MULLVAD VPN

GUÍA DE PRIVACIDAD

Mullvad a fondo

Guía completa

Esta guía explica cómo funciona Mullvad VPN y qué protege de verdad: la cuenta sin datos personales, el pago anónimo, los servidores que no guardan nada, el cifrado WireGuard, los túneles resistentes a la computación cuántica y las defensas contra el análisis de tráfico.

De la VPN anónima al tráfico cifrado y ofuscado

Contenido

INTRODUCCIÓN Y BASES

· Cómo usar esta guía 3

· Los conceptos básicos 3

CAPÍTULOS

01 Qué es Mullvad y qué problema resuelve 5

02 La cuenta anónima: un número de 16 dígitos 7

03 Pagos y precio 8

04 La política de no logs 9

05 La redada de 2023 10

06 Servidores sin disco y auditorías externas 11

07 WireGuard por dentro 12

08 GotaTun y el adiós a OpenVPN 15

09 Túneles resistentes a la computación cuántica 17

10 Multihop: dos saltos en vez de uno 19

11 DAITA y el análisis de tráfico 20

12 DNS, bloqueadores, kill switch y fugas 21

13 Mullvad Browser y la relación con Tor 23

14 Limitaciones y lo que una VPN no puede hacer 24

15 Buenas prácticas 26

INTRODUCCIÓN

Cómo usar esta guía

Público y prerrequisitos. No hace falta saber de redes ni de criptografía. La sección "Antes de empezar" explica desde cero qué es una dirección IP, qué es el DNS y qué hace exactamente una VPN. Después la guía va subiendo de nivel poco a poco.

Estado del producto. Mullvad cambia con frecuencia. Esta guía recoge la situación actual: solo WireGuard (OpenVPN se retiró en enero de 2026), túneles resistentes a la computación cuántica en todas las plataformas de escritorio y móviles, y GotaTun como implementación propia de WireGuard, ya disponible en Android y en despliegue en el resto de plataformas. Si un detalle puede haber cambiado, consulta la web y el blog de Mullvad.

Cómo leerla. Si partes de cero, empieza por "Antes de empezar". Los capítulos 1 a 6 explican el modelo de privacidad: qué datos existen y cuáles no. Los capítulos 7 a 11 explican la tecnología de red y de cifrado. Los capítulos 12 a 15 son prácticos: fugas, navegador, límites y buenas costumbres.

ANTES DE EMPEZAR

Los conceptos básicos

Para entender qué aporta una VPN hay que conocer cuatro piezas de internet: la dirección IP, el DNS, el cifrado y quién puede ver qué en el camino entre tu dispositivo y una web.

La dirección IP

Cada conexión a internet usa una **dirección IP**, un número parecido a `203.0.113.45` que funciona como la dirección postal de tu conexión. Cuando abres una web, el servidor necesita saber a dónde mandar la respuesta, así que tu IP viaja con cada petición.

Tu IP la asigna tu operador (el proveedor de internet, o ISP). Revela aproximadamente en qué ciudad estás y qué operador usas. Y como el operador sabe a qué cliente se la asignó, puede enlazar esa IP con tu nombre y tu dirección.

El DNS: la agenda de internet

Los ordenadores se encuentran por número, pero las personas usamos nombres como `ejemplo.org`. El **DNS** es la agenda que traduce el nombre en el número. Antes de visitar una web, tu dispositivo pregunta a un servidor DNS "¿cuál es la IP de ejemplo.org?". Por defecto esa pregunta la responde el servidor de tu operador, que así se entera de todos los sitios que visitas, aunque el contenido de la página vaya cifrado.

Cifrar es esconder el contenido

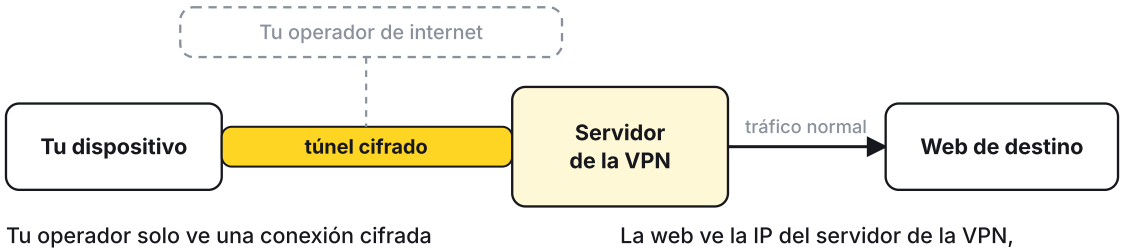
Cifrar es convertir un mensaje en un revoltijo que solo puede deshacer quien tiene la clave. Hoy casi todas las webs usan HTTPS, que cifra el contenido entre tu navegador y la web. Pero el cifrado no esconde con quién hablas: tu operador sigue viendo a qué servidores te conectas, cuándo y cuántos datos intercambias.

