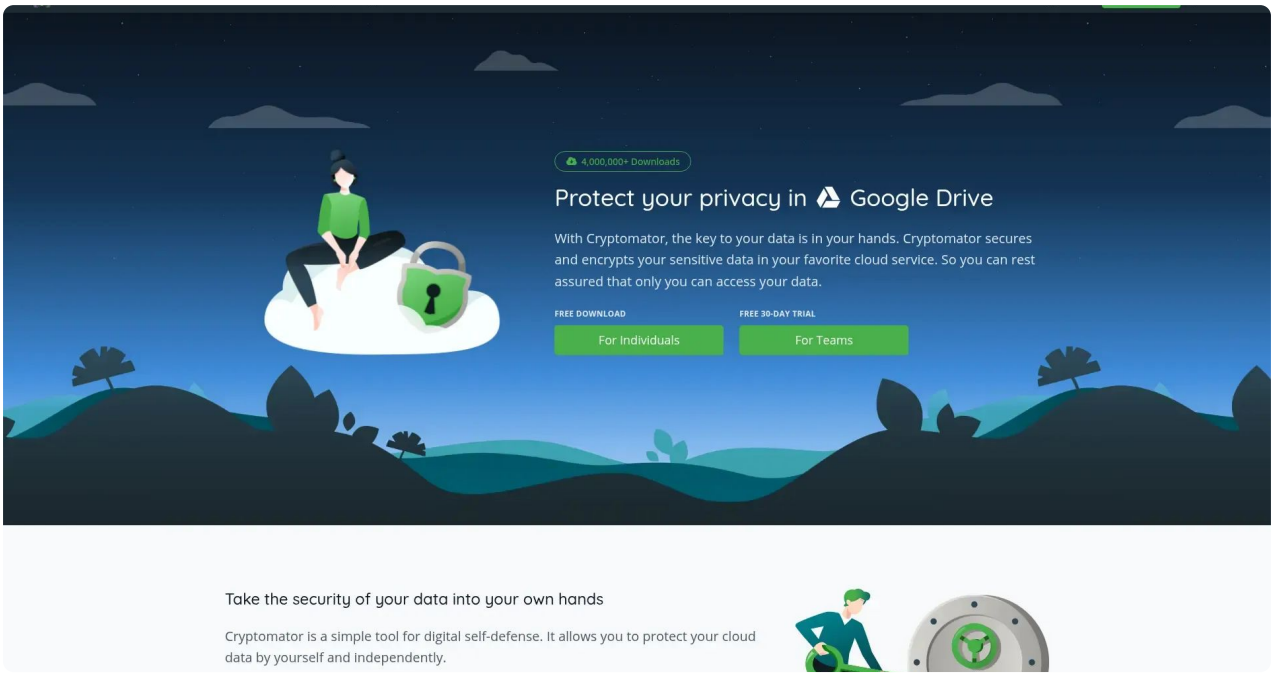

Cryptomator

Herramienta de cifrado de código abierto diseñada para profesionales y empresas que necesitan proteger archivos confidenciales en nubes como Google Drive o Dropbox. Utiliza arquitectura Zero Knowledge para garantizar que solo el usuario acceda a sus datos, cifrando nombres y contenido de archivos individualmente antes de la sincronización. Es ideal para sectores legales, sanitarios y financieros que deben cumplir con el RGPD mientras utilizan servicios de almacenamiento público de forma segura.

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

Contenido del Dossier

INFORMACIÓN DE LA HERRAMIENTA

Qué y para quién es
Cryptomator es una herramienta de cifrado de archivos de código abierto diseñada específicamente para proteger los datos almacenados en servicios de almacenamiento en la nube. A diferencia de las soluciones de cifrado de disco completo, Cryptomator cifra los archivos de forma individual antes de que se sincronicen con proveedores como Google Drive, Dropbox o OneDrive. Está dirigido a profesionales y empresas que gestionan información confidencial, datos de clientes o propiedad intelectual y requieren una capa de seguridad adicional e independiente de las políticas de privacidad de los proveedores de hosting.

