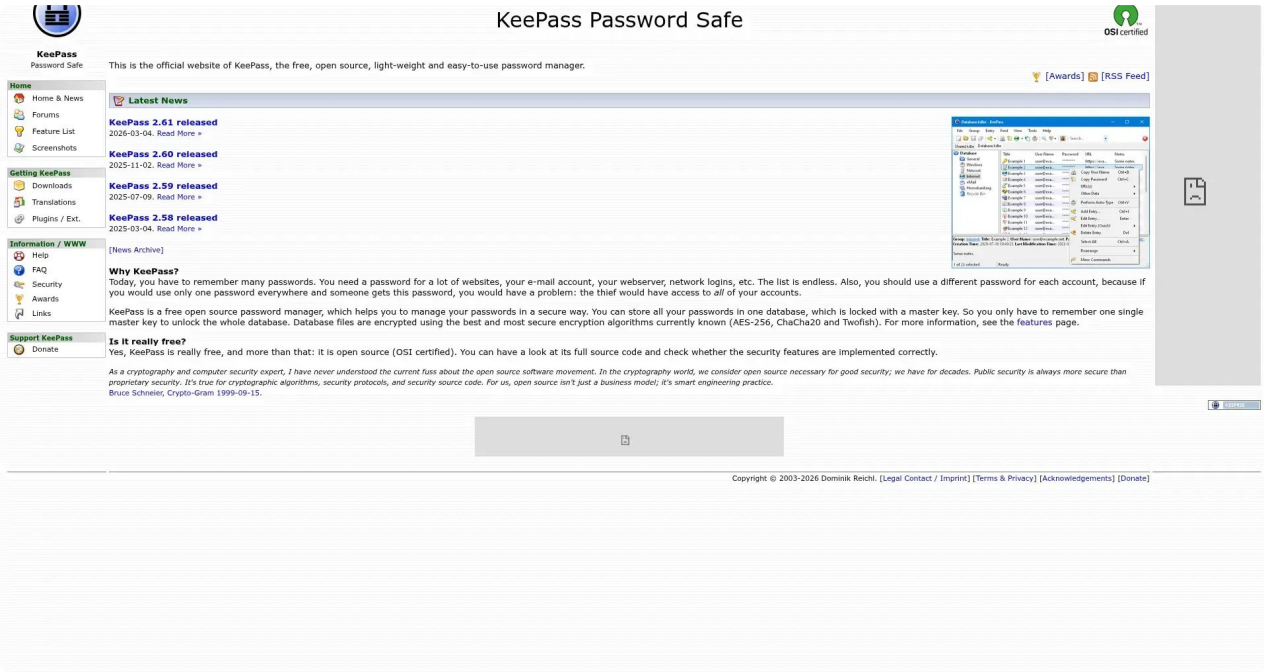

KeePass

KeePass es un gestor de contraseñas de código abierto diseñado para administradores de sistemas, departamentos de IT y perfiles técnicos que requieren soberanía total sobre sus datos. Permite almacenar credenciales en una base de datos local cifrada con AES-256, eliminando la dependencia de la nube. Es ideal para sectores críticos como banca o defensa, ofreciendo funciones avanzadas como Auto-Type, gestión de archivos adjuntos y una arquitectura extensible mediante plugins comunitarios.

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

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
KeePass es un gestor de contraseñas de escritorio, gratuito y de código abierto (Open Source), diseñado para almacenar y gestionar credenciales en una base de datos local cifrada. A diferencia de las soluciones basadas en la nube, KeePass otorga al usuario el control absoluto sobre la ubicación y seguridad de sus datos. En el ámbito profesional, es la herramienta de referencia para administradores de sistemas, departamentos de IT y perfiles técnicos en sectores con altas exigencias de cumplimiento y soberanía del dato (banca, industria, defensa) que buscan evitar la dependencia de proveedores externos (SaaS).

Principal ventaja profesional
Máxima seguridad y control de la infraestructura: al ser una aplicación local sin almacenamiento en la nube predeterminado, elimina el riesgo de brechas de seguridad masivas en servidores de terceros y permite su uso en entornos aislados o redes corporativas restringidas.

