MULLVAD VPN

GUÍA DE PRIVACIDAD

Mullvad VPN

Los principios, sin tecnicismos

Qué hace una VPN y por qué Mullvad es distinta.

01

Qué es Mullvad

Mullvad es una VPN: un servicio que protege tu conexión a internet y esconde de dónde sales. Lo ofrece una empresa sueca desde 2009 y se distingue por una idea muy simple: saber lo menos posible de sus clientes.

SIN DATOS PERSONALES

Para abrir una cuenta no hace falta nombre, correo ni teléfono.

SIN REGISTROS

No guarda qué webs visitas, ni cuándo, ni desde dónde.

CÓDIGO ABIERTO

Sus aplicaciones se pueden revisar, y empresas externas las auditan.

02

Cuatro ideas previas

Con estas cuatro ideas se entiende todo lo demás.

1. **La dirección IP.** Es la dirección postal de tu conexión. Cada web que visitas la ve, y con ella sabe aproximadamente en qué ciudad estás y qué operador usas.
2. **El DNS.** Es la agenda de internet: traduce un nombre como "ejemplo.org" en la dirección del ordenador que lo aloja. Por defecto, tu operador responde a esas preguntas, así que sabe qué webs quieres visitar.
3. **El cifrado.** Convierte un mensaje en un revoltijo que solo se puede deshacer con una clave. Protege el contenido, pero no esconde con quién hablas.
4. **El túnel.** Una VPN cierra un túnel cifrado entre tu dispositivo y un servidor suyo. Tu tráfico entra por un lado y sale a internet por el otro, con la dirección del servidor y no la tuya.

03

El problema: alguien siempre ve tu tráfico

Sin VPN, tu operador ve a qué servidores te conectas y las webs ven tu IP. Con VPN, esa mirada pasa del operador al proveedor de la VPN. La VPN no elimina la confianza: la traslada.

> **La pregunta clave.** Si el proveedor ve tu tráfico, lo importante es qué hace con él y qué puede demostrar. Mullvad intenta que la respuesta sea "nada" y que no tengas que fiarte solo de su palabra.

04

Los tres principios de privacidad

Mullvad reduce lo que sabe de ti en tres frentes a la vez.

QUIÉN ERES

Cuenta anónima

Un número al azar en lugar de un perfil.

QUIÉN PAGA

Pago sin rastro

Efectivo por correo o Monero.

QUÉ HACES

Servidores sin memoria

Sin disco, sin registros.

Quién eres: una cuenta anónima

Al crear la cuenta, Mullvad te da un número de 16 dígitos generado al azar. Ese número es tu usuario y tu contraseña a la vez. No hay formulario ni correo, así que no existe una base de datos con tu nombre. Es como entrar a una consigna con un ticket numerado: quien guarda las maletas no sabe quién eres. La contrapartida es que, si pierdes el número, no hay forma de recuperarlo.

Quién paga: pagos sin rastro

Una cuenta anónima no sirve si el pago te identifica. Por eso Mullvad acepta efectivo enviado por correo y Monero, además de tarjeta y otros métodos. El precio es siempre el mismo, 5 euros al mes, sin renovaciones automáticas. Pagas el tiempo que quieres y, cuando se

acaba, la cuenta caduca.

Qué haces: servidores sin memoria

Los servidores de Mullvad funcionan solo con memoria RAM, sin disco duro. Cuando se apagan o se reinician, todo lo que había dentro se borra. Es como una pizarra que se limpia sola: aunque alguien se llevara el servidor, no encontraría un historial. En abril de 2023 la policía sueca se presentó en la oficina de Mullvad con una orden de registro y se marchó sin llevarse datos de clientes, porque Mullvad dijo no tener ninguno.

> Los tres principios funcionan juntos: Mullvad no sabe quién eres, no sabe quién paga y no guarda lo que haces. Si alguien le pidiera datos, no tendría qué entregar.

05

Una conexión, paso a paso

1. Abres la aplicación de Mullvad e introduces tu número de cuenta de 16 dígitos.
2. Tu dispositivo crea un par de claves. La privada se queda en el dispositivo y solo se comparte la pública.
3. La aplicación abre un túnel cifrado hacia un servidor de Mullvad, usando el protocolo WireGuard.
4. Tu tráfico y tus consultas de DNS entran en el túnel. Tu operador solo ve una conexión cifrada hacia Mullvad.
5. El servidor envía tu tráfico a internet con su propia dirección IP, compartida con muchos otros usuarios.
6. Las webs ven la IP del servidor y no la tuya. Si el túnel se cae, el "kill switch" corta la conexión para que no se escape nada.

06

Protecciones adicionales

Además del túnel básico, Mullvad ofrece tres defensas para amenazas más avanzadas.

FUTURO

Túneles cuánticos

Añaden una capa que resistiría a los ordenadores cuánticos del futuro.

DOS SALTOS

Multihop

El tráfico pasa por dos servidores, de forma que ninguno conoce a la vez quién eres y qué haces.

DISFRAZ

DAITA

Mezcla tráfico falso para que no se reconozca qué web visitas por la forma del tráfico.

Por qué importan

Los ordenadores cuánticos todavía no pueden romper el cifrado actual, pero alguien podría grabar hoy tu tráfico cifrado y abrirlo dentro de unos años. Los túneles resistentes a esa amenaza ya están activados por defecto en las aplicaciones de escritorio. El multihop y DAITA son opciones para quien necesita un nivel de protección mayor, a costa de algo de velocidad.

07

Cómo empezar

1. **Instala la aplicación oficial** desde la web de Mullvad y genera tu número de cuenta.
2. **Guarda el número en un gestor de contraseñas.** Es tu único acceso: si lo pierdes, no hay forma de recuperarlo.
3. **Elige cómo pagar según lo que busques.** Para anonimato, efectivo o Monero; para comodidad, tarjeta.
4. **Activa el kill switch** y los túneles cuánticos, y prueba la conexión con la herramienta de la web de Mullvad.

REFERENCIA

Glosario rápido

TÉRMINO	SIGNIFICADO
VPN	Túnel cifrado hacia un servidor que esconde tu IP
IP	La dirección de tu conexión a internet
DNS	La agenda que traduce nombres de web en direcciones
Cifrado	Convertir datos en algo ilegible sin la clave
Logs	Registros de quién hizo qué y cuándo
WireGuard	El protocolo de túnel moderno que usa Mullvad
Kill switch	Corte automático si la VPN falla
Multihop	Pasar por dos servidores en lugar de uno
DAITA	Defensa que disfraza el patrón del tráfico

> **Siguiente paso.** La guía completa, "Mullvad a fondo", explica cada una de estas piezas con más detalle: los pagos, la redada de 2023, WireGuard, los túneles cuánticos y los límites de una VPN.

Fuentes: web y blog de Mullvad, CyberInsider, TechRadar y Ghacks.