Qué ve cada uno sin VPN

QUIÉN	QUÉ VE SIN VPN
Tu operador de internet	Qué servidores visitas, cuándo y cuántos datos; normalmente también tus consultas DNS
La web que visitas	Tu IP, y con ella tu ciudad aproximada y tu operador
La red Wi-Fi pública	Qué servidores visitas y cuándo, si no hay cifrado extra
Cualquiera que vigile tu tramo	El destino de cada conexión y su volumen

Qué hace una VPN

Una **VPN** (red privada virtual) crea un túnel cifrado entre tu dispositivo y un servidor del proveedor. Todo tu tráfico entra en el túnel y sale a internet desde ese servidor.



Qué ve cada parte cuando usas una VPN.

El efecto es doble:

- Tu operador solo ve que hay una conexión cifrada hacia el proveedor de la VPN, no los sitios que visitas.
- Las webs ven la IP del servidor de la VPN, no la tuya.

Fíjate en lo que cambia: la confianza se desplaza. Antes, tu operador veía tu tráfico. Ahora lo ve el proveedor de la VPN. Por eso lo importante de una VPN no es el túnel, sino **qué hace el proveedor con lo que ve** y qué puede demostrar. Esa es la pregunta que organiza toda esta guía.

Glosario rápido

TÉRMINO	SIGNIFICADO
IP	Dirección de tu conexión a internet
ISP	Tu operador o proveedor de internet
DNS	La agenda que traduce nombres de web en IP
VPN	Túnel cifrado hacia un servidor del proveedor
Cifrado	Convertir datos en algo ilegible sin la clave
Clave	Número secreto que cifra o descifra
Servidor	Ordenador del proveedor por donde sale tu tráfico
Logs	Registros de lo que ocurrió: quién, cuándo, a dónde

CAPÍTULO 1

Qué es Mullvad y qué problema resuelve

Mullvad VPN es un servicio de VPN que ofrece la empresa sueca Amagicom desde Gotemburgo. Lleva operando desde 2009 y se distingue menos por la tecnología de túnel, que es estándar, que por **cuánto sabe de ti**: casi nada, y por diseño.

Qué hace una VPN y qué no

Hay que separar lo que una VPN protege de lo que no toca.

UNA VPN SÍ HACE	UNA VPN NO HACE
Oculta tu IP real a las webs que visitas	No te hace anónimo si inicias sesión con tu cuenta
Impide que tu operador o una red Wi-Fi vean los sitios que visitas	No protege de virus ni de páginas de estafa
Cifra el tramo entre tu dispositivo y el servidor	No cifra el tramo entre el servidor y la web (eso lo hace HTTPS)
Te hace parecer en otro país	No evita que te identifique el navegador (huella digital)

Modelo de amenazas

Un **modelo de amenazas** responde a tres preguntas: qué quieres proteger, de quién y qué estás dispuesto a hacer para ello. Para una VPN, los adversarios típicos son estos:

1. **Tu operador y las redes en las que te conectas** (cafés, hoteles, trabajo). Una VPN bien usada les impide ver tus destinos.
2. **Las webs y los anunciantes**, que usan tu IP para ubicarte y cruzar perfiles. La VPN cambia esa IP, aunque no frena otras formas de rastreo.
3. **Quien pueda pedir datos al proveedor de la VPN** (un juzgado, una policía). La mejor defensa es que el proveedor no tenga datos que entregar.
4. **Un observador que mira ambos extremos de la conexión.** Contra este adversario la VPN ayuda poco; se explica en el capítulo 14.

Mullvad está pensado sobre todo para los casos 1, 2 y 3. Para el 4 ofrece mitigaciones parciales (DAITA, multihop), pero ninguna herramienta lo resuelve del todo.

La idea central: confiar lo menos posible

Un proveedor de VPN ve tu tráfico por fuerza. Mullvad intenta que eso importe lo menos posible con cuatro decisiones de diseño que desarrollan los próximos capítulos:

- Una cuenta que no contiene datos personales.
- Pagos que se pueden hacer sin dejar rastro.
- Servidores que no guardan registros.
- Auditorías externas y código abierto, para que no tengas que creer en su palabra.

CAPÍTULO 2

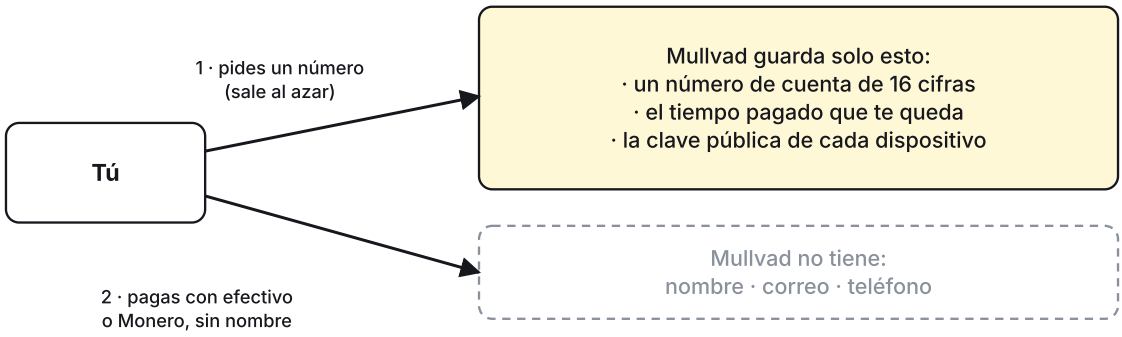
La cuenta anónima: un número de 16 dígitos

Para crear una cuenta en Mullvad no hay formulario. Pulsas un botón y la web te da un **número de cuenta de 16 dígitos** generado al azar. Ese número es tu único identificador: sirve como usuario y como contraseña a la vez.

