear una base de datos o una caja fuerte eliges una **contraseña maestra**, un **archivo de clave** o ambos. A partir de estas credenciales Obskura obtiene la clave de cifrado con Argon2id, un algoritmo pensado precisamente para hacer lentísimos los intentos de adivinar la contraseña. Después los datos se cifran con AES-256, el estándar aprobado para la información clasificada **TOP SECRET**.

Las credenciales nunca se guardan en ningún sitio. Sin ellas el contenido es ilegible para cualquiera, desarrolladores incluidos.

IMPORTANTE

No hay ninguna forma de recuperar una contraseña olvidada o un archivo de clave perdido. Elige una contraseña que recuerdes y guarda una copia del archivo de clave en un lugar seguro y separado.

EN RESUMEN

AES-256-GCM · XChaCha20-Poly1305 · Serpent · Twofish · Camellia · Cascadas de cifrados · Argon2id hasta 2 GiB · HKDF-SHA256 · AES-SIV para los nombres de archivo · Memoria borrada al cerrar · Sin cuentas · SFTP · WebDAV · SMB · FTPS · Tiempo real · Copia de seguridad automática · Rutas por dispositivo · 8 idiomas · macOS · Windows · Linux

PRIMEROS PASOS

02 INSTALACIÓN Y PRIMER INICIO

macOS

Abre el archivo `.dmg` y arrastra Obskura a **Aplicaciones**. En el primer inicio, si macOS bloquea la app, ve a **Ajustes del Sistema → Privacidad y seguridad** y elige **Abrir igualmente**.

Windows

Ejecuta el instalador `.exe`, que usa automáticamente el idioma de Windows, o inicia la versión portátil sin instalar nada. Si aparece el aviso de SmartScreen, haz clic en **Más información → Ejecutar de todas formas**.

Linux

Usa el paquete `.deb` (Debian, Ubuntu), `.rpm` (Fedora, openSUSE) o la `.AppImage`, que no necesita instalación: hazla ejecutable y ábrela.

PRIMER INICIO: IDIOMA Y CLAVE DE ACCESO

Obskura se abre en el idioma del sistema (italiano, inglés, alemán, español, ruso, chino, japonés o árabe; para los demás usa el inglés). En el primer inicio te pide crear la **clave de acceso de Obskura** o, si ya usas Obskura en otro ordenador, introducir la que generaste allí. El capítulo 11 explica para qué sirve.

LA PANTALLA INICIAL

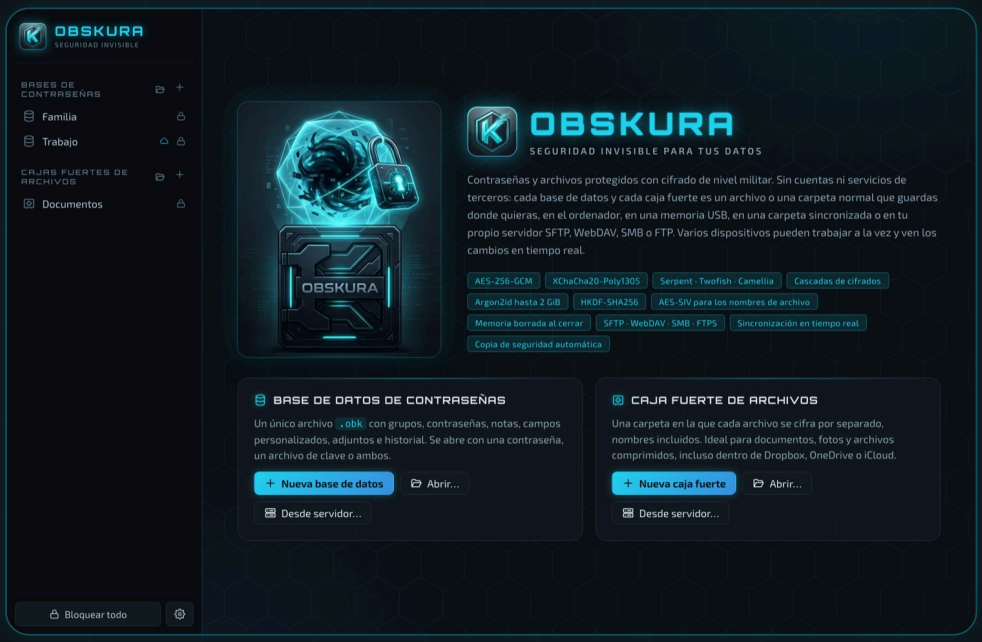


FIG. 1 La pantalla de bienvenida, con la barra lateral.

La **barra lateral** contiene las secciones **Bases de contraseñas** y **Cajas fuertes de archivos**. Junto a cada título hay dos botones: la carpeta para **abrir** un elemento existente y el **+** para crear uno nuevo.

- Cada elemento abierto recientemente queda en la lista, solo con su nombre: las rutas no aparecen nunca. El candado indica el estado: **cerrado** si está bloqueado, **abierto** si está desbloqueado.
- Al pasar sobre un elemento aparece una **×** para quitarlo de los recientes (el archivo no se borra) o un candado para bloquearlo enseguida.
- Abajo: **Bloquear todo** y el engranaje de los **Ajustes**.

PROTEGER LOS DATOS

03 CONTRASEÑAS Y ARCHIVOS DE CLAVE

Las bases de datos y las cajas fuertes se abren con una **contraseña maestra**, un **archivo de clave** o ambos juntos. La combinación de los dos es la protección más fuerte: hace falta algo que *sabes* y algo que *tienes*.

CONTRASEÑA MAESTRA

Una frase larga es más segura que una palabra compleja: cuatro o cinco palabras al azar son fáciles de recordar y dificilísimas de adivinar. El indicador bajo el campo estima su robustez en bits.

El botón del dado abre el **generador** si prefieres una contraseña aleatoria.



FIG. 2 Creación de una base de datos con las opciones de cifrado abiertas.

ARCHIVO DE CLAVE

Como en KeePass, **cualquier archivo** puede servir de clave. Puedes elegir **Usar un archivo existente** o **Generar uno nuevo**: Obskura crea un archivo de clave aleatorio en la ubicación que indiques.

Guárdalo, por ejemplo, en una memoria USB, separado de la base de datos. Obskura recuerda dónde está en cada dispositivo y lo busca sola cada vez que se abre (capítulo 11).

OPCIONES DE CIFRADO

Con **Opciones de cifrado** eliges lo costosa que debe ser la derivación de la clave y qué cifrado usar. Los valores predeterminados, Estándar y AES-256-GCM, ya son seguros para cualquier uso; todas las alternativas se describen en la página siguiente.

> **EL ARCHIVO DE CLAVE NUNCA DEBE MODIFICARSE**
>
> Si usas un archivo cualquiera (una foto, un documento) como clave, el mínimo cambio lo inutiliza. Los archivos generados por Obskura tienen un formato de texto reconocido que sigue siendo válido aunque cambien los saltos de línea. En cualquier caso, guarda una copia de seguridad.

PROTEGER LOS DATOS

03 ELEGIR EL CIFRADO

DERIVACIÓN DE LA CLAVE (ARGON2ID)

Argon2id transforma tus credenciales en la clave de cifrado: cuanta más memoria y pasadas usa, más costoso es para un atacante probar millones de contraseñas.