Para quién no es
No es adecuado para usuarios o empresas que buscan una experiencia de uso "llave en mano" con sincronización nativa automática entre dispositivos sin configuración previa. Profesionales de departamentos de marketing, ventas o perfiles no técnicos pueden percibir su interfaz como anticuada o compleja de configurar para el uso compartido en equipo.

Funcionalidades clave
- Cifrado robusto: Utiliza AES-256, ChaCha20 y Twofish para proteger la base de datos completa (no solo las contraseñas).
- Auto-Type: Simulación de pulsaciones de teclas para completar formularios y registros de forma automática en cualquier aplicación o sitio web.
- Gestión de archivos adjuntos: Permite almacenar documentos, certificados o claves PGP directamente dentro de la base de datos cifrada.
- Generador de contraseñas: Herramienta avanzada para crear claves aleatorias basadas en reglas personalizables (longitud, caracteres especiales, exclusión de caracteres similares).
- Arquitectura de plugins: Capacidad de extender sus funciones mediante complementos de la comunidad para añadir sincronización en la nube, integración con navegadores o soporte para nuevos formatos.
- Protección de memoria: Cifra las contraseñas mientras la aplicación está en ejecución para evitar que sean extraídas mediante volcados de memoria del sistema operativo.

Precios
KeePass es un software totalmente gratuito bajo licencia de código abierto.
- Versión gratuita: El software es Open Source (GPLv2), completo y sin limitaciones de tiempo ni funcionalidades.
- Rango de precios: 0€ (Sin planes de suscripción ni costes de licencia).

Perfil del usuario
- Empresas que operan en sectores críticos con políticas de seguridad que prohíben el uso de gestores de contraseñas en la nube.
- Departamentos de IT, seguridad informática y desarrollo de software.
- Administradores de sistemas (SysAdmins) que necesitan gestionar credenciales de servidores y servicios de red de forma local.

Nivel técnico requerido
- Nivel técnico requerido para su uso: Medio. Los usuarios deben entender el concepto de base de datos local y gestión de clave maestra/archivo de llaves.
- Nivel técnico requerido para su instalación/configuración: Medio-Alto. La sincronización entre dispositivos o la integración con navegadores suele requerir la instalación manual de plugins o la configuración de repositorios compartidos (SMB, WebDAV, etc.).
- Conocimientos necesarios: Manejo de directorios de archivos, conceptos básicos de criptografía y familiaridad con el uso de extensiones de software.

Ejemplos de uso profesional
- Gestión centralizada de credenciales de administrador en un equipo de sistemas mediante el uso de un

archivo de base de datos compartido en un servidor local.
- Almacenamiento seguro de licencias de software corporativo y certificados digitales adjuntos a las entradas correspondientes.
- Automatización del login en aplicaciones de escritorio corporativas que no soportan gestores de contraseñas estándar mediante la función Auto-Type.

Uso y distribución
- Versión escritorio: Windows (nativo), Linux y macOS (mediante Mono o puertos específicos).
- Versión móvil: Disponible a través de puertos de la comunidad (KeePass2Android, KeePassium, Strongbox, etc.).
- Versión web: Disponible mediante proyectos de terceros como KeeWeb.
- CLI: Disponible mediante herramientas de línea de comandos como KPCLI.

Open source
KeePass es software libre certificado por la OSI, distribuido bajo la Licencia Pública General de GNU (GPL) versión 2 o posterior. El código fuente es auditable por cualquier organización.

Integraciones
- Facilidad de integración: Requiere conocimientos técnicos para su implementación mediante plugins (Full Code).
- API propia: No dispone de API nativa tipo REST, pero su arquitectura basada en archivos .kdbx permite que otras aplicaciones interactúen con los datos.
- Descripción: Existen más de 100 plugins desarrollados por la comunidad que permiten integraciones con navegadores (Chrome, Firefox, Edge), servicios de almacenamiento (Google Drive, Dropbox, OneDrive) y protocolos de red (SSH, FTP).