Principal ventaja profesional
La arquitectura de "conocimiento cero" (Zero Knowledge), que garantiza que ni el proveedor de almacenamiento ni los desarrolladores del software tengan acceso a las claves de cifrado o a los datos, permitiendo cumplir con normativas estrictas de protección de datos (RGPD) en entornos de nube pública.

Para quién no es
No es una herramienta adecuada para usuarios que buscan una solución de copia de seguridad integral del sistema operativo, ni para equipos que requieren edición colaborativa simultánea en tiempo real sobre archivos cifrados (como Google Docs), ya que el cifrado impide la indexación y manipulación directa por parte del servidor de la nube.

Funcionalidades clave
- Cifrado transparente: Los archivos se visualizan como una unidad virtual en el sistema, permitiendo trabajar con ellos como si estuvieran en un disco duro local.
- Estructura de archivos cifrada: Cifra tanto el contenido de los archivos como sus nombres y la estructura de las carpetas.
- Cifrado AES-256: Utiliza estándares de cifrado simétrico de alta seguridad.
- Independencia del proveedor: Funciona con cualquier servicio que sincronice carpetas locales o mediante protocolos como WebDAV.
- Sin registro en la nube: No requiere la creación de cuentas ni el almacenamiento de claves en servidores externos.

Precios
- Versión gratuita: La aplicación de escritorio para Windows, macOS y Linux es totalmente gratuita y de código abierto bajo licencia GPLv3.
- Rango de precios: Las aplicaciones móviles tienen un coste de pago único (aprox. 10€ - 15€) o funcionan bajo un modelo de donación/pago por uso en algunas funciones.
- Versiones de pago: Existe un Hub gestionado para empresas con funciones de administración de equipos y gestión de accesos, basado en un modelo de suscripción por usuario/mes.

Perfil del usuario
Empresas de sectores legales, sanitarios, consultoría financiera y departamentos de recursos humanos o I+D que manejan archivos sensibles.
- Responsables de cumplimiento (Compliance Officers).
- Administradores de sistemas y seguridad IT.
- Consultores independientes y perfiles técnicos.
- Abogados y gestores que almacenan documentación de terceros en nubes públicas.

Nivel técnico requerido
- Nivel técnico para su uso: Bajo. Se maneja como una unidad de disco adicional.
- Nivel técnico para instalación/configuración: Medio. Requiere crear una "bóveda" y definir su ubicación en la carpeta de sincronización de la nube.
- Conocimientos necesarios: Comprensión básica de la gestión de archivos y la importancia de la custodia de la contraseña maestra (no recuperable).

Ejemplos de uso profesional
- Almacenamiento de contratos y nóminas en Dropbox garantizando que los empleados de Dropbox no puedan acceder a la información.
- Archivo de historiales clínicos en Google Drive cumpliendo con estándares de privacidad técnica.

- Protección de copias de seguridad de bases de datos o secretos industriales antes de subirlos a servidores remotos.

Uso y distribución
- Versión web: No disponible por diseño de seguridad (el descifrado es siempre local).
- Versión escritorio: Windows, macOS (incluyendo soporte para procesadores Apple Silicon) y distribuciones Linux (AppImage, PPA, Flatpak).
- Versión móvil: Android e iOS.
- CLI: Interfaz de línea de comandos disponible para automatización y usuarios avanzados.

Open source
El software es de código abierto, lo que permite auditorías independientes del código. El núcleo de cifrado es público y está disponible en repositorios de GitHub.

Integraciones
- Facilidad de integración: No code. Se integra a nivel de sistema de archivos.
- Servidor MCP: No aplica directamente, pero soporta montado de unidades mediante WebDAV, FUSE y WinFp.
- Integraciones nativas: Integración directa con las aplicaciones de "Archivos" en iOS y proveedores de documentos en Android.