NIVEL	PARÁMETROS	TIEMPO DE APERTURA
Estándar	256 MiB de memoria, 3 pasadas	unos 0,5–1 segundos
Alta	1 GiB, 4 pasadas	unos 2–4 segundos
Extrema	2 GiB, 6 pasadas	unos 5–12 segundos

NIVEL EXTREMO

Cada apertura requiere **2 GiB de memoria libre**. En un ordenador con poca RAM la base de datos o la caja fuerte podrían no abrirse: elígelo solo si usarás tus archivos en ordenadores adecuados.

CIFRADOS

Todos los cifrados usan claves de 256 bits y están **autenticados**: se detecta cualquier alteración de los datos.

CIFRADO	CARACTERÍSTICAS
AES-256-GCM	**Predeterminado.** Estándar estadounidense aprobado para información TOP SECRET, el más rápido gracias a la aceleración por hardware.
XChaCha20-Poly1305	Cifrado de flujo, rápido en cualquier procesador incluso sin instrucciones AES.
Serpent-256-GCM	Finalista del concurso AES, con el mayor margen de seguridad (32 rondas). Más lento.
Twofish-256-GCM	Finalista del concurso AES, diseñado por Bruce Schneier y colaboradores.
Camellia-256-GCM	Estándar internacional ISO/IEC, recomendado en Europa (NESSIE) y Japón (CRYPTREC).
Cascada AES · Twofish · Serpent	**La opción más fuerte.** Tres cifrados en secuencia con claves independientes: los datos siguen protegidos aunque algún día se rompieran dos de los tres algoritmos.
Cascada AES · XChaCha20	Combina un cifrado por bloques y uno de flujo, de familias completamente distintas.

CAJAS FUERTES

En las cajas fuertes el cifrado elegido protege tanto las claves como el contenido de cada archivo. Si lo cambias con **Cambiar contraseña / archivo de clave**, los archivos existentes siguen cifrados con el anterior y los que añadas desde entonces usan el nuevo. El cifrado activo se indica abajo a la derecha en la caja fuerte.

GESTOR DE CONTRASEÑAS

04 BASES DE DATOS DE CONTRASEÑAS

CREAR UNA BASE DE DATOS

1. Haz clic en **Nueva base de datos** en la pantalla inicial, o en el **+** junto a **Bases de contraseñas**.
2. Escribe un **nombre** y elige dónde guardar el archivo `.obk`: **En este ordenador…** o **En un servidor…**.
3. Establece contraseña y/o archivo de clave (capítulo 03).
4. Pulsa **Crear**. La base de datos se abre ya desbloqueada.

ABRIR Y DESBLOQUEAR

1. Selecciona la base de datos en la barra lateral, o usa el icono de carpeta para abrir un archivo `.obk` existente.
2. Introduce la contraseña. El archivo de clave y la copia de seguridad se buscan automáticamente; si no se encuentra el archivo de clave, elígelo con **Elegir…**.
3. Pulsa **Desbloquear** o `Intro`.

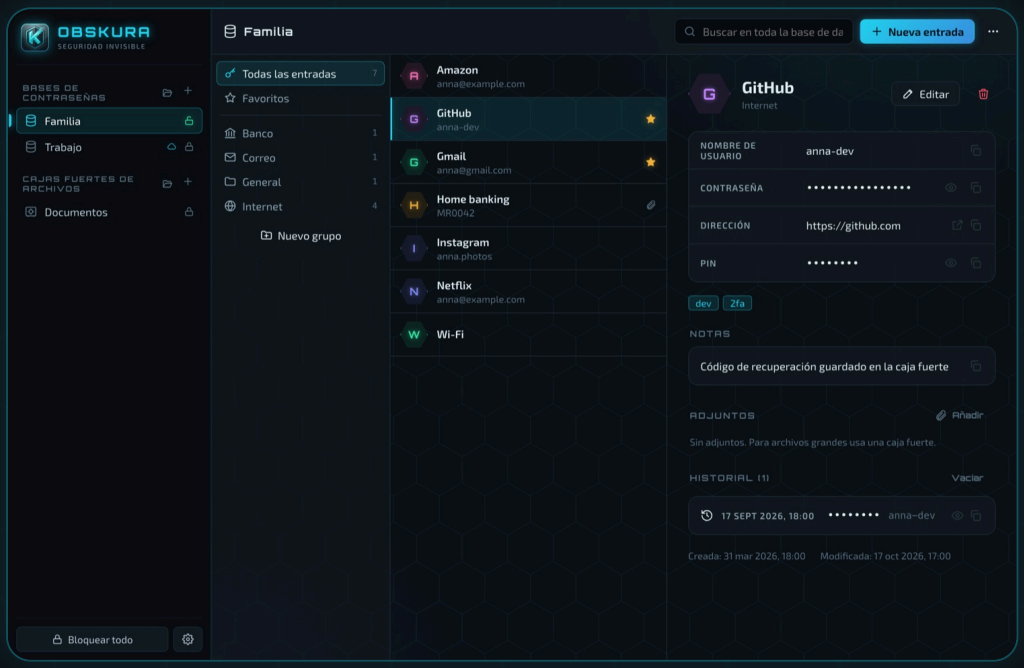


FIG. 3 Una base de datos desbloqueada: grupos, lista de entradas y detalle de la entrada seleccionada.

LAS TRES COLUMNAS

- **Grupos**: **Todas las entradas**, **Favoritos** y tus carpetas. Al pasar sobre un grupo aparecen los comandos para crear un subgrupo, editarlo o eliminarlo; **Nuevo grupo** está al final de la lista.
- **Entradas**: título y nombre de usuario de cada entrada. La estrella indica los favoritos y el clip los adjuntos. Con un **doble clic** copias directamente la contraseña.
- **Detalle**: todos los campos de la entrada, con botones para mostrar, copiar o abrir la dirección en el navegador.

BASES DE DATOS DE CONTRASEÑAS

05 GESTIONAR LAS ENTRADAS

Para añadir una entrada pulsa **Nueva entrada** (o `Ctrl/⌘` + `N`); para cambiarla, selecciónala y pulsa **Editar**. Guarda con el botón de abajo o con `Ctrl/⌘` + `S`. Cada cambio se escribe enseguida en el archivo de la base de datos.



FIG. 4 El editor de una entrada con el generador abierto.

CAMPOS DE UNA ENTRADA

Título y grupo	Nombre de la entrada y carpeta en la que está.
Nombre de usuario	Cuenta, correo o número de cliente.
Contraseña	Con indicador de robustez y generador.
Dirección	Se abre en el navegador desde el detalle.
Notas	Texto libre, cifrado como todo lo demás.
Etiquetas	Palabras clave separadas por comas.
Caducidad	Fecha a partir de la cual cambiar la contraseña.

La **estrella** de arriba añade la entrada a **Favoritos**.

GENERADOR DE CONTRASEÑAS

Haz clic en el dado del campo de contraseña. Elige la **longitud** (de 8 a 64 caracteres) y las familias de caracteres (`a–z`, `A–Z`, `0–9`, `!@#$`); con **Excluir ambiguos** evitas caracteres que se confunden como l, 1, O y 0. Después **Regenerar**, **Copiar** o **Usar esta contraseña**. Las contraseñas salen del generador aleatorio criptográfico del sistema.