No se pide nombre, ni correo, ni teléfono. La web de Mullvad lo resume así: no piden ningún dato personal, ni siquiera el correo.

Por qué funciona

Lo que no se recoge no se puede perder, filtrar ni entregar. Si una autoridad pide a Mullvad "los datos del cliente X", no existe un campo donde buscar un nombre. Tampoco hay lista de correos que robar en una brecha.



El pago y la cuenta no se enlazan con ninguna identidad.

La cuenta se crea y se paga sin ningún dato personal.

El precio de este diseño

No hay recuperación de cuenta. Si pierdes el número, pierdes el acceso y el tiempo pagado: no existe un "he olvidado mi contraseña" porque Mullvad no sabe a quién escribirle. Guarda el número en un gestor de contraseñas. Y trata el número como una llave: quien lo tenga puede usar tu cuenta.

Dispositivos

Cada cuenta admite hasta cinco dispositivos a la vez. Al añadir un dispositivo, la app genera en él un par de claves de WireGuard y entrega a Mullvad solo la clave pública (capítulo 7). La clave privada nunca sale del dispositivo.

CAPÍTULO 3

Pagos y precio

De nada sirve una cuenta anónima si el pago te identifica. Un pago con tarjeta deja un rastro en el banco y en el procesador de pagos, y ese rastro enlaza tu nombre con una cuenta de Mullvad.

Un precio plano

Mullvad cobra **5 euros al mes**, sin descuentos por pagar años por adelantado y sin plan gratuito. Es un precio que no cambia con la duración: pagar 12 meses cuesta 12 veces lo que un mes. Tampoco hay renovación automática: pagas tiempo, y cuando se acaba, la cuenta caduca. Mullvad canceló incluso las suscripciones recurrentes de PayPal que quedaban, porque una suscripción obliga a guardar datos de pago.

Este modelo también explica por qué Mullvad no hace marketing agresivo ni paga a afiliados: su web dice que evita las reseñas pagadas y los programas de afiliación.

Formas de pago

MÉTODO	QUÉ RASTRO DEJA
Efectivo por correo	El más bajo: un sobre con dinero y tu número de cuenta, sin remitente obligatorio
Monero	Muy bajo: la propia moneda oculta emisor, receptor y cantidad
Bitcoin y Bitcoin Cash	Bajo, pero la cadena de bloques es pública y puede analizarse
Tarjeta, transferencia, Swish, otros	Alto: el banco o el procesador conoce el pago
Vales de revendedores	Depende de dónde se compre el vale

Mullvad empezó a aceptar Monero oficialmente en mayo de 2022. Es una elección coherente con su filosofía: Monero oculta quién paga y cuánto, igual que la cuenta de Mullvad oculta quién eres.

El efectivo

El pago en efectivo funciona así: en la web generas un código ligado a tu número de cuenta, metes billetes en un sobre con ese código y lo envías a la oficina de Mullvad. Se acepta en varias divisas. Es el método más anónimo, aunque también el más lento.

Qué se guarda del pago

Mullvad guarda lo mínimo para acreditar el pago y evitar duplicados, y según se ha publicado lo borra a las pocas semanas. Los métodos con intermediario (tarjeta, PayPal) siguen dejando su propio registro en el procesador, fuera del control de Mullvad. Si tu objetivo es el anonimato, elige efectivo o Monero.

CAPÍTULO 4

La política de no logs

Un **log** es un registro de actividad: quién se conectó, a qué hora, desde qué IP y a dónde fue. La política de **no logs** de Mullvad consiste en no guardar ninguno de esos registros.

Qué no guarda

- Qué sitios visitas ni qué contenido envías.
- Tus consultas DNS.
- Tu IP real ni las marcas de tiempo de tus conexiones.
- Cuánto ancho de banda usas.

Qué sí existe

Para funcionar, Mullvad necesita unos pocos datos: tu número de cuenta, la fecha de caducidad del tiempo pagado, las claves públicas de tus dispositivos y un contador de dispositivos conectados para aplicar el límite de cinco. Ninguno de ellos dice qué haces con la VPN.

De la promesa a la arquitectura

Cualquier VPN puede escribir "no logs" en su web. Lo que importa es que el sistema no pueda guardarlos aunque quisiera, y que alguien independiente lo verifique. Mullvad intenta cubrir las dos cosas con servidores sin disco (capítulo 6) y con auditorías externas. Aun así, una política de no logs sigue siendo, en última instancia, una afirmación sobre el comportamiento de una empresa. Por eso el capítulo siguiente es tan relevante: es la única vez que se ha puesto a prueba con una orden judicial.

CAPÍTULO 5

La redada de 2023

El 18 de abril de 2023, al menos seis agentes de la División de Operaciones Nacionales de la policía sueca se presentaron en la oficina de Mullvad en Gotemburgo con una orden de registro. Buscaban ordenadores con datos de clientes.