Notas finales
Información legal, licencias, contratos
La versión de escritorio se distribuye bajo la licencia GNU General Public License v3.0. Esto implica que el usuario tiene libertad de uso y modificación. Para el uso corporativo con gestión centralizada de llaves, se aplica el contrato de servicio de Cryptomator Hub.
Otros
Es importante destacar que si se pierde la contraseña maestra y no se dispone de la clave de recuperación generada durante la creación de la bóveda, los datos son técnicamente imposibles de recuperar.

Para más información:
- https://cryptomator.org
- https://cryptomator.org/pricing
- https://github.com/cryptomator/cryptomator
- https://twitter.com/cryptomator
- https://discord.gg/cryptomator

CONSEJOS DE IMPLANTACIÓN

Aplicación profesional
- Cryptomator es ideal para pequeñas y medianas empresas (PYMES), autónomos del sector legal y financiero, y departamentos de I+D que utilizan nubes públicas pero manejan datos sensibles.
- Presupuesto: Bajo para uso individual (gratuito en escritorio) y escalable mediante Cryptomator Hub para gestión de equipos.
- Puntos clave: Garantiza el cumplimiento del RGPD al usar nubes de proveedores estadounidenses, ya que el cifrado en origen impide el acceso de terceros a los datos.

Madurez digital requerida
- Usuarios: Familiaridad básica con el explorador de archivos y conceptos de unidades virtuales. Es crítico el entendimiento de que no existe la función "recuperar contraseña" mediante email.
- Empresa: Debe tener implementada una política de uso de almacenamiento en la nube (OneDrive, Google Drive, Dropbox) y protocolos de custodia de claves de recuperación.

Plan orientativo de implantación
Pasos necesarios y estimaciones
- Tiempos: La instalación técnica toma menos de 30 minutos por puesto. El despliegue organizacional puede durar de 1 a 2 semanas según el volumen de datos a migrar.
- Evaluación inicial: Identificar qué carpetas de la nube contienen PII (Información Personal Identificable) o propiedad intelectual para priorizar su cifrado.
- Prueba de concepto: Crear una bóveda de prueba en un equipo para verificar la velocidad de sincronización y la compatibilidad con el software ofimático local.
- Configuración: Instalación del software, creación de bóvedas y, sobre todo, generación y almacenamiento seguro de las claves de recuperación (recovery keys) fuera de la propia nube.
- Seguimiento: Verificación de que los archivos se cierran y bloquean correctamente al finalizar la jornada para asegurar el cifrado.

Necesidades de formación del equipo
- Diferenciación entre el archivos cifrado (en la carpeta de la nube) y la unidad virtual (donde se trabaja).
- Protocolos de seguridad para la gestión de la contraseña maestra.
- Limitaciones con el trabajo colaborativo: formación sobre por qué no pueden editar un archivo simultáneamente en la web de Google Drive si está cifrado.

Perfiles necesarios
- Perfiles técnicos: Administrador de sistemas para la instalación masiva o configuración de Cryptomator Hub si se requiere gestión centralizada.
- Personal externo: Consultor de ciberseguridad o DPO (Delegado de Protección de Datos) para validar el cumplimiento normativo.
- Otros: Responsable de seguridad de la información para la custodia de las llaves de emergencia.

Retorno de la inversión
- Tiempos: Reducción de riesgos legales y multas por brechas de datos en la nube.
- KPIs: Porcentaje de documentos sensibles cifrados vs. total de documentos en la nube, número de incidencias de acceso no autorizado resueltas por el cifrado.

Otros
- Rendimiento: Al trabajar con archivos individuales, solo se resincronizan los archivos modificados, lo que ahorra ancho de banda comparado con el cifrado de contenedores rígidos (como VeraCrypt).
- Limitación técnica: El cifrado oculta nombres de archivos y estructura, lo que puede dificultar la búsqueda de archivos desde la interfaz web del proveedor de nube.
- Backup: Es vital recordar que Cryptomator protege la privacidad, no la disponibilidad. Se deben mantener copias de seguridad de las bóvedas cifradas para evitar pérdidas por corrupción de datos o borrado accidental.

PREGUNTAS FRECUENTES

¿Qué es Cryptomator y en qué se diferencia de otras soluciones de cifrado?