Notas finales
información legal, licencias, contratos
El software se entrega "tal cual", sin garantías expresas. Al ser GPLv2, la propiedad intelectual pertenece a Dominik Reichl y otros contribuyentes, permitiendo su uso comercial, modificación y redistribución siempre que se mantenga la misma licencia y se proporcione el código fuente.

Otros
Es altamente recomendable realizar copias de seguridad periódicas del archivo de la base de datos (.kdbx). Si se pierde la clave maestra o el archivo de llaves (Key File), no existe posibilidad de recuperación de los datos por parte de terceros.

Para más información:
- Sitio web oficial: https://keepass.info
- Precios y donaciones: https://keepass.info/donate.html
- Licencias y contratos: https://keepass.info/help/v2/license.html
- Repositorio de plugins: https://keepass.info/plugins.html
- Foros de soporte: https://sourceforge.net/p/keepass/discussion/

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
KeePass es ideal para corporaciones con normativas estrictas de soberanía del dato y seguridad (infraestructuras críticas, sectores legales o gubernamentales) que requieren evitar el almacenamiento de credenciales en servidores de terceros. Es especialmente útil en equipos técnicos donde el control del archivo de base de datos (.kdbx) se integra en flujos de trabajo locales o mediante redes internas. El presupuesto es nulo en licencias, permitiendo una escalabilidad teórica ilimitada sin costes por usuario, aunque requiere inversión en tiempo de configuración inicial y mantenimiento.

Madurez digital requerida
- Los usuarios deben poseer competencias digitales intermedias, especialmente en la gestión de archivos, comprensión de rutas de red y manejo de políticas de contraseñas robustas.
- La organización debe tener una cultura de seguridad establecida, con procedimientos claros para el respaldo de datos y gestión de acceso físico o lógico a los sistemas de almacenamiento.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- Tiempos estimados de despliegue: De 1 a 3 semanas dependiendo del volumen de usuarios y la complejidad de la infraestructura de red existente.
- Evaluación inicial: Auditoría de las credenciales actuales del equipo técnico y definición de la arquitectura de almacenamiento (local individual o compartido vía red interna).
- Configuración y diseño: Selección de los algoritmos de cifrado y derivación de claves apropiados (AES-256 / Argon2). Definición del método de acceso: clave maestra única, archivo de llaves (Key File) o combinación de ambos.
- Piloto: Implementación en el departamento de IT para testar la sincronización mediante protocolos internos (SMB/WebDAV) o almacenamiento seguro en servidores locales.
- Despliegue: Instalación masiva mediante scripts de despliegue o imágenes de sistema.
- Seguimiento y Backup: Establecimiento de tareas automáticas de respaldo para el archivo .kdbx a una ubicación segura fuera de línea.

Necesidades de formación del equipo
Es imprescindible formar a la plantilla en la importancia del resguardo de la Clave Maestra y el Archivo de Llaves, ya que su pérdida implica la pérdida total e irrecuperable de los datos. Se requiere capacitación en el uso de la función Auto-Type y en la gestión segura de archivos adjuntos dentro de la herramienta.

Perfiles necesarios
- Perfiles técnicos: Administrador de sistemas para la configuración de la seguridad de red y despliegue de la aplicación.
- Personal externo: No suele ser necesario, salvo consultoría puntual de ciberseguridad para auditoría de políticas de acceso.
- Otros: Responsable de Seguridad de la Información (CISO) para de definir las políticas de rotación de claves maestras.

Retorno de la inversión
- El retorno de la inversión se observa de forma inmediata en el ahorro de costes de licencias recurrentes (SaaS) que suelen oscilar entre 3€ y 8€ por usuario/mes.
- Mitigación de riesgos económicos derivados de una brecha en la nube de un proveedor externo.
- KPIs para medir éxito: Tiempo medio de acceso a credenciales, reducción de solicitudes de recuperación de contraseñas al equipo de soporte y cumplimiento de auditorías de seguridad interna.

