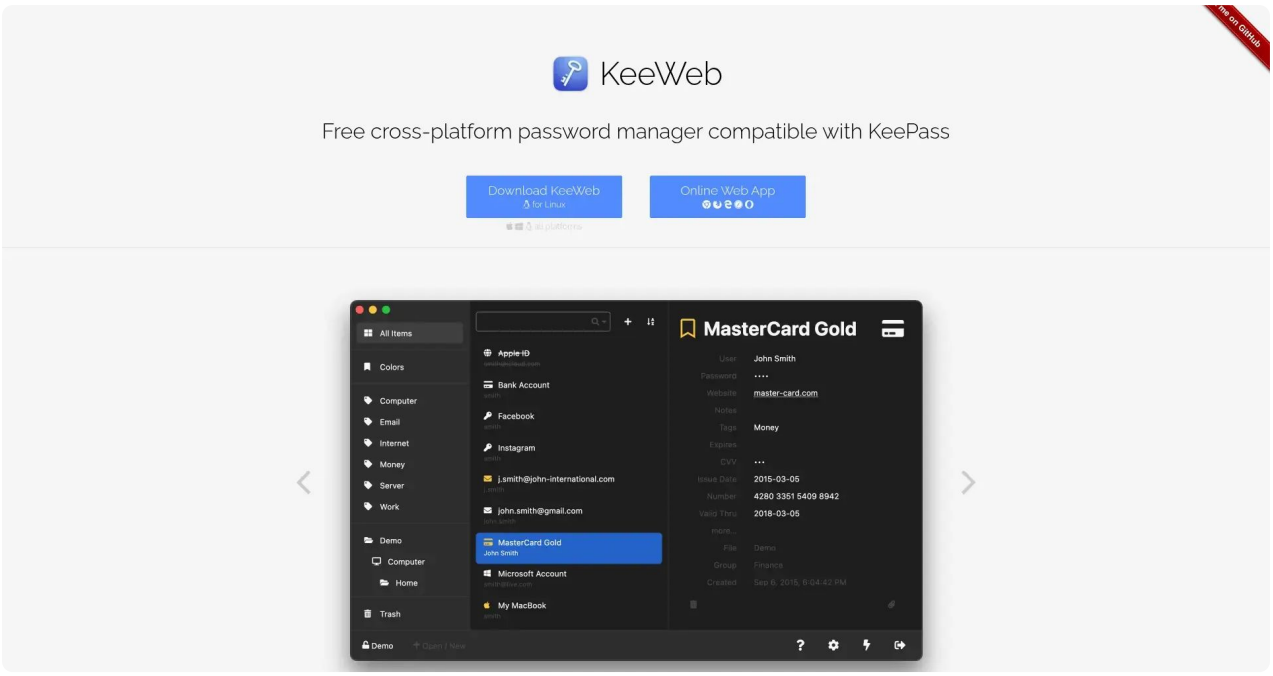

KeeWeb

KeeWeb es un gestor de contraseñas multiplataforma de código abierto diseñado para profesionales de IT, administradores de sistemas y perfiles técnicos que requieren soberanía total sobre sus credenciales. Permite gestionar bases de datos en formato KeePass (KDBX) desde el navegador, escritorio o servidor propio sin depender de nubes propietarias. Es la solución ideal para departamentos de ciberseguridad que buscan una herramienta gratuita, segura y compatible con estándares industriales.

Visitar Sitio Oficial Preguntar a ChatGPT Preguntar a Claude Preguntar a Grok

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
KeeWeb es un gestor de contraseñas multiplataforma de código abierto compatible con el formato de base de datos KeePass (KDBX). Está diseñado para profesionales que buscan una solución de gestión de credenciales soberana, donde la base de datos permanece bajo control total del usuario sin depender de nubes propietarias. Es ideal para departamentos de IT, administradores de sistemas y perfiles técnicos en sectores con estrictos requisitos de privacidad y seguridad de datos.

Principal ventaja profesional
La soberanía total del dato combinada con la versatilidad de acceso: permite gestionar bases de datos KeePass desde un navegador web, aplicación de escritorio o servidor propio, manteniendo la compatibilidad con el ecosistema estándar de archivos .kdbx sin costes de licencia.

Para quién no es
No es una herramienta para usuarios domésticos que busquen una experiencia automatizada "estilo SaaS" (como Dashlane o LastPass) o empresas que no tengan capacidad para gestionar sus propios archivos de backup. Profesionales que requieran sincronización nativa integrada sin configurar servicios externos (WebDAV, Dropbox, etc.) pueden encontrarla compleja.

funcionalidades clave
- Compatibilidad nativa con archivos KDBX (KeePass v2.x).
- Cifrado seguro del lado del cliente mediante Web Crypto API.
- Gestor de archivos integrado para múltiples fuentes de almacenamiento.
- Generador de contraseñas con reglas personalizables.
- Soporte para adjuntos, iconos personalizados y campos adicionales.
- Sincronización automática al detectar cambios en el archivo de origen.
- Soporte para temas (oscuro, claro) y visualización de entradas en modo tabla o lista.