CAMPOS PERSONALIZADOS

Añade información extra como PIN, códigos de recuperación o preguntas de seguridad. Marca **Protegido** para mostrarlos ocultos, como una contraseña.

ADJUNTOS E HISTORIAL

Adjunta archivos de hasta **64 MB** cada uno (para archivos más grandes usa una caja fuerte). Cada cambio conserva la versión anterior: el **Historial** guarda las últimas **20** y permite copiar una contraseña antigua.

BASES DE DATOS DE CONTRASEÑAS

06 HERRAMIENTAS DE LA BASE DE DATOS

BUSCAR

El campo **Buscar en toda la base de datos** de arriba (o `Ctrl/⌘` + `F`) filtra las entradas de todos los grupos mientras escribes. `Esc` vacía la búsqueda.

COPIAR DE FORMA SEGURA

Los botones de copia junto al nombre de usuario, la contraseña y los campos protegidos ponen el valor en el portapapeles, que Obskura **vacía automáticamente** a los 20 segundos (se puede cambiar en los ajustes). El portapapeles solo se vacía si aún contiene el valor copiado: si entretanto has copiado otra cosa, no lo toca.

EL MENÚ DE LA BASE DE DATOS

El botón ⋯ de arriba a la derecha contiene:

OPCIÓN	PARA QUÉ SIRVE
Propiedades de la base de datos	Cambiar el nombre y la descripción de la base de datos.
Cambiar contraseña / archivo de clave	Establecer nuevas credenciales. La base de datos se vuelve a cifrar con claves nuevas.
Guardar una copia de seguridad…	Escribir una copia cifrada de la base de datos en otra ubicación.
Copia de seguridad automática…	Configurar el segundo destino de las copias (capítulo 12).
Dispositivos y rutas…	Ver qué dispositivos usan la base de datos y sus rutas (capítulo 11).
Importar / Exportar	Desde un gestor en línea o desde CSV, y hacia CSV (capítulo 13).
Bloquear base de datos	Cerrar la base de datos y borrar sus datos de la memoria.

GUARDADO Y SINCRONIZACIÓN

Cada cambio se guarda enseguida de forma **atómica**: el archivo nuevo se escribe aparte y sustituye al antiguo solo cuando está completo, así que un corte de luz no puede corromperlo. Si entretanto otro ordenador ha modificado la base de datos, Obskura **combina** las dos versiones antes de guardar: no se pierde nada (capítulo 10). El único caso que requiere decidir es cuando en otro dispositivo se han cambiado la **contraseña o el archivo de clave**: Obskura propone bloquear la base de datos para volver a abrirla con las nuevas credenciales.

> **CONSEJO**
>
> Para usar la misma base de datos en varios ordenadores ponla en tu servidor (capítulo 09) o en una carpeta sincronizada: puedes tenerla abierta en todas partes a la vez.

ARCHIVOS CIFRADOS

07 CAJAS FUERTES DE ARCHIVOS

Una caja fuerte es una carpeta que contiene tus archivos cifrados. Vista desde fuera es solo un conjunto de archivos con nombres ilegibles: no se sabe ni qué contienen ni cómo están organizados.

CREAR UNA CAJA FUERTE

1. Haz clic en **Nueva caja fuerte**, o en el **+** junto a **Cajas fuertes de archivos**.
2. Elige un nombre y la carpeta donde crearla, incluso dentro de Dropbox, OneDrive o iCloud Drive, o en un servidor.
3. Establece contraseña y/o archivo de clave y pulsa **Crear**.

AÑADIR ARCHIVOS

- **Arrastra** archivos y carpetas desde Finder / Explorador a la ventana: se cifran en la carpeta que estás viendo.
- O usa **Añadir archivos** o **Añadir carpeta**.
- Los originales no se tocan: una vez cifrados puedes borrarlos tú.

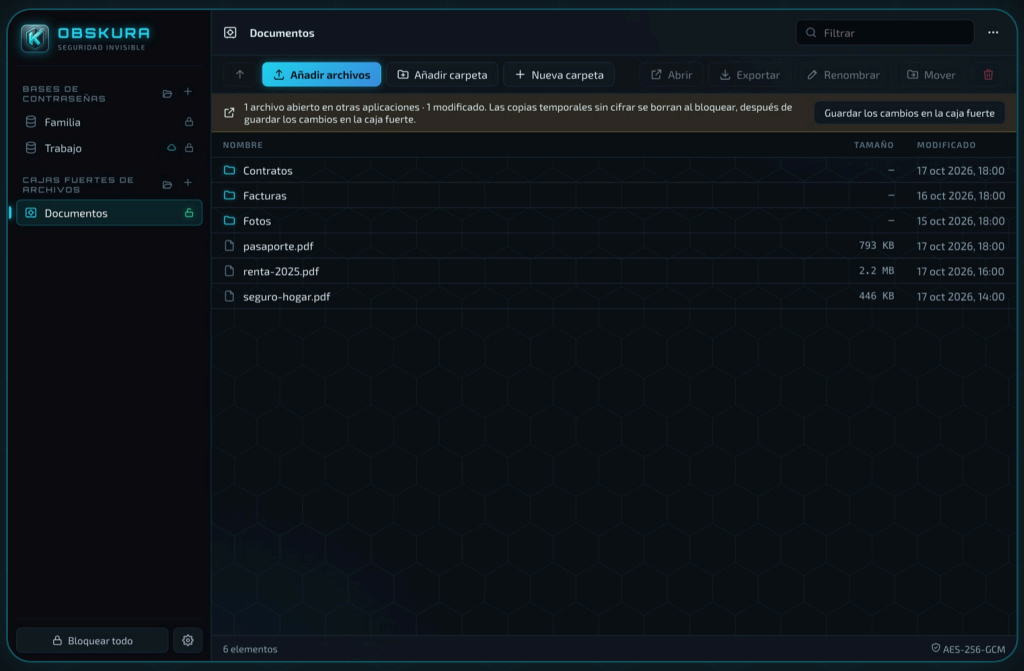


FIG. 5 Una caja fuerte desbloqueada.

LA BARRA DE COMANDOS

↑ vuelve a la carpeta superior · **Nueva carpeta** crea una subcarpeta · **Abrir**, **Exportar**, **Renombrar**, **Mover** y **Eliminar** actúan sobre los elementos seleccionados. Seleccionas varios con `Ctrl/⌘` + clic o `Mayús` + clic. Abajo, la barra de estado muestra el número de elementos y el progreso de las operaciones.

CAJAS FUERTES DE ARCHIVOS

08 TRABAJAR CON LOS ARCHIVOS

ABRIR Y MODIFICAR UN ARCHIVO

Haz doble clic en un archivo (o selecciónalo y pulsa **Abrir**). Obskura lo descifra en una carpeta temporal protegida y lo abre con la aplicación predeterminada del sistema.

1. Modifica y guarda el archivo normalmente en la otra aplicación.
2. En Obskura aparece una franja que indica los archivos abiertos y los modificados.
3. Pulsa **Guardar los cambios en la caja fuerte** para volver a cifrar la nueva versión.