Cryptomator es una herramienta de código abierto diseñada para el cifrado de archivos en el lado del cliente, específicamente optimizada para la nube. A diferencia del cifrado de disco completo (como BitLocker o VeraCrypt), que cifra sectores de almacenamiento, Cryptomator cifra archivos de forma individual. Esto permite que los servicios de sincronización como Google Drive o Dropbox detecten cambios en archivos específicos y los suban a la red sin necesidad de resincronizar todo el contenedor de datos.

¿Cómo ayuda Cryptomator al cumplimiento del RGPD en empresas?

Gracias a su arquitectura de 'Conocimiento Cero' (Zero Knowledge), Cryptomator garantiza que solo el profesional que posee la clave maestra pueda acceder al contenido. Esto permite a las empresas utilizar proveedores de nube pública para almacenar datos sensibles, ya que, incluso en caso de una brecha de seguridad en el servidor del proveedor o una solicitud legal de acceso a los datos, la información permanece cifrada e inaccesible para terceros, cumpliendo así con los requisitos técnicos de protección de datos.

¿Es Cryptomator una tecnología de código abierto (Open Source)?

Sí, el software es de código abierto y se distribuye bajo la licencia GNU General Public License (GPLv3). El código fuente es público y está disponible en GitHub para auditorías independientes, lo que garantiza que no existen puertas traseras y que la comunidad técnica puede verificar la integridad de los algoritmos de cifrado utilizados.

¿Qué sucede si pierdo mi contraseña maestra?

Al ser una herramienta de seguridad estricta sin servidores centrales que almacenen credenciales, no existe una función de 'recuperar contraseña'. Si el profesional pierde la contraseña maestra y no cuenta con la clave de recuperación generada durante la creación de la bóveda, los datos se vuelven técnicamente irrecuperables. Es fundamental gestionar estas credenciales mediante un gestor de contraseñas o copias de seguridad físicas seguras.

¿Cuál es el coste de uso para un entorno profesional?

La aplicación de escritorio para Windows, macOS y Linux es gratuita y funciona bajo un modelo de donación voluntaria. Las aplicaciones móviles para Android e iOS requieren un pago único por licencia. Para organizaciones que necesitan gestión centralizada de accesos y administración de equipos, existe 'Cryptomator Hub', que opera bajo un modelo de suscripción por usuario.

¿Permite la edición colaborativa en tiempo real como Google Docs?

No. Debido a que el cifrado y descifrado ocurren localmente en el dispositivo del usuario, los servidores de la nube no pueden leer ni indexar el contenido de los archivos. Esto impide la edición simultánea en tiempo real dentro de las interfaces web de los proveedores. Para editar un archivo, se debe abrir desde la unidad virtual localmente y, una vez guardado, el cliente de la nube sincronizará la versión cifrada actualizada.

¿Qué estándares de seguridad utiliza para proteger la información?

Cryptomator utiliza estándares de grado militar, incluyendo el cifrado AES-256 para el contenido de los archivos y los nombres de los mismos. Además, implementa Scrypt para el endurecimiento de la clave maestra contra ataques de fuerza bruta y protege la estructura de directorios para evitar que se filtre información a través de la arquitectura de las carpetas.

¿Es compatible con todos los servicios de almacenamiento en la nube?

Es compatible con cualquier servicio que sincronice una carpeta local en el ordenador, como OneDrive, Dropbox, iCloud o Google Drive. También soporta conexiones directas a través de protocolos estándar como WebDAV, lo que facilita su integración con servidores NAS o servicios de almacenamiento que no disponen de cliente de escritorio oficial.

¿Existe una versión web para acceder a los archivos desde cualquier navegador?

No existe una versión web por diseño de seguridad. Para mantener el principio de 'Conocimiento Cero', el descifrado debe ocurrir siempre en un entorno local controlado por el usuario. Permitir el descifrado en un navegador web implicaría enviar la clave maestra a un servidor o ejecutar código JavaScript que podría ser vulnerable a interceptaciones.