Precios
- Gratuito y Open Source: La herramienta es totalmente gratuita bajo licencia MIT. No existen versiones premium, costes de suscripción o limitaciones funcionales.

Perfil del usuario
Empresas de ciberseguridad, consultorías tecnológicas, agencias de IT y departamentos de desarrollo que priorizan el almacenamiento local o privado.
- Administradores de sistemas y redes.
- Desarrolladores de software.
- Responsables de seguridad de la información (CISO).
- Consultores independientes que manejan múltiples entornos de clientes.

Nivel técnico requerido
- Nivel técnico para su uso: Medio. Requiere comprender el concepto de base de datos de contraseñas y gestión de archivos.
- Nivel técnico para instalación/configuración: Bajo para la versión web/escritorio; Medio-Alto si se desea auto-alojar en un servidor propio mediante Docker o despliegue manual.
- Conocimientos necesarios: Manejo de protocolos de red (si se usa WebDAV), gestión de archivos .kdbx y principios básicos de criptografía asimétrica.

Ejemplos de uso profesional
- Centralización de credenciales de servidores en un archivo compartido vía WebDAV para el equipo de infraestructura.
- Uso como herramienta portátil en entornos corporativos restringidos donde no se permite la instalación de software (vía versión web).
- Gestión de seeds de recuperación y claves API para equipos de desarrollo.

Uso y distribución
- Versión web: Acceso directo desde navegadores modernos.
- Versión escritorio: Aplicaciones nativas para Windows, macOS (Intel y Apple Silicon) y Linux (AppImage,

deb, rpm).
- Auto-alojamiento: Imagen de Docker disponible para despliegue en infraestructura interna.

Open source
KeeWeb es un proyecto de código abierto publicado bajo la licencia MIT, lo que permite su uso, modificación y distribución incluso en entornos comerciales sin restricciones.

Integraciones
- Facilidad de integración: No code para usuarios finales; Full code para despliegues personalizados.
- Almacenamiento en la nube: Integración nativa con Dropbox, Google Drive, OneDrive y cualquier servicio compatible con WebDAV (como Nextcloud o OwnCloud).
- Sincronización local: Capacidad para leer y escribir en el sistema de archivos local en las versiones de escritorio.

Notas finales
información legal, licencias, contratos
- Licencia: MIT. El software se proporciona "tal cual", sin garantías. La propiedad intelectual del código pertenece a los contribuyentes del proyecto. Al ser una herramienta cliente-side, el desarrollador no tiene acceso a las contraseñas ni a los archivos de los usuarios.

Otros
- Incluye soporte para plugins y traducciones comunitarias.
- Permite la visualización de archivos KDBX protegidos por llave de archivo (Key File) además de la contraseña maestra.

Para más información:
- Sitio web oficial: https://keeweb.info
- Repositorio en Github: https://github.com/keeweb/keeweb
- Enlace al despliegue web oficial: https://app.keeweb.info
- Wiki y documentación: https://github.com/keeweb/keeweb/wiki
- Twitter (X): https://x.com/keeweb_official

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
KeeWeb se dirige a empresas de servicios IT, departamentos de ciberseguridad y consultorías que requieren un control absoluto sobre su bóveda de contraseñas. Al ser compatible con el estándar KeePass (.kdbx), es ideal para infraestructuras que prohíben el uso de nubes propietarias. El presupuesto de adquisición es nulo al ser Open Source (licencia MIT), centrando el coste exclusivamente en la infraestructura de almacenamiento (servidores propios, Nextcloud o WebDAV) y tiempo de configuración. Puntos clave son su seguridad cliente-side (el cifrado ocurre en el dispositivo del usuario) y su versatilidad para usarse como aplicación portable sin instalación.

Madurez digital requerida
- Usuarios: Es necesario que el personal tenga conocimientos sobre la gestión de archivos de bases de datos y la importancia de la custodia de la clave maestra y el "Key File". No es apto para perfiles con baja autonomía técnica.
- Empresa: La organización debe contar con políticas claras de backup de datos, ya que al no ser un servicio SaaS, la pérdida del archivo .kdbx implica la pérdida total de las credenciales si no existen copias de seguridad.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- Tiempos de despliegue: Entre 1 y 3 días para una configuración corporativa estándar.
- Evaluación inicial: Definir el método de almacenamiento centralizado (WebDAV es la opción profesional preferida para equipos).
- Configuración y piloto: Despliegue de la versión web auto-alojada mediante Docker para garantizar que el acceso web sea privado. Configuración de plugins de navegador para la autocompletación.
- Capacitación: Instrucción en la generación de contraseñas seguras y la gestión de entradas compartidas.
- Seguimiento: Auditoría periódica de la integridad de los archivos de base de datos y revisión de logs de acceso en el servidor de almacenamiento.