> **COPIAS TEMPORALES SIN CIFRAR**
>
> Mientras un archivo está abierto, su copia descifrada existe en el disco. Al bloquear la caja fuerte, Obskura guarda primero los cambios pendientes y después **borra las copias temporales**. Cierra el archivo en la otra aplicación antes de bloquear.

EXPORTAR

Exportar descifra los elementos seleccionados, carpetas incluidas, en una carpeta que elijas. Los archivos exportados quedan **sin cifrar**: usa esta función solo cuando los necesites fuera de la caja fuerte.

ORGANIZAR

Renombra con **Renombrar** o `F2`; mueve con **Mover** eligiendo la carpeta de destino. **Eliminar** (o `Supr`) siempre pide confirmación. El campo **Filtrar** muestra solo los elementos cuyo nombre contiene el texto introducido.

SINCRONIZACIÓN CON LA NUBE

Cada archivo de la caja fuerte se cifra por separado: si cambias un documento, el servicio de sincronización sube solo ese archivo. Por eso las cajas fuertes funcionan bien dentro de Dropbox, OneDrive, Google Drive o iCloud Drive.

CÓMO ES UNA CAJA FUERTE EN EL DISCO

ELEMENTO	CONTENIDO
`vault.obkv`	Las claves de la caja fuerte, cifradas con tus credenciales.
`vault.obkv.bak`	Copia idéntica de seguridad, por si el primer archivo se daña.
`vault.obkx`	El archivo complementario, cifrado con la clave de acceso: archivo de clave, copia de seguridad y rutas de cada dispositivo (capítulo 11).
`d/`	Todos los archivos y carpetas cifrados, uno junto a otro: la estructura real no es visible.

Para abrir una caja fuerte existente usa el icono de carpeta junto a **Cajas fuertes de archivos** y elige su carpeta principal. No modifiques ni muevas a mano los archivos de su interior.

DÓNDE GUARDAR

09 SERVIDORES REMOTOS

Las bases de datos y las cajas fuertes no tienen por qué estar en el ordenador: Obskura las abre y guarda directamente en tu servidor, sin programas de sincronización de por medio. Los datos viajan y se quedan en el servidor **ya cifrados**: el administrador del servidor, o quien lo vulnerara, solo ve archivos ilegibles.

PROTOCOLO	DÓNDE SE USA	NOTAS
SFTP	NAS (Synology, QNAP, TrueNAS), servidores Linux, VPS	Recomendado. Contraseña o clave SSH.
WebDAV	Nextcloud, ownCloud, Synology, QNAP, Box, Koofr	Sobre HTTPS. Para Nextcloud la ruta es `/remote.php/dav/files/<usuario>`.
SMB	Carpetas compartidas de Windows, NAS, Samba	SMB 2 y 3; indica el nombre del recurso compartido.
FTPS	Alojamientos y servidores FTP con TLS	FTP cifrado con `AUTH TLS`.
FTP	Servidores FTP tradicionales	Las credenciales del servidor viajan sin cifrar: mejor FTPS o SFTP.

CONFIGURAR UNA CONEXIÓN

1. Abre **Ajustes → Conexiones a servidores** y pulsa **Nueva conexión**.
2. Elige el protocolo e introduce dirección, puerto (si no es el estándar), usuario y contraseña.
3. Pulsa **Probar conexión** y después **Guardar**.

La contraseña del servidor va al **llavero del sistema** (Llavero de macOS, Administrador de credenciales de Windows, Secret Service en Linux), nunca al archivo de ajustes. También se copia, cifrada, en el archivo complementario: tus otros ordenadores recrean la conexión solos.

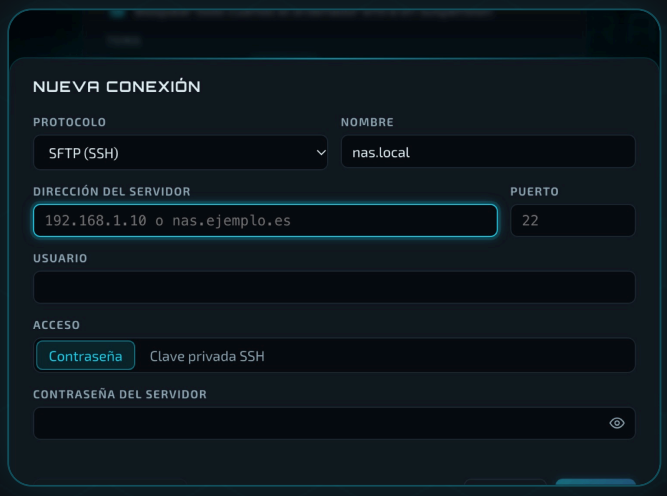


FIG. 6 Una nueva conexión SFTP.

CLAVE DEL SERVIDOR (SFTP)

En la primera conexión Obskura muestra la **huella** de la clave del servidor y te pide aceptarla, como hace `ssh`. Si más adelante la huella cambia, la conexión se rechaza hasta que vuelvas a confirmarla: podría ser alguien haciéndose pasar por tu servidor. Si no ha cambiado nada en el servidor, no la aceptes.

ABRIR Y GUARDAR EN UN SERVIDOR

- **Abrir:** el icono de carpeta junto a **Bases de contraseñas** o **Cajas fuertes de archivos** ofrece **Desde este ordenador…** y **Desde un servidor…**. Lo mismo en la pantalla inicial con **Desde servidor…**.
- **Crear:** en la ventana **Nueva base de datos** o **Nueva caja fuerte** elige **En un servidor…** en lugar de **En este ordenador…**.
- Los elementos en un servidor aparecen entre los recientes con el icono de la **nube**; una vez abiertos muestran la etiqueta `SERVIDOR` en la barra superior.



FIG. 7 El navegador del servidor: elige la conexión y la carpeta.

En el navegador elige la conexión arriba a la izquierda y muévete por las carpetas. Para una base de datos haz clic en el archivo `.obk`; para una caja fuerte entra en su carpeta (la que tiene `vault.obkv`) y pulsa **Abrir esta caja fuerte**. Con el icono de carpeta+ creas una carpeta nueva en el servidor.

RENDIMIENTO

Las bases de datos son pequeñas y se abren en un instante incluso en remoto. Las cajas fuertes transfieren un archivo cada vez, cuando lo abres o lo exportas: con archivos muy grandes cuenta la velocidad de la conexión.

COLABORACIÓN

10 VARIOS DISPOSITIVOS EN TIEMPO REAL

La misma base de datos o la misma caja fuerte pueden estar abiertas a la vez en varios ordenadores: los cambios hechos en uno aparecen en los demás en pocos segundos.