Qué pasó

Según Mullvad, el personal explicó a los agentes que no existen datos de clientes que incautar y les mostró cómo funciona el servicio. La policía se marchó sin llevarse equipos ni información. Nueve días después, las autoridades suecas declararon que el registro se había hecho a petición de Alemania, dentro de una investigación en curso.

Qué demuestra y qué no

La redada es un dato valioso porque es una prueba real, no una promesa: una autoridad con orden judicial no encontró nada que llevarse. Pero conviene medir bien su alcance.

- **Demuestra** que, en esa fecha, Mullvad no entregó datos de clientes y que la policía no encontró registros que incautar.
- **No demuestra** que nunca ocurrirá nada distinto, ni que los servidores físicos no pudieran vigilarse por otras vías. Una prueba sola no es una garantía.

Mullvad recordó después que la jurisdicción sueca da protección a sus clientes, y sus servidores funcionan sin disco, algo que se explica en el capítulo siguiente.

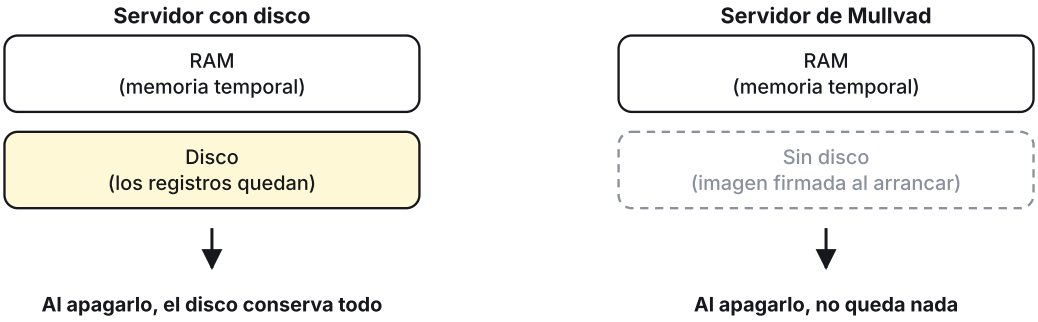
CAPÍTULO 6

Servidores sin disco y auditorías externas

Una promesa es más creíble cuando la arquitectura la hace difícil de romper y cuando alguien ajeno la revisa.

Servidores que solo usan memoria RAM

Los servidores de Mullvad funcionan **sin disco**: el sistema operativo arranca desde una imagen firmada y trabaja únicamente en la memoria RAM. La RAM pierde su contenido al apagarse, así que cualquier reinicio o corte de corriente borra todo lo que hubiera en la máquina.



La RAM se borra al apagarse; un disco, no.

Esto tiene dos consecuencias prácticas:

- Aunque alguien incautara un servidor físico, al apagarlo no quedaría nada que recuperar.
- Es difícil que un fallo o una instalación descuidada deje registros olvidados en un disco.

El límite es que la RAM sí contiene datos mientras el servidor está encendido. Una intervención con el equipo en marcha sigue siendo una amenaza teórica, y por eso importa que el propio sistema no acumule datos sensibles.

Auditorías independientes

Mullvad encarga auditorías externas periódicas de su aplicación y de su infraestructura a empresas como Cure53, Assured Security Consultants y otras, y publica los informes en su web, incluidos los hallazgos que no le favorecen. Las revisiones han encontrado problemas menores que se corrigieron, sin hallazgos críticos en los informes públicos.

Un ejemplo reciente es la auditoría de **GotaTun**, la implementación propia de WireGuard (capítulo 8). Assured Security Consultants revisó su código entre enero y febrero de 2026, y Mullvad publicó el resultado en marzo de 2026. Encontró dos problemas de gravedad baja y nueve observaciones informativas, y ninguno crítico, alto ni medio. Uno de los dos fallos menores era un método de generar identificadores de sesión heredado del proyecto original, que podía dar a un observador pasivo algo de información. Mullvad lo corrigió en la versión 0.3.0.

Cómo leer una auditoría

- Una auditoría revisa un **alcance concreto** en un momento concreto. La de GotaTun, por ejemplo, no cubría DAITA.
- Que no aparezcan fallos graves no es una prueba de que no existan.
- Que se publique el informe completo es una buena señal, porque deja revisar lo que se dijo.
- El código de las aplicaciones de Mullvad es abierto, lo que permite además la revisión de cualquiera.

CAPÍTULO 7

WireGuard por dentro

WireGuard es el protocolo de túnel que usa Mullvad. Lo diseñó Jason Donenfeld como una alternativa más simple y rápida a protocolos anteriores. Mullvad lo adoptó pronto, en 2017, y desde enero de 2026 es el único que ofrece.

Por qué importa que sea simple

Cuanto menos código hay, menos sitios donde esconder un fallo. WireGuard es mucho más corto que sus predecesores y eso lo hace más fácil de auditar. Además es opinado: no ofrece listas de algoritmos entre los que elegir, sino un conjunto fijo y moderno. Eso evita ataques que fuerzan a usar una opción débil.