Necesidades de formación del equipo
El equipo debe ser formado en el manejo del flujo de sincronización para evitar conflictos de escritura (merge de archivos) y en el uso de la autenticación de dos factores soportada por el estándar KeePass.

Perfiles necesarios
- Perfiles técnicos: Administrador de sistemas con conocimientos en Docker y protocolos de red (si se desea auto-alojar).
- Personal externo: Generalmente no es necesario, aunque un consultor en seguridad puede validar la robustez de la arquitectura de almacenamiento elegida.

Retorno de la inversión
- Tiempos: Reducción drástica del tiempo de acceso a credenciales en equipos técnicos frente a métodos manuales o descentralizados.
- KPIs: Ahorro en costes de licencias SaaS (proyectado por usuario/año), reducción de incidencias relacionadas con pérdida de credenciales y cumplimiento de normativas de soberanía de datos (GDPR/Esquema Nacional de Seguridad).

Otros
- Seguridad adicional: KeeWeb soporta la integración con YubiKey y otros dispositivos hardware para el desbloqueo de la base de datos, lo que añade una capa de seguridad física crítica en entornos de alta sensibilidad.
- Offline-first: La herramienta funciona perfectamente sin conexión a internet, sincronizando los cambios una vez se recupera la conectividad con el servidor de archivos.

PREGUNTAS FRECUENTES

¿Qué es KeeWeb y qué relación tiene con KeePass?

KeeWeb es un gestor de contraseñas de código abierto compatible con el formato de base de datos KeePass (.kdbx). Actúa como una interfaz moderna y multiplataforma que permite abrir y editar archivos creados originalmente en KeePass sin necesidad de migraciones de datos, manteniendo la total soberanía sobre el archivo de credenciales.

¿Es una tecnología segura para uso profesional?

Sí, utiliza estándares de cifrado de grado militar como AES-256 e implementa Argon2id para la derivación de claves, lo que ofrece alta resistencia ante ataques de fuerza bruta. El cifrado se realiza estrictamente en el lado del cliente (Navegador o App de escritorio), asegurando que ninguna clave maestra o dato en claro sea transmitido por la red.

¿Ha pasado auditorías de seguridad externas?

KeeWeb fue objeto de una auditoría de seguridad y pruebas de penetración (pentesting) por parte de la firma especializada Hackmanit en 2020. Las vulnerabilidades identificadas en aquel momento fueron corregidas. Al ser open source bajo licencia MIT, su código es auditable de forma pública y continua por la comunidad en GitHub.

¿Tiene versión gratuita o requiere suscripción?

Es una herramienta completamente gratuita y sin modelo de suscripción. Al ser software libre distribuido bajo la licencia MIT, no existen limitaciones funcionales ni costes por número de dispositivos o usuarios. El proyecto se mantiene mediante contribuciones comunitarias y donaciones.

¿Es posible descargarlo de GitHub o usarlo offline?

Sí, el código fuente está disponible en GitHub bajo el repositorio de KeeWeb. Se puede descargar la versión de escritorio para uso offline o incluso alojar una instancia propia utilizando la imagen oficial de Docker, lo que garantiza el acceso a las contraseñas sin dependencia de servidores externos.

¿Cómo cumple con la normativa de privacidad y protección de datos?

Al ser una aplicación cliente-side donde el usuario gestiona su propio archivo .kdbx, KeeWeb no recopila, almacena ni procesa datos personales en servidores de terceros. Esto facilita el cumplimiento de normativas como el RGPD, ya que el control y la responsabilidad sobre la ubicación del dato recaen íntegramente en la organización o profesional que lo utiliza.

¿Qué opciones de sincronización ofrece para equipos de IT?

Admite sincronización con servicios de almacenamiento en la nube populares (Dropbox, Google Drive, OneDrive) y protocolos profesionales como WebDAV. Esto permite a departamentos de IT centralizar archivos de credenciales compartidos en servidores propios como Nextcloud u OwnCloud de forma segura.

¿Qué nivel de mantenimiento tiene el proyecto actualmente?

Aunque el proyecto ha pasado por periodos de menor actividad en el repositorio principal, mantiene una comunidad activa y ha incorporado nuevos mantenedores recientemente para actualizar dependencias críticas y corregir fallos. Para entornos que requieran actualizaciones constantes, se recomienda el uso de la versión de escritorio o el auto-alojamiento para controlar el ciclo de vida del software.