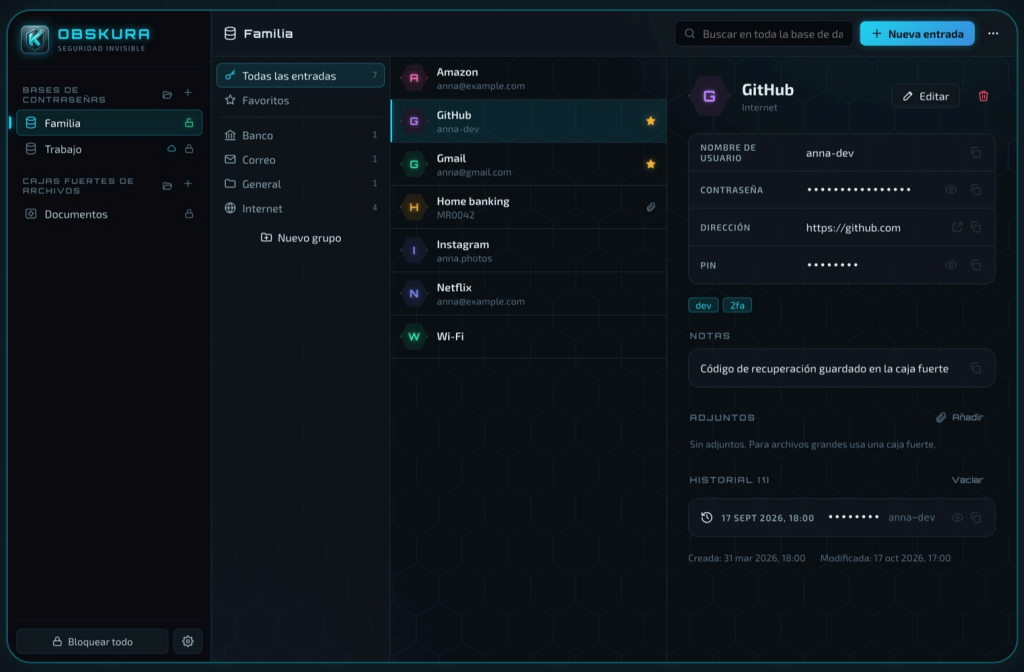


FIG. 8 Una notificación: otro dispositivo ha añadido y modificado entradas.

CÓMO FUNCIONA

- Obskura comprueba el archivo cada **2 segundos** en el disco local o en una carpeta sincronizada, cada **5 segundos** en un servidor. La comprobación solo lee los primeros 88 bytes del archivo.
- Cuando encuentra una versión nueva la **combina** con la tuya entrada por entrada, muestra una notificación con las entradas añadidas, modificadas o eliminadas y actualiza la lista al instante.
- Si dos personas modifican la **misma entrada**, gana el cambio más reciente; el otro no se pierde: va al **Historial** de la entrada.
- Una eliminación llega a todos, salvo que entretanto alguien haya modificado esa entrada: en ese caso el cambio tiene prioridad y la entrada se queda.
- En las cajas fuertes, cuando alguien añade, renombra o elimina archivos en la carpeta que estás viendo, la lista se actualiza sola.

RELOJES DE LOS ORDENADORES

Para decidir qué cambio es más reciente Obskura usa la hora de los ordenadores: mantenlos sincronizados (ajuste automático de la hora, normalmente activo en todos los sistemas).

ENCONTRARLO TODO, EN TODAS PARTES

11 CLAVE DE ACCESO Y DISPOSITIVOS

Junto a cada base de datos y cada caja fuerte hay un pequeño archivo cifrado que recuerda dónde están el archivo de clave, las copias de seguridad y los servidores, y cómo llega a ellos cada uno de tus dispositivos. Lo protege la clave de acceso de Obskura.

LA CLAVE DE ACCESO DE OBSKURA

Es un código de 55 caracteres generado en el primer inicio (o introducido, si lo creaste en otro ordenador). Se queda en el llavero del sistema; desde **Ajustes → Clave de acceso de Obskura** puedes:

- **Mostrar**: verla y copiarla para introducirla en otro ordenador.
- **Cambiar clave…**: generar una nueva. Obskura vuelve a cifrar enseguida los archivos complementarios accesibles; los demás se actualizan al abrirlos (las claves anteriores siguen sirviendo para leerlos).
- **Introducir clave…**: usar la clave actual si se cambió en otro ordenador.

LOS ARCHIVOS COMPLEMENTARIOS

Están cifrados con AES-256-GCM y son ilegibles sin la clave de acceso:

ARCHIVO	CONTIENE
`.obk.obkx`	Junto a cada base de datos: ubicación del archivo de clave, configuración de la copia de seguridad, conexiones a servidores y los registros de los dispositivos.
`vault.obkx`	Dentro de cada caja fuerte: la misma información.
`recenti.obkx`	En la carpeta de datos de la app: la lista de recientes. En el disco no quedan rutas sin cifrar.

ABRIR DESDE OTRO ORDENADOR

Una vez introducida la clave de acceso en el nuevo ordenador, basta con seleccionar la base de datos: Obskura lee el archivo complementario, recrea las conexiones a servidores que falten, encuentra el archivo de clave (en la ubicación conocida para ese dispositivo, junto a la base de datos, en las rutas de los demás dispositivos o en la copia de seguridad) y propone la copia de seguridad si el original no está accesible.

IMPORTANTE

La clave de acceso no sustituye la contraseña de las bases de datos: sin la contraseña (y el archivo de clave) los datos siguen siendo ilegibles. Aun así guárdala en un lugar seguro: sin ella tendrás que elegir a mano el archivo de clave y las copias de seguridad.

DISPOSITIVOS Y RUTAS

Cada ordenador que usa Obskura tiene un **identificador único**, generado en el primer inicio, y un **nombre** (el del ordenador, editable en **Ajustes → Nombre de este dispositivo**). Cada vez que abre una base de datos o una caja fuerte, escribe su propio registro en el archivo complementario cifrado:

DATO	EJEMPLO
Identificador y nombre	`3f2a9c1e-…` · «MacBook de casa»
Sistema y versión	macOS · Obskura 0.3.0 · último acceso
Ruta de la base de datos	`/Users/ana/Dropbox/cuentas.obk` en el Mac, `D:\Dropbox\cuentas.obk` en el PC
Ruta del archivo de clave	`/Volumes/USB/clave.obkey` o `E:\clave.obkey`
Copia de seguridad propia	una carpeta de ese dispositivo, o la configuración común (capítulo 12)

LA VENTANA «DISPOSITIVOS Y RUTAS»

En el menú ⋯ de una base de datos o una caja fuerte elige **Dispositivos y rutas…**:

- ves todos los dispositivos registrados, con sistema, versión, último acceso, uso del archivo de clave y destino de la copia de seguridad;
- el icono del ojo muestra las rutas de cada uno; el lápiz renombra este dispositivo;
- la papelera **olvida** un dispositivo que ya no usas: sus rutas y su copia de seguridad se quitan del archivo (si vuelve a abrirlo, se registra de nuevo).

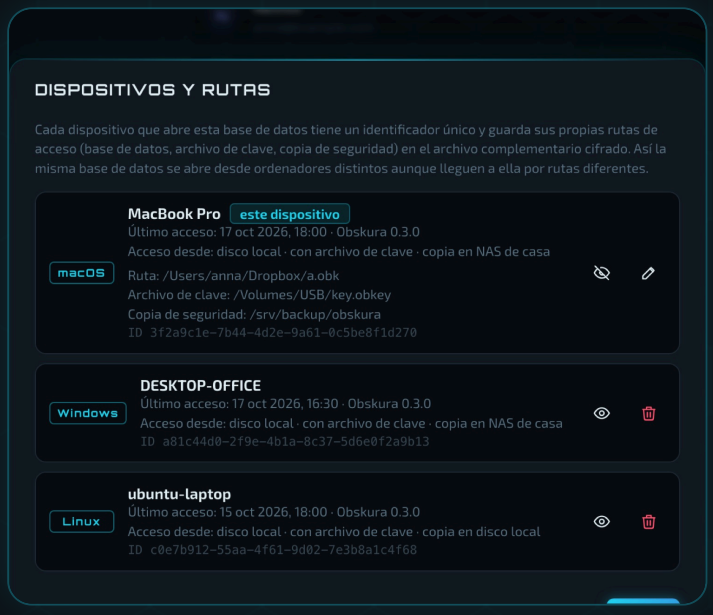


FIG. 9 Los dispositivos que usan una base de datos.