Las piezas criptográficas

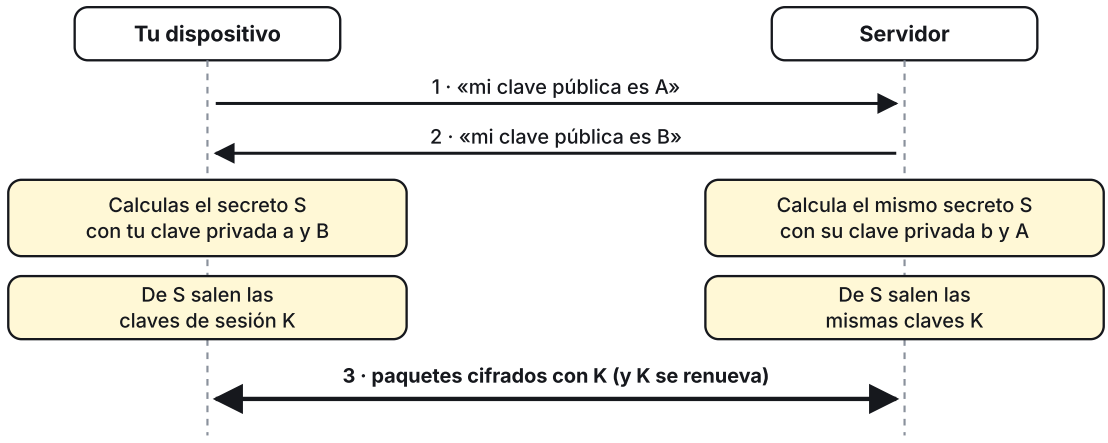
WireGuard se construye sobre el marco **Noise**, que define cómo dos partes se ponen de acuerdo en claves secretas. Cada pieza hace un trabajo concreto:

PIEZA	PARA QUÉ SIRVE
Curve25519	Intercambio de claves: dos partes calculan un secreto compartido sin enviarlo
ChaCha20-Poly1305	Cifra los paquetes y comprueba que nadie los ha alterado
BLAKE2s	Función hash: convierte datos en una huella de tamaño fijo
HKDF	Deriva varias claves a partir de un secreto compartido

Cómo se establece un túnel

1. **Cada dispositivo tiene un par de claves.** La clave privada se queda en el dispositivo; la pública se registra en Mullvad.
2. **Apretón de manos.** El dispositivo y el servidor intercambian claves públicas y calculan, con Curve25519, un secreto compartido que solo ellos conocen.
3. **Claves de sesión.** Del secreto se derivan claves temporales para cifrar los paquetes.
4. **Renovación periódica.** Las claves de sesión se cambian con frecuencia. Así, si un día alguien consigue una clave de sesión, solo descifra un tramo corto del tráfico y no el pasado entero. A esta propiedad se la llama **secreto hacia adelante**.

Todo viaja sobre UDP y el sistema es discreto: si alguien envía paquetes sin una clave válida, el servidor no responde, así que desde fuera no se anuncia como un servicio abierto.



Apretón de manos de WireGuard: se intercambian claves públicas, nunca el secreto.

El acuerdo de claves, paso a paso

El corazón de WireGuard es un truco matemático llamado **intercambio de claves Diffie-Hellman**. Sirve para que dos partes que nunca se han visto acaben con el mismo secreto hablando en público, sin enviarlo. Una imagen: tú y el servidor partís de un bote de pintura amarilla que todo el mundo conoce, y cada uno le añade un color secreto propio. Os intercambiáis los botes mezclados y cada uno vuelve a añadir su secreto al bote que recibe. Los dos acabáis con exactamente la misma mezcla. Quien solo vio los botes por el camino no puede separar los colores.

FÓRMULA CLAVE.

$$S = a \cdot B = b \cdot A = (a\,b) \cdot G$$

En palabras: tú y el servidor llegáis al mismo número secreto S combinando cada uno su clave privada con la clave pública del otro.

Qué es cada símbolo:

- `G`: un punto fijo y público de la curva Curve25519. Es el bote de pintura amarilla del que todos parten.
- `a` y `b`: las claves privadas, la tuya y la del servidor. Son números aleatorios y nunca salen del dispositivo.
- `A = a·G` y `B = b·G`: las claves públicas. Se obtienen "sumando G consigo mismo" `a` o `b` veces. Se pueden publicar porque, dada `A`, recuperar `a` es inviable (el problema del logaritmo discreto).
- `·`: aquí no es una multiplicación corriente, sino sumar un punto de la curva consigo mismo muchas veces.
- `S`: el secreto compartido, igual para los dos.

Un ejemplo con números pequeños. Para poder seguirlo con lápiz usamos una versión más sencilla que la curva: aritmética de reloj de 23 horas (módulo 23) con base 5. La idea es idéntica.

1. Tú eliges en secreto `a = 6` y calculas `A = 5⁶ mod 23 = 8`. Publicas el 8.
2. El servidor elige en secreto `b = 15` y calcula `B = 5¹⁵ mod 23 = 19`. Publica el 19.
3. Tú calculas `19⁶ mod 23 = 2`.
4. El servidor calcula `8¹⁵ mod 23 = 2`.

Los dos tenéis el 2 sin habérselo enviado a nadie. Un espía vio el 5, el 23, el 8 y el 19, pero no el 6 ni el 15. Con números tan pequeños podría probarlos todos; con los números de 256 bits de Curve25519 no hay tiempo suficiente en el universo.