Otros
Es fundamental destacar que al ser una herramienta de código abierto, la auditoría del código fuente es posible, lo que garantiza la ausencia de puertas traseras. Se recomienda el uso de plugins específicos como KeePassRPC para mejorar la integración con navegadores de forma segura si la empresa así lo requiere.

PREGUNTAS FRECUENTES

¿Qué es KeePass y cuál es su principal diferencia con otros gestores de contraseñas?

KeePass es un gestor de contraseñas de escritorio, gratuito y de código abierto (Open Source). Su principal diferencia radica en que es una solución local; a diferencia de los servicios basados en la nube (SaaS), los datos no se almacenan en servidores de terceros, sino en una base de datos cifrada bajo el control directo del usuario.

¿Qué coste tiene KeePass para un entorno profesional?

KeePass es totalmente gratuito y no tiene planes de suscripción. Se distribuye bajo la licencia GNU GPLv2, lo que permite su uso en entornos corporativos, comerciales y profesionales sin coste alguno por licencia.

¿Es KeePass una tecnología segura y auditable?

Sí. Al ser software de código abierto certificado por la OSI, el código fuente es público y puede ser auditado de forma independiente para verificar que no cumple con puertas traseras. Utiliza algoritmos de cifrado robustos como AES-256, ChaCha20 y Twofish, además de proteger la memoria RAM para evitar que las claves sean extraídas durante la ejecución.

¿Cumple con la normativa de soberanía del dato y privacidad?

KeePass es una de las herramientas de referencia para sectores con altas exigencias de cumplimiento (banca, defensa, industria) porque garantiza la soberanía total del dato. Al no existir una infraestructura centralizada ni transmisión automática a la nube, el profesional tiene el control absoluto sobre dónde reside la información y quién accede a ella.

¿Es posible sincronizar contraseñas entre varios dispositivos?

KeePass no ofrece sincronización nativa automática. Sin embargo, esto es posible mediante la instalación de plugins desarrollados por la comunidad o mediante el uso de protocolos de red (SMB, WebDAV) y servicios de almacenamiento en la nube, requiriendo una configuración manual por parte del usuario.

¿Se puede integrar KeePass con navegadores web como Chrome o Firefox?

La integración no es nativa tras la instalación básica, pero es posible mediante la arquitectura de plugins. El usuario debe instalar complementos específicos (como KeePassRPC o extensiones de la comunidad) para habilitar el autocompletado en navegadores.

¿Qué sucede si olvido la clave maestra o pierdo el archivo de llaves?

Debido a su diseño de seguridad de conocimiento cero y enfoque local, no existe un mecanismo de recuperación de cuentas ni soporte técnico que pueda restablecer el acceso. Si se pierde la clave maestra o el archivo de llaves (Key File), el acceso a la base de datos se pierde de forma permanente.

¿Es compatible con sistemas operativos móviles?

Aunque no existe una versión móvil oficial desarrollada por el autor original, el formato de archivo .kdbx es un estándar abierto que permite el uso de aplicaciones compatibles desarrolladas por terceros, como KeePass2Android para Android o KeePassium y Strongbox para iOS.

¿Qué nivel de conocimientos técnicos se requiere para su implementación corporativa?

Se requiere un nivel técnico medio-alto. Mientras que el uso básico es accesible, la configuración de bases de datos compartidas en red, la gestión de certificados adjuntos o la automatización mediante Auto-Type requiere que el personal de IT esté familiarizado con la gestión de directorios, permisos de red y administración de plugins.

¿Está disponible el código fuente en plataformas como GitHub?

KeePass mantiene su desarrollo principal y repositorio en SourceForge, aunque existen numerosos espejos y proyectos derivados (forks) en GitHub que facilitan el acceso al código para auditorías y contribuciones de la comunidad.