POR QUÉ ES ÚTIL

La misma base de datos en Dropbox tiene rutas distintas en Mac, Windows y Linux, y la memoria USB con el archivo de clave cambia de letra o de nombre. Gracias a los registros por dispositivo cada uno encuentra sus propias rutas, sin sobrescribir las de los demás.

SEGURIDAD DE LOS DATOS

12 COPIA DE SEGURIDAD AUTOMÁTICA

Cada base de datos y cada caja fuerte puede tener un **segundo destino**, en este ordenador (por ejemplo un disco externo) o en cualquier servidor configurado. Con cada cambio Obskura copia allí la nueva versión en segundo plano, sin ralentizarte.

1. En el menú ⋯ de la base de datos o de la caja fuerte elige **Copia de seguridad automática…**
2. Activa **Copia de seguridad automática activada** y elige la carpeta: **En este ordenador…** o **En un servidor…**.
3. Si el destino es un servidor, puedes marcar **Usar esta configuración en todos los dispositivos**.
4. Para las bases de datos elige cuántas **copias fechadas** conservar.
5. Pulsa **Guardar**. Con **Ejecutar ahora** fuerzas una copia completa.



FIG. 10 Copia de seguridad en un NAS, común a todos los dispositivos.

QUÉ	CÓMO SE COPIA
Base de datos	El archivo `.obk` en la carpeta de copia, más las copias fechadas `nombre.AAAAMMDD-hhmmss.obk`; las más antiguas por encima del límite se eliminan.
Caja fuerte	Una réplica de la carpeta cifrada: con cada cambio solo se vuelven a copiar los archivos afectados. La copia se abre como una caja fuerte normal.
Archivo de clave	Opcional: se copia una vez, al guardar el ajuste, en la carpeta que indiques.

UNA COPIA PARA CADA DISPOSITIVO

- Cada dispositivo tiene su **propia configuración**, guardada con su identificador en el archivo complementario: una carpeta local (por ejemplo el disco externo del Mac) solo vale en ese dispositivo.
- Un destino en un servidor puede convertirse en **común**: los demás dispositivos lo usan, salvo los que tengan configuración propia. La ventana indica quién lo estableció.
- Las copias siguen **cifradas**: no hace falta confiar en el destino de la copia.
- Si una copia falla aparece un aviso; Obskura lo vuelve a intentar con el siguiente cambio.

ARCHIVO DE CLAVE Y COPIA DE SEGURIDAD

No pongas el archivo de clave en la misma carpeta que la copia: quien accediera a esa carpeta tendría la base de datos y la mitad de las credenciales.

DESDE Y HACIA OTROS PROGRAMAS

13 IMPORTAR Y EXPORTAR

IMPORTAR DESDE UN GESTOR EN LÍNEA

Obskura accede directamente a tu antiguo servicio, descarga la caja fuerte cifrada y la descifra en tu ordenador, sin pasar por un archivo exportado sin cifrar. Las credenciales solo sirven para ese acceso y no se guardan.

1. Abre la base de datos de destino y elige ⋯ → **Importar desde un gestor en línea…**
2. Elige el servicio y accede; si usas verificación en dos pasos Obskura te pide el código.
3. Revisa la vista previa: número de entradas, carpetas, ejemplos.
4. Decide si recrear las carpetas como grupos y si omitir las entradas ya existentes, y pulsa **Importar**.

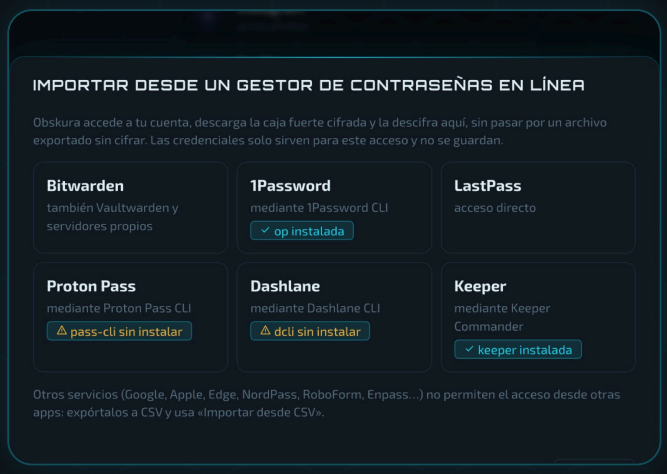


FIG. 11 La elección del servicio desde el que importar.

SERVICIO	ACCESO
Bitwarden / Vaultwarden	Directo, también bitwarden.eu y servidores propios; como alternativa, con la clave API personal.
LastPass	Directo, con verificación en dos pasos (código o confirmación en el teléfono).
1Password	Mediante 1Password CLI (`op`), autorizada por la app de 1Password o con correo, contraseña y Secret Key.
Proton Pass	Mediante Proton Pass CLI (`pass-cli`), con acceso desde el navegador.
Dashlane	Mediante Dashlane CLI (`dcli`), tras un primer `dcli sync` en el terminal.
Keeper	Mediante Keeper Commander (`keeper`).

Se conservan carpetas, campos personalizados, códigos TOTP, tarjetas y notas. Otros servicios (Google, Apple, Edge, NordPass…) no permiten el acceso desde otras apps: expórtalos a CSV.

IMPORTAR DESDE CSV (KEEPASS Y OTROS)

1. En el programa de origen exporta a CSV: KeePass 2 **Archivo → Exportar → KeePass CSV (1.x)**, KeePassXC **Base de datos → Exportar → Archivo CSV**, Bitwarden, 1Password, Chrome, Edge y Firefox desde sus ajustes.
2. En Obskura abre la base de datos y elige ⋯ → **Importar desde CSV (KeePass, …)…**
3. Elige el archivo: Obskura reconoce el formato y las columnas y muestra una vista previa.
4. Decide si recrear los grupos del archivo y si omitir las entradas ya existentes, y pulsa **Importar**.



FIG. 12 Vista previa de una exportación de KeePassXC.

Se conservan grupos, etiquetas, códigos TOTP (guardados como campo protegido), fechas de creación y caducidades; las columnas no reconocidas se convierten en campos personalizados. Volver a importar el mismo archivo no crea duplicados.

EXPORTAR A CSV

⋯ → **Exportar a CSV…** crea un archivo con las columnas de KeePassXC, más etiquetas, caducidad, favoritos y campos personalizados: se puede volver a importar en Obskura, en KeePassXC y en la mayoría de gestores de contraseñas.