Por qué funciona: el orden no importa al multiplicar. Tú calculas `a·(b·G)` y el servidor `b·(a·G)`, y los dos son `(a·b)·G`. Es la misma propiedad que `6 × 15 = 15 × 6`, solo que aplicada a puntos de la curva.

El secreto `S` no se usa tal cual. Se pasa por una función derivadora que produce las claves de sesión, y estas alimentan al cifrado de cada paquete:

$$(\text{paquete cifrado},\ \text{sello}) = \text{ChaCha20-Poly1305}(K,\ n,\ \text{mensaje})$$

En palabras: con la clave de sesión `K` y un contador `n` que nunca se repite, el mensaje sale ilegible y con un sello que delata cualquier alteración.

Qué sabe el servidor

El servidor conoce tu clave pública y la IP desde la que te conectas en ese momento, porque la necesita para devolverte los paquetes. Mullvad diseña el sistema para que esa información no se guarde en disco ni se registre (capítulos 4 y 6). Ese dato en memoria es el equivalente de una línea telefónica activa: existe mientras dura la llamada.

CAPÍTULO 8

GotaTun y el adiós a OpenVPN

Durante años Mullvad ofreció dos protocolos: **OpenVPN**, el veterano, y WireGuard. Dos protocolos significan dos bases de código que mantener, probar y auditar. En 2025 Mullvad decidió concentrarse en uno.

La retirada de OpenVPN

La versión 2025.14 de la aplicación de escritorio eliminó la opción de elegir OpenVPN. El 15 de enero de 2026 Mullvad apagó los servidores de OpenVPN que quedaban, así que desde entonces todo el servicio funciona con WireGuard. Quien usara OpenVPN en un router o en una aplicación de terceros tuvo que migrar a WireGuard antes de esa fecha.

La decisión se apoyó en que WireGuard ya soporta lo que antes era exclusivo de OpenVPN, como los modos para saltarse bloqueos de red (UDP sobre TCP y Shadowsocks).

Qué es GotaTun

Las aplicaciones móviles de Mullvad usaban `wireguard-go`, una implementación de WireGuard escrita en el lenguaje Go. Tras años de fricción con ella, Mullvad creó **GotaTun**, su propia implementación escrita en **Rust**. El nombre rinde homenaje al túnel Götatunneln de Gotemburgo.

- GotaTun nació como bifurcación (fork) de BoringTun, la implementación en Rust de Cloudflare.
- Es código abierto bajo licencia BSD de tres cláusulas.
- Incorpora las funciones propias de Mullvad, como multihop y DAITA.
- Llegó primero a Android, a finales de noviembre de 2025. Mullvad prevé llevarla al resto de plataformas durante 2026.

Según los datos internos de Mullvad, la tasa de cierres inesperados percibida por los usuarios de Android bajó del 0,40 % al 0,01 % tras adoptar GotaTun en la versión 2025.10, con mejoras en velocidad y consumo de batería.

Por qué Rust

La mayor parte de los fallos graves de seguridad en software de red nacen de errores de memoria: leer o escribir donde no se debe. Rust está diseñado para impedir esa clase de errores en tiempo de compilación. Escribir la pieza que maneja todo tu tráfico en un lenguaje así reduce el riesgo.

Qué se usa en cada plataforma

Mullvad usa distintas implementaciones de WireGuard según la plataforma y las funciones activadas. En Linux, por ejemplo, se usa por defecto la implementación del núcleo por rendimiento, y GotaTun entra cuando se activan funciones como multihop o DAITA. El reparto cambia con las versiones, así que para el estado exacto conviene mirar la página técnica de Mullvad.

CAPÍTULO 9

Túneles resistentes a la computación cuántica

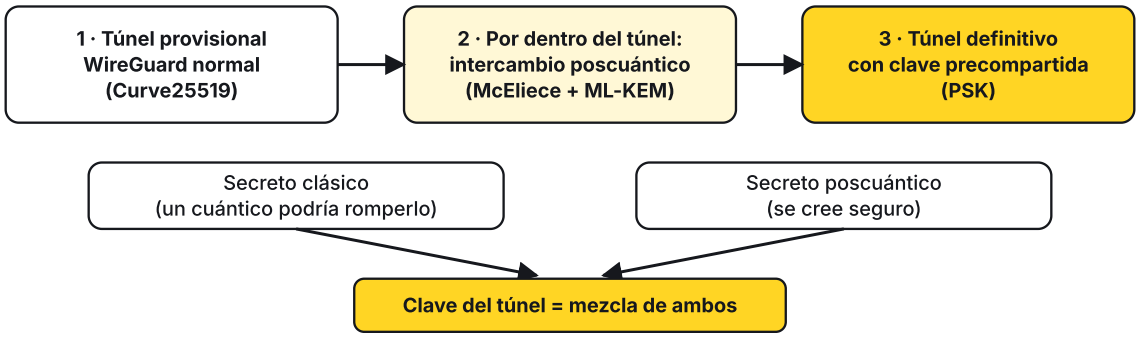
Un **ordenador cuántico** suficientemente potente podría romper los intercambios de claves que se usan hoy, incluido Curve25519. Aún no existe uno capaz, pero hay un riesgo ya presente: alguien puede **grabar hoy tráfico cifrado** y guardarlo hasta que exista la máquina que lo abra. Es lo que se llama "guardar ahora, descifrar después".