CONTRATOS Y CONDICIONES

Principales recomendaciones
- **Soberanía digital**: Al ser una herramienta local (on-premise), la empresa es la única responsable de la custodia del archivo de base de datos (.kdbx). Se recomienda establecer políticas estrictas de copias de seguridad cifradas.
- **Gestión de Plugins**: Muchos plugins son desarrollados por terceros. En entornos corporativos, conviene auditar o limitar el uso de extensiones para evitar fugas de datos hacia servicios en la nube no autorizados.
- **Diferenciación de versiones**: Aunque KeePass (original) y KeePassXC (comunidad) comparten formato, para entornos profesionales modernos se suele recomendar KeePassXC por su soporte nativo multiplataforma y una base de código más actualizada.
- **Doble Factor**: Implementar el uso de archivos de llave ("Key Files") adicionales a la contraseña maestra, almacenados en dispositivos físicos separados (pendrives o tokens hardware) para elevar el nivel de cumplimiento ante auditorías.

Ley de Inteligencia Artificial (AI Act)
- **Impacto Nulo/Bajo**: KeePass no es un sistema de IA ni utiliza algoritmos de aprendizaje automático para su funcionamiento principal.
- **Transparencia en el desarrollo**: Sus mantenedores (en especial el equipo de la rama KeePassXC) han declarado públicamente un control estricto sobre el uso de IA generativa en la escritura de su código, asegurando que ninguna función del software depende de IA, manteniendo la predictibilidad y seguridad del cifrado.

Privacidad y protección de datos
- **Responsabilidades**: La empresa usuaria actúa como Responsable del Tratamiento. KeePass, al no ser un servicio SaaS, no actúa como Encargado del Tratamiento ya que no tiene acceso a los datos.
- **Ubicación de los datos**: Local. El usuario decide si permanecen en el equipo, en un servidor de archivos interno (SMB/NFS) o en una nube privada (Nextcloud).
- **Transferencia internacional**: No existen transferencias internacionales de datos por defecto, lo que facilita el cumplimiento del RGPD en comparación con soluciones cloud estadounidenses.
- **Derechos ARCO**: Es responsabilidad de la empresa garantizar que la información personal almacenada en las bases de datos de KeePass sea accesible, rectificable o suprimible por los empleados según la normativa vigente.

Propiedad intelectual
- **Propiedad de los datos**: Todos los datos y secretos almacenados pertenecen exclusivamente a la empresa licenciataria.
- **Propiedad del software**: El código fuente es propiedad de sus respectivos autores bajo licencia GNU GPLv2. Esto permite a la empresa modificar el software para adaptarlo a sus necesidades de seguridad, siempre que se respeten los términos de la licencia de código abierto.

Usos y prohibiciones
- **Usos admitidos**: Uso profesional en cualquier sector, incluido el gubernamental (está recomendado oficialmente por agencias de ciberseguridad europeas).
- **Prohibiciones**: No existen restricciones de uso comercial, pero la licencia GPL impide cerrar el código si se redistribuye una versión modificada del software.

Seguridad y certificaciones
- **Seguridad**: Utiliza cifrado de nivel militar (AES-256, ChaCha20). Incluye protección contra volcados de memoria para evitar que las claves sean leídas mientras la aplicación está abierta.
- **Certificaciones**:
- **ANSSI (Francia)**: Ha recibido la certificación CSPN (Certification de Sécurité de Premier Niveau), reconocida internacionalmente.
- **BSI (Alemania)**: Recomendado por la Oficina Federal de Seguridad de la Información alemana.
- **UE**: Auditado bajo el programa EU-FOSSA de la Comisión Europea.

Otros
- **Interoperabilidad**: El formato .kdbx es un estándar de facto que garantiza que la empresa no sufra "vendor lock-in" (secuestro por proveedor); los datos (contraseñas/documentos) podrán exportarse o abrirse con otras

herramientas compatibles en el futuro.

Fuentes consultada:
- Condiciones y Licencia GPL
- Certificación de seguridad ANSSI
- Auditorías y certificaciones KeePassXC
- Política de calidad y control de código (IA)

Para más información y herramientas:

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

Inicio Todas las herramientas Categorías