EL CSV NO ESTÁ CIFRADO

El archivo contiene todas las contraseñas sin cifrar. Úsalo solo para trasladar los datos y luego bórralo. Tras la importación borra también el CSV exportado del programa antiguo. Para las copias usa la copia de seguridad automática, que sigue cifrada.

PERSONALIZAR

14 IDIOMAS

Obskura habla ocho idiomas y se pueden añadir otros: todos los textos de la app están en archivos XML, uno por idioma.

ELEGIR EL IDIOMA

Al iniciar, Obskura usa el idioma del sistema; si no está entre los incluidos usa el inglés. En **Ajustes → Idioma** puedes dejar **Automático** o elegir uno: el cambio es inmediato, también para los mensajes de error. El árabe se lee de derecha a izquierda y la interfaz se invierte en consecuencia.

Italiano	it
English	en
Deutsch	de
Español	es
Русский	ru
中文（简体）	zh
日本語	ja
العربية	ar

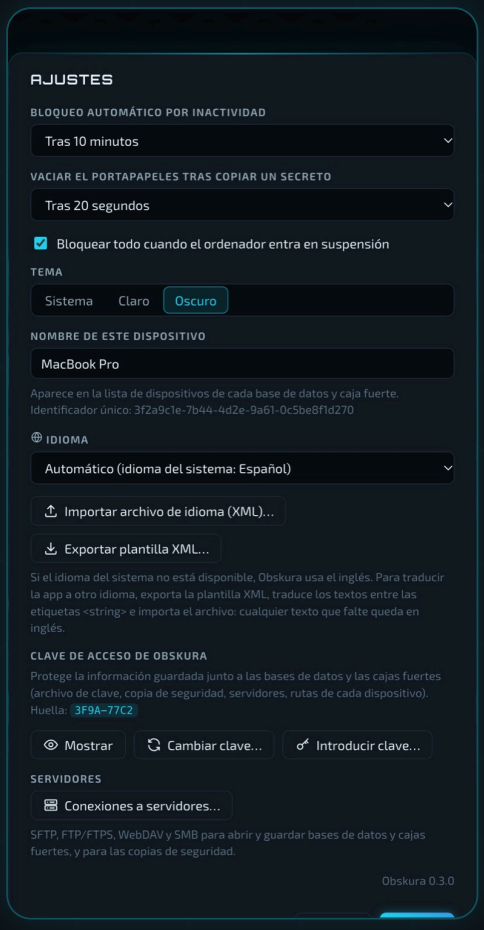


FIG. 13 La sección Idioma de los ajustes.

AÑADIR UN IDIOMA

1. En **Ajustes → Idioma** pulsa **Exportar plantilla XML...**: obtienes el archivo completo del idioma actual (o descarga desde la web el zip con los XML de todos los idiomas).
2. Cambia en la cabecera `code` (el código del idioma, por ejemplo `fr` o `pt-BR`), `name` y, para los idiomas de derecha a izquierda, `dir="rtl"`.
3. Traduce el texto de cada elemento `<string>` con cualquier editor de texto, guardando en UTF-8.
4. Pulsa **Importar archivo de idioma (XML)...**: el idioma aparece en la lista al instante y se usa automáticamente en los sistemas en ese idioma.

EL FORMATO DEL ARCHIVO

Un archivo de idioma es un XML con un elemento `<language>` y un `<string>` por cada texto:

```
<?xml version="1.0" encoding="UTF-8"?>
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.cancel">Annuler</string>
  <string key="db.syncFailed">Échec de la synchronisation : {message}</string>
  <string key="vault.itemsN.one">{count} élément</string>
  <string key="vault.itemsN.other">{count} éléments</string>
</language>
```

- el atributo `key` no se traduce ni se cambia;
- los marcadores entre llaves, como `{count}` o `{name}`, se dejan como están: la app los sustituye por números y nombres;
- las etiquetas `<b>` y `<code>` del texto deben conservarse;
- las claves que terminan en `.one`, `.two`, `.few`, `.many` y `.other` son las formas de plural: usa las de tu idioma; `.other` es obligatoria;
- un texto que falta se muestra en inglés, así que una traducción parcial ya funciona.

CORREGIR UN IDIOMA INCLUIDO

Un archivo XML con el mismo `code` que un idioma incluido (por ejemplo `es`) no lo sustituye: solo corrige las entradas que contiene. En los ajustes aparece con la indicación **correcciones** y se quita con la ×, volviendo a los textos originales.

CONSEJO

Los archivos importados se quedan en la carpeta de datos de la app y solo valen en ese ordenador: impórtalos también en los demás.

TRADUCIR CON LA PLANTILLA XML VACÍA

Para un idioma nuevo puedes partir de la plantilla vacía `obskura-translation-template.xml`, que se descarga desde el sitio web (`obskura.bytenooks.com`, sección Descarga). Tiene una línea por cada texto de la aplicación: el texto se escribe entre `<string …>` y `</string>`, y el atributo `en` contiene el texto inglés de referencia y puede quedarse donde está (la aplicación lo ignora).

```
<language code="fr" name="Français" english-name="French" dir="ltr">
  <string key="common.lock" en="Lock">Verrouiller</string>
  <string key="common.settings" en="Settings">Paramètres</string>
  <string key="common.cancel" en="Cancel">Annuler</string>
</language>
```

1. Descarga la plantilla y guárdala con el código de tu idioma, por ejemplo `fr.xml`.
2. En la primera línea `<language>` rellena `code`, `name`, `english-name` y, si hace falta, `dir="rtl"`.
3. Escribe las traducciones con un editor de texto que guarde en UTF-8, respetando las reglas anteriores.
4. **Borra las líneas que no traduzcas**: un texto vacío aparecería en blanco en la aplicación, mientras que una línea ausente se muestra en inglés.
5. Importa el archivo en **Ajustes → Idioma** y comprueba los textos en la aplicación.

COMPARTE TU TRADUCCIÓN

Envíala al desarrollador desde la página de contacto del sitio: elige el tema «Traducción» y adjunta el archivo XML (hasta 3 MB; un archivo de idioma completo ocupa unos 100–150 KB). Las traducciones recibidas podrán incluirse en próximas versiones.

SEGURIDAD

15 BLOQUEO Y AJUSTES

Al bloquear una base de datos o una caja fuerte, Obskura cierra la sesión y **borra de la memoria** las claves y los datos descifrados. Para volver a abrirlas hacen falta otra vez las credenciales.

FORMAS DE BLOQUEAR

- **Bloquear todo** al pie de la barra lateral, o `Ctrl/⌘` + `L`.
- El candado junto a un elemento desbloqueado de la barra lateral, o la opción **Bloquear** del menú ⋯.
- **Automáticamente**, tras un periodo de inactividad o cuando el ordenador entra en suspensión.