Qué se rompe y qué no

La parte que cifra los paquetes (ChaCha20) no es el punto débil. El punto débil es el **acuerdo de claves** al inicio, porque su seguridad depende de problemas matemáticos que un ordenador cuántico resolvería deprisa. Si se rompe el acuerdo, se obtiene la clave y el resto cae.

Qué hace Mullvad

Mullvad ofrece túneles resistentes a la computación cuántica en todas las plataformas. El mecanismo aprovecha una opción que WireGuard ya incluye, la **clave precompartida** (PSK), que se mezcla en el cálculo de las claves de sesión.



Túnel resistente a la cuántica: dos capas de seguridad mezcladas.

El proceso es este:

1. La app abre un primer túnel de WireGuard normal hacia el servidor.
2. Por ese túnel, dispositivo y servidor se ponen de acuerdo en un secreto nuevo usando **algoritmos poscuánticos**: Classic McEliece y Kyber (hoy estandarizado como ML-KEM).

3. Se cierra ese primer túnel y se abre uno definitivo que usa el secreto nuevo como clave precompartida.

El resultado es un túnel que es seguro si **cualquiera** de las dos capas resiste: la clásica o la poscuántica. Un atacante tendría que romper las dos. A esto se le llama diseño **híbrido**, y evita apostar todo a algoritmos nuevos que todavía tienen pocos años de análisis.

Una imagen para entender por qué hacen falta las dos capas: es una caja fuerte con dos cerraduras en serie. Para abrirla se necesitan las dos llaves. Si un ordenador cuántico futuro consigue la primera (la clásica), la segunda (la poscuántica) sigue cerrada, y viceversa.

FÓRMULA CLAVE.

$$K = \mathrm{HKDF}\left(S_{\text{clásico}},\ S_{\text{poscuántico}}\right)$$

En palabras: la clave final del túnel se obtiene mezclando los dos secretos, el del intercambio de claves normal y el del intercambio poscuántico; sin conocer ambos no se puede calcular.

Qué es cada pieza:

- `S_clásico`: el secreto del intercambio Curve25519 del capítulo 7. Un ordenador cuántico podría calcularlo.
- `S_poscuántico`: el secreto acordado con Classic McEliece y ML-KEM por el primer túnel. Se cree seguro frente a ordenadores cuánticos. En WireGuard entra por la clave precompartida (PSK).
- `HKDF`: la función que mezcla secretos y entrega una clave que parece aleatoria. Si falta cualquiera de los ingredientes, el resultado es imposible de adivinar.
- `K`: la clave con la que se cifran los paquetes del túnel definitivo.

Por qué funciona: HKDF se comporta como una batidora de una sola dirección. Si un atacante conoce un ingrediente pero no el otro, la mezcla sigue siendo indistinguible de un número al azar. Por eso basta con que una de las dos capas resista.

Estado actual

En la aplicación, una conexión con esta protección muestra el estado "conexión segura cuántica" en verde. Desde la versión de escritorio 2025.2 está activada por defecto en Windows, de modo que ya es el comportamiento por defecto en todas las plataformas de escritorio. Mullvad también informó de que sus túneles no se ven afectados por las vulnerabilidades en algunas implementaciones de Kyber que se divulgaron en su día.

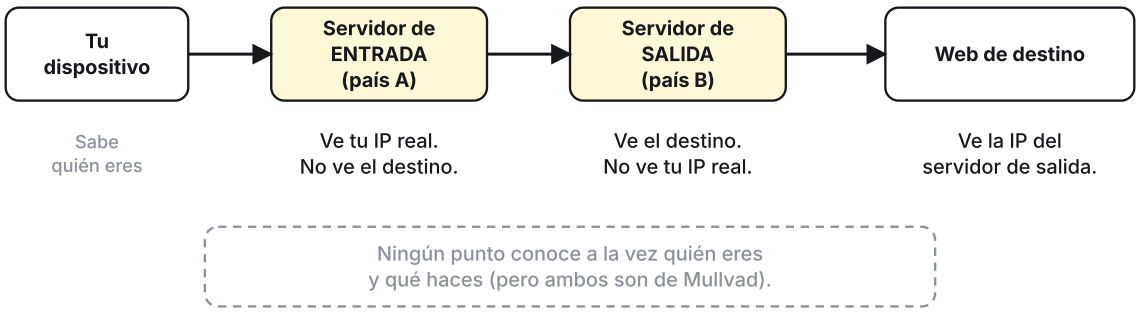
CAPÍTULO 10

Multihop: dos saltos en vez de uno

Con una VPN normal, un solo servidor ve a la vez tu IP real y el destino de tu tráfico. Si ese servidor fuera vigilado, quien lo observe podría enlazar ambos datos. El **multihop** reparte esa información entre dos servidores.

Cómo funciona

Tu tráfico entra por un servidor de **entrada**, que lo reenvía a un servidor de **salida**, y es este último el que lo entrega a internet. Los dos servidores pueden estar en países distintos.