¿Es compatible con hardware de seguridad como YubiKey?

Sí, KeeWeb soporta el uso de archivos de llave (Key Files) y es compatible con dispositivos YubiKey para añadir una capa de autenticación de segundo factor (2FA) a nivel de apertura de base de datos, reforzando la protección del archivo contra robos de identidad.

CONTRATOS Y CONDICIONES

Princiaples recomendaciones
- Al ser una herramienta de "lado del cliente" (client-side), la empresa es la única responsable de la custodia, integridad y copia de seguridad de la base de datos (archivo .kdbx).
- Si se utiliza la versión web oficial (app.keeweb.info), es fundamental verificar que la conexión sea HTTPS para evitar la interceptación de datos durante la carga de la aplicación en el navegador.
- Para un entorno profesional con políticas de seguridad estrictas, se recomienda el auto-alojamiento (self-hosting) mediante Docker en servidores propios para evitar la dependencia de dominios externos.
- Es necesario establecer una política corporativa sobre el uso de servicios de terceros (Dropbox, Google Drive, OneDrive) para la sincronización, ya que estos servicios sí podrían estar sujetos a transferencias internacionales de datos.
- Se debe auditar el uso de plugins de terceros, ya que al ser código abierto, la integración de complementos no oficiales puede comprometer la seguridad de la bóveda de contraseñas.

Privacidad y protección de datos
- Responsabilidades: La empresa actúa como Responsable del Tratamiento. KeeWeb no actúa como Encargado del Tratamiento porque no tiene acceso a los datos; es una herramienta técnica que procesa la información localmente en el dispositivo del usuario.
- Ubicación de los datos: Los datos no se almacenan en los servidores de KeeWeb. Residen donde el usuario decida (disco duro local, servidor corporativo WebDAV o nubes comerciales).
- Transferencia internacional: No existe transferencia de datos por parte de la herramienta. Sin embargo, si el usuario configura la sincronización con proveedores de EE.UU. (Google, Microsoft, Dropbox), la empresa debe asegurar que exista un Marco de Privacidad de Datos (Data Privacy Framework) o Cláusulas Contractuales Tipo.
- Derechos ARCO: La empresa debe gestionar los derechos de acceso o supresión internamente, ya que el desarrollador de KeeWeb no posee las llaves ni los datos para dar cumplimiento a estas peticiones.

Propiedad intelectual
- Propiedad de datos: Los datos y contraseñas pertenecen exclusivamente a la empresa usuaria.
- Propiedad del resultado/procesamiento: El software se distribuye bajo Licencia MIT, lo que permite a la empresa española modificar el código, integrarlo en herramientas internas y usarlo comercialmente sin pagar cánones.
- El copyright del código fuente pertenece a los colaboradores del proyecto, pero se otorga permiso perpetuo de uso sin restricciones.

Usos y prohibiciones
- Usos admitidos: Uso comercial, modificación del código fuente, redistribución y despliegue en entornos privados de servidor.
- Usos prohibidos: No se permite el uso de la marca o logotipos de KeeWeb de forma que sugiera un respaldo oficial del proyecto a un producto derivado. La licencia MIT excluye explícitamente cualquier garantía por parte de los autores.

Seguridad y certificaciones
- Seguridad: Utiliza Web Crypto API para el cifrado y descifrado. No se envían las contraseñas maestros ni el contenido de la base de datos a ningún servidor externo durante el procesamiento normal.
- Certificaciones: Al ser un proyecto comunitario de código abierto, no cuenta con certificaciones ISO 27001 o SOC2 de serie, pero su arquitectura permite que la infraestructura donde se aloje cumpla con dichas normativas mediante auditorías internas.

Otros
- Impacto legal: Bajo. Al ser una herramienta de gestión local y open source, el riesgo de incumplimiento por parte del proveedor es inexistente, trasladándose la responsabilidad totalmente a la gestión técnica de la empresa.
- Cumplimiento RGPD: Al no haber recogida de datos personales por parte de la web de la herramienta (en su funcionamiento estándar de gestión de archivos locales), facilita el cumplimiento del principio de "Privacidad por Defecto y desde el Diseño".

Fuentes consultada:

- Contratos: https://github.com/keeweb/keeweb/blob/master/LICENSE
- Condiciones: https://github.com/keeweb/keeweb/wiki/Security
- Licencias: https://opensource.org/license/mit
- Repositorio oficial: https://github.com/keeweb/keeweb

Para más información y herramientas:

Explora look4.tools para descubrir las mejores soluciones tecnológicas del mercado.

Inicio Todas las herramientas Categorías