



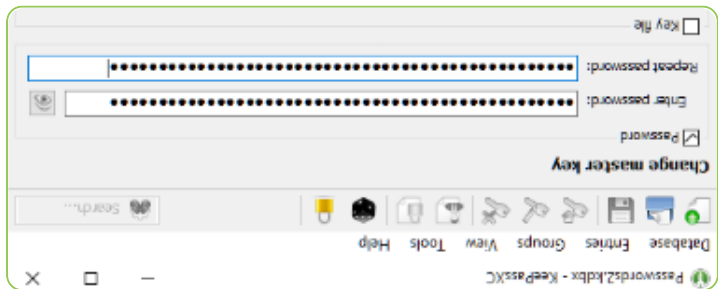
- Descarga KeePassXC desde su sitio oficial: <https://keepassxc.org/>
- Sigue las instrucciones de instalación según tu sistema operativo.

## Paso 1: Instalación

Es un gestor de contraseñas de código abierto que te permite almacenar y administrar de forma segura tus credenciales en una **base de datos cifrada**. A diferencia de otros servicios en la nube, KeePassXC funciona completamente en tu dispositivo, **sin necesidad de conexión a internet** y sin depender de servidores remotos.

## Paso 2: Creación de la base de datos de contraseñas

- Abre KeePassXC.
- Haz clic en "Crear nueva base de datos".
- Asigna un nombre y selecciona una ubicación para guardar el archivo de base de datos (extensión .kdbx).
- Crea una contraseña maestra: Usa una contraseña segura y fácil de recordar.

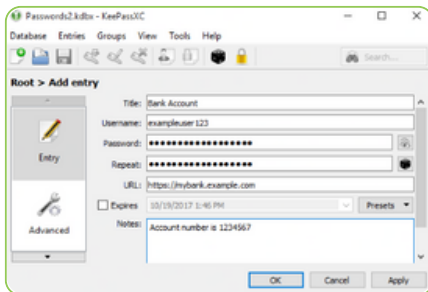


- Opcional: Configura una clave adicional como un archivo llave o YubiKey para mayor seguridad.



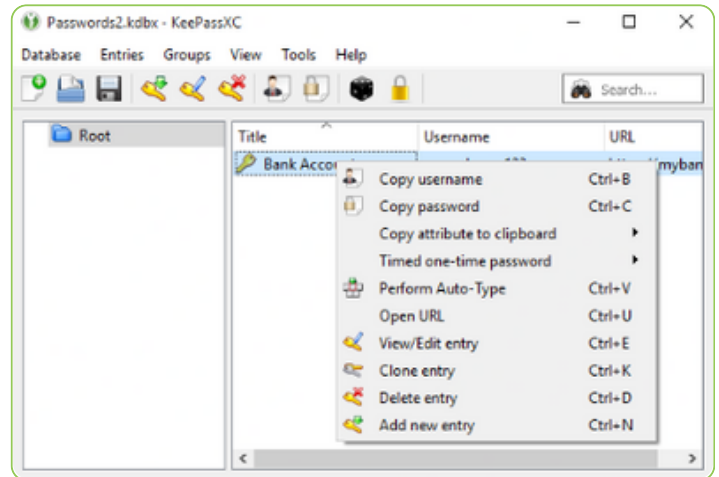
### Paso 3: Añadir contraseñas

- Abre tu base de datos introduciendo la contraseña maestra.
- Haz clic en "Añadir Entrada" (icono con un signo más o botón derecho en la lista).
- Introduce los datos:
  1. Título: Ej. "Correo Electrónico Gmail".
  2. Usuario: Tu nombre de usuario o correo electrónico.
  3. Contraseña: Usa el generador de KeePassXC para crear contraseñas seguras.
  4. URL: Si aplica, introduce la dirección del sitio web.
- Guarda la entrada.



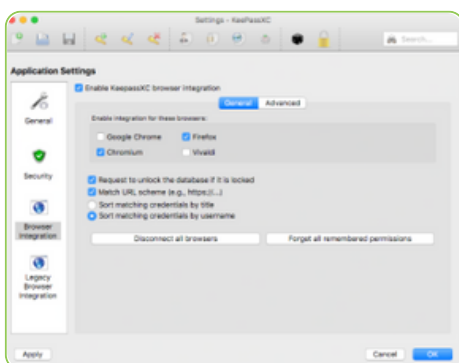
### Paso 4: Usar el Generador de Contraseñas

- En el menú superior, haz clic en "Generador de Contraseñas" y configura:
  1. Longitud.
  2. Inclusión de mayúsculas, números y símbolos.
- Copia la contraseña generada y úsala donde necesites.



### Paso 5: Integración con navegadores (opcional)

- Instala la extensión del navegador correspondiente - KeePassXC-Browser para Chrome, Firefox o Edge.
- Activa la integración desde KeePassXC:
  1. Ve a Herramientas > Configuración > Integración del Navegador.
  2. Sigue las instrucciones para enlazar KeePassXC con el navegador.
- Utiliza la extensión para autocompletar contraseñas en sitios web.



### Paso 6: Realizar Respaldo y Sincronización

- Respaldo Manual:
  1. Copia el archivo .kdbx en una unidad externa o en un servicio en la nube.
- Sincronización:
  1. Usa servicios como Nextcloud, Google Drive o Dropbox para sincronizar tu archivo en múltiples dispositivos.
  2. Recuerda usar cifrado adicional si lo almacenas en la nube. Así tus contraseñas estarán completamente seguras.

### Recomendaciones

- **Bloquea** KeePassXC si te alejas del dispositivo (icono de candado).
- **No guardes** la contraseña maestra en dispositivos inseguros.

¡Ahora estás listx para gestionar tus contraseñas de manera eficiente y segura!