CONTRATOS Y CONDICIONES

Principales recomendaciones
- La arquitectura técnica de Cryptomator se basa en el "Conocimiento Cero" (Zero Knowledge), lo que significa que el fabricante no tiene acceso a las claves ni a los archivos decodificados.
- Es imperativo establecer una política interna de custodia de contraseñas maestras y claves de recuperación. La pérdida de estas claves implica la pérdida irreversible de los datos, ya que no existe un mecanismo de recuperación por parte del proveedor.
- Para uso profesional en equipos, se recomienda la implementación de Cryptomator Hub (SaaS o Self-Hosted) para gestionar permisos de acceso de forma centralizada sin comprometer el cifrado extremo a extremo.

Privacidad y protección de datos
- Responsabilidades: La empresa usuaria actúa como Responsable del Tratamiento. Skymatic GmbH (el fabricante) es únicamente el proveedor del software y, en la versión de escritorio, no tiene acceso a los datos tratados, por lo que no suele requerirse un Acuerdo de Encargo de Tratamiento (DPA), salvo si se utiliza el servicio gestionado de Cryptomator Hub.
- Ubicación de los datos: Los datos cifrados se almacenan en el proveedor de nube que elija la empresa (Google, Dropbox, etc.). El software Hub Managed se aloja en centros de datos con certificación ISO 27001 dentro de la Unión Europea (Alemania).
- Transferencia internacional: El uso de Cryptomator se considera una "medida técnica suplementaria" adecuada según las directrices del SEPD y sentencias del Consejo de Estado belga (2021). Esto permite el uso de nubes extracomunitarias (EE. UU.) cumpliendo con el RGPD, ya que el proveedor del almacenamiento solo aloja datos cifrados inteligibles.
- Derechos ARCO: La empresa debe garantizar estos derechos directamente, ya que el software solo facilita la seguridad técnica y no interfiere en la gestión de la base de datos de los interesados.

Propiedad intelectual
- Propiedad de datos: La empresa usuaria mantiene la propiedad total de los datos almacenados y de las claves de cifrado generadas.
- Propiedad del resultado/procesamiento: El software de escritorio se distribuye bajo licencia Open Source GPLv3, lo que permite auditar el código pero obliga a compartir las modificaciones si se distribuyen. Cryptomator Hub tiene licencias comerciales específicas que prohíben la ingeniería inversa o el uso para crear productos competidores.

Usos y prohibiciones
- Usos admitidos: Cifrado de documentos confidenciales, historiales clínicos, nóminas y secretos comerciales en entornos de nube pública o almacenamiento compartido.
- Usos prohibidos: No debe utilizarse para el almacenamiento de datos que requieran edición colaborativa en tiempo real por el servidor (como Google Docs nativo), ya que el cifrado impide estas funciones. Queda prohibido el uso de la infraestructura de Cryptomator Hub para actividades ilícitas o que dañen la integridad de los servidores del proveedor.

Seguridad y certificaciones
- Seguridad: Cifrado AES-256 (simétrico) aplicado a nivel de archivo (File-side encryption). Los nombres de archivos y estructuras de carpetas también son cifrados (obfuscation).
- Certificaciones: El centro de datos utilizado para la versión Managed de Cryptomator Hub cuenta con la certificación ISO/IEC 27001:2022. El código fuente es abierto y está sujeto a auditorías públicas y comunitarias periódicas.

Otros
- Legislación aplicable: La relación contractual con Skymatic GmbH se rige por la legislación de Alemania, con tribunales competentes en Bonn.
- Continuidad: Al ser de código abierto, la empresa usuaria tiene garantizada la posibilidad de descifrar sus datos incluso si Skymatic GmbH cesara su actividad, siempre que conserve el software y las claves.

Fuentes consultadas:
- Cumplimiento RGPD en Cryptomator
- Términos y condiciones de Cryptomator Hub
- Condiciones de licencia y uso

- Repositorio oficial de código (GitHub)
- Información corporativa Skymatic GmbH

Para más información y herramientas:

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

Inicio Todas las herramientas Categorías