AJUSTES

AJUSTE	EFECTO	PREDETERMINADO
Bloqueo automático por inactividad	Bloquea todo tras 1–60 minutos sin usar ratón ni teclado, o nunca.	10 minutos
Vaciar el portapapeles	Vacía el portapapeles 10–120 segundos después de copiar un secreto, o nunca.	20 segundos
Bloqueo en suspensión	Bloquea todo cuando el ordenador entra en suspensión.	Activado
Tema	Sistema, Claro u Oscuro.	Oscuro
Nombre de este dispositivo	Aparece en la lista de dispositivos de cada base de datos y caja fuerte; debajo está el identificador único.	Nombre del ordenador
Idioma	Automático o uno de los idiomas disponibles; importación y exportación de archivos XML (capítulo 14).	Automático
Clave de acceso de Obskura	Mostrar, cambiar o introducir la clave (capítulo 11).	—
Servidores	Las conexiones SFTP, FTP/FTPS, WebDAV y SMB (capítulo 09).	—

Los ajustes no contienen secretos: las contraseñas de los servidores están en el llavero del sistema y la lista de recientes está cifrada con la clave de acceso.

REFERENCIA

16 ATAJOS Y CRIPTOGRAFÍA

ATAJOS DE TECLADO

TECLAS	DÓNDE	ACCIÓN
`Ctrl/⌘` + `L`	En cualquier sitio	Bloquear todo
`Esc`	Ventanas de diálogo	Cierra la ventana
`Ctrl/⌘` + `F`	Base de datos	Buscar
`Ctrl/⌘` + `N`	Base de datos	Nueva entrada
`Ctrl/⌘` + `S`	Editor de una entrada	Guardar la entrada
Doble clic	Lista de entradas	Copiar la contraseña
`Ctrl/⌘` + `A`	Caja fuerte	Seleccionar todo
`Enter`	Caja fuerte	Abre el archivo o la carpeta
`F2`	Caja fuerte	Renombrar
`Del` · `⌘` + `⌫`	Caja fuerte	Eliminar los elementos seleccionados
`⌫`	Caja fuerte	Volver a la carpeta superior

DETALLES CRIPTOGRÁFICOS

COMPONENTE	ALGORITMO
Derivación de la clave	Argon2id: 256 MiB / 3 pasadas, 1 GiB / 4 pasadas o 2 GiB / 6 pasadas, sal aleatoria de 256 bits.
Clave compuesta	SHA-256 de la contraseña (normalizada NFC) y el archivo de clave, como KeePass KDBX4.
Cifrado	AES-256, XChaCha20, Serpent, Twofish, Camellia o cascadas, siempre autenticados (GCM o Poly1305); en las cascadas cada capa tiene su propia clave derivada mediante HKDF.
Subclaves	HKDF-SHA256 con una semilla nueva en cada guardado.
Integridad	Cabecera autenticada: cualquier alteración impide abrir.
Nombres en las cajas fuertes	AES-SIV, vinculados a la carpeta que los contiene.
Contenido de los archivos	Bloques de 64 KiB, clave aleatoria por archivo, protección contra reordenación y truncamiento.
Archivos complementarios	AES-256-GCM con una clave derivada mediante HKDF de la clave de acceso de Obskura (256 bits aleatorios).
Memoria	Las claves y los datos sin cifrar se quedan en el proceso nativo y se borran al cerrar.

SOPORTE

17 BUENAS PRÁCTICAS Y PROBLEMAS

BUENAS PRÁCTICAS

- **Activa la copia de seguridad automática** o copia con regularidad los archivos `.obk` y las carpetas de las cajas fuertes en un disco externo. Ya están cifrados, así que la copia es segura dondequiera que la guardes.
- **Guarda el archivo de clave por separado** de la base de datos y ten al menos una copia de reserva.
- **Guarda la clave de acceso de Obskura** en papel o en un lugar distinto del ordenador.
- **Usa una contraseña distinta para cada servicio**, creada con el generador: solo tendrás que recordar una.
- **Bloquea cuando te alejes**: `Ctrl/⌘` + `L` es el gesto más rápido.
- **Olvida los dispositivos** que ya no uses, desde la ventana **Dispositivos y rutas**.

PREGUNTAS FRECUENTES

HE OLVIDADO LA CONTRASEÑA MAESTRA. ¿PUEDO RECUPERARLA?

No. Es justo lo que hace seguro a Obskura: nadie, ni siquiera los desarrolladores, puede abrir una base de datos o una caja fuerte sin las credenciales correctas.

«CONTRASEÑA O ARCHIVO DE CLAVE INCORRECTOS», PERO ESTOY SEGURO DE QUE SON CORRECTOS.

Comprueba que has elegido el mismo archivo de clave usado al crearla y que no se ha modificado. Si usaste contraseña *y* archivo de clave, hacen falta los dos. Revisa también el Bloq Mayús.

LA APERTURA TARDA UNOS SEGUNDOS. ¿ES NORMAL?

Sí: es el tiempo de Argon2id, buscado para frenar a quien intenta adivinar la contraseña. Con el nivel Alta hacen falta unos segundos y 1 GiB de memoria libre; con Extrema hasta 12 segundos y 2 GiB.

EN OTRO ORDENADOR NO SE ENCUENTRA EL ARCHIVO DE CLAVE.

Conecta la unidad que lo contiene: Obskura lo busca en la ruta que ese ordenador usó la última vez, junto a la base de datos, en las rutas de los demás dispositivos y en la copia de seguridad. Si no lo encuentra, elígelo con **Elegir…**: la próxima vez la ruta quedará recordada para ese dispositivo.

APARECE «PROTEGIDA CON UNA CLAVE DE ACCESO DISTINTA».

La clave de acceso se ha cambiado en otro ordenador. Haz clic en **Introduce la clave actual** y usa la nueva; de todos modos puedes desbloquear con la contraseña y elegir a mano el archivo de clave.

HA APARECIDO «CREDENCIALES CAMBIADAS EN OTRO SITIO».

En otro dispositivo alguien ha cambiado la contraseña o el archivo de clave de la base de datos. Elige **Bloquear** y vuelve a abrirla con las nuevas credenciales; **Sobrescribir** anularía el cambio hecho en otro sitio.

NO CONSIGO CONECTAR CON EL SERVIDOR.

Comprueba dirección, puerto y credenciales con **Probar conexión**. Para WebDAV verifica la ruta base (para Nextcloud `/remote.php/dav/files/<usuario>`); para SMB el nombre del recurso compartido. Con un certificado autofirmado activa **Aceptar certificados autofirmados** solo en una red de confianza.

LOS CAMBIOS EN UN ARCHIVO DE LA CAJA FUERTE NO APARECEN GUARDADOS.

Asegúrate de haber guardado el archivo en la otra aplicación y pulsa **Guardar los cambios en la caja fuerte**. Si bloqueas la caja fuerte con el archivo aún abierto, Obskura intenta guardarlo de todos modos antes de borrar la copia temporal.

LA APP SE ABRE EN UN IDIOMA QUE NO ES EL MÍO.

Obskura sigue el idioma del sistema; si el tuyo no está incluido usa el inglés. Elige el idioma en **Ajustes → Idioma** o importa un archivo XML (capítulo 14).

MACOS O WINDOWS DICEN QUE LA APP NO ESTÁ VERIFICADA.

La app no está firmada con un certificado comercial. Sigue las instrucciones del capítulo 02 para abrirla la primera vez.



OBSKURA

SEGURIDAD INVISIBLE PARA TUS DATOS

Gestor de contraseñas y cajas fuertes de archivos cifradas · en tu ordenador o en tu servidor

macOS · Windows · Linux · Versión **0.3.0**

https://obskura.bytenooks.com