Multihop: cada servidor conoce solo una mitad de la información.

QUIÉN	QUÉ VE
Servidor de entrada	Tu IP real, pero no el destino final
Servidor de salida	El destino, pero no tu IP real: solo ve la IP del servidor de entrada
La web de destino	La IP del servidor de salida

Qué aporta y qué no

- **Aporta** que ningún punto de la cadena conozca a la vez quién eres y qué haces, siempre que ambos servidores no los controle el mismo actor. Es especialmente útil si te preocupa un solo país o un solo centro de datos.
- **Cuesta** más latencia, porque el tráfico recorre un camino más largo.

- **No convierte a Mullvad en dos empresas**: ambos saltos son de Mullvad, así que sigues confiando en el mismo proveedor. El multihop ayuda contra un servidor aislado o un entorno vigilado, no contra el propio proveedor.

CAPÍTULO 11

DAITA y el análisis de tráfico

El cifrado esconde el contenido, pero no esconde la **forma** del tráfico: el tamaño de los paquetes, el ritmo al que llegan y cuánto dura cada ráfaga. Esa forma es una huella.

El problema

Cada web produce un patrón de tráfico reconocible. Cargar una página de un periódico genera una secuencia de paquetes distinta que cargar un vídeo o una web de correo. Un observador que vea tu conexión cifrada, como tu operador, puede entrenar un sistema de **inteligencia artificial** para reconocer esos patrones y deducir qué webs visitas **sin descifrar nada**. A esto se le llama análisis de tráfico o *website fingerprinting*.

La defensa: DAITA

DAITA (siglas de "defensa contra el análisis de tráfico guiado por IA") es una función de la aplicación de Mullvad que añade ruido para estropear esa huella.



DAITA tapa la forma del tráfico con relleno y paquetes de tamaño fijo.

Hace tres cosas:

1. **Tráfico falso aleatorio**: envía paquetes de relleno en momentos impredecibles, de modo que no se vea cuándo estás realmente activo.
2. **Distorsión del patrón**: mientras visitas una web, mete paquetes falsos en ambos sentidos para que el patrón resultante no se parezca al de esa web.
3. **Tamaño constante**: hace que todos los paquetes tengan el mismo tamaño, para que los pequeños no delaten nada.

DAITA se basa en **Maybenot**, un marco de código abierto para definir defensas de este tipo. Mullvad lo ayuda a financiar y lo desarrolló junto con la Universidad de Karlstad, con investigación publicada en abierto.

Limitaciones

- Tiene un coste: el tráfico falso consume ancho de banda y puede ralentizar.
- Por ahora está disponible solo en una selección de servidores, que Mullvad puede ampliar.
- Dificulta el análisis de tráfico, pero no lo hace imposible: es una reducción del riesgo, no una garantía.
- La auditoría de GotaTun no cubrió DAITA, así que esta función tiene un historial de revisión menos extenso que el túnel básico.

CAPÍTULO 12

DNS, bloqueadores, kill switch y fugas

Una VPN puede tener un túnel perfecto y aun así delatarte si algo escapa por fuera de él. Estos son los tres puntos donde suele ocurrir.

DNS dentro del túnel

Recuerda que el DNS es la agenda que revela qué webs quieres visitar. Cuando usas Mullvad, **todas tus consultas DNS pasan por el túnel cifrado** y las resuelve Mullvad en el propio servidor, en lugar de enviarse a tu operador. Si esas consultas salieran por fuera del túnel, tu operador seguiría viendo todas las webs que visitas aunque la VPN estuviera encendida. Eso es una **fuga de DNS**.

Bloqueadores de contenido

La aplicación permite activar **bloqueadores de contenido a nivel de DNS**: cuando una app o una web pide un dominio de publicidad, de rastreo o de malware, el servidor DNS responde que no existe y la petición nunca sale. Se pueden activar por categorías. Es una ayuda cómoda y funciona en todo el dispositivo, pero es una capa básica: no sustituye a un bloqueador de anuncios en el navegador ni detiene el rastreo que no depende de dominios conocidos.

El kill switch

¿Qué pasa si el túnel se cae un segundo? Sin protección, el dispositivo vuelve a enviar el tráfico por la conexión normal y revela tu IP real. El **kill switch** (interruptor de corte) evita eso: si hay problemas de conectividad con la VPN activa, la app bloquea automáticamente todo el tráfico de red hasta que el túnel vuelva. La aplicación incluye además un modo de bloqueo más estricto, para que no salga nada si la VPN no está conectada.

Otras fugas habituales

FUGA	QUÉ ES	CÓMO EVITARLA
IPv6	Tu dispositivo usa una segunda dirección que no pasa por el túnel	Usar la app oficial, que gestiona IPv6; comprobarlo con una prueba de fugas
WebRTC	El navegador puede revelar tu IP real a una web mediante una tecnología de videollamadas	Usar un navegador que lo bloquee o limite (como Mullvad Browser)
Aplicaciones fuera del túnel	Algunas apps se salen de la VPN por la configuración de la red local	Revisar la división de túnel (split tunneling) y desactivarla si no la necesitas
Conexión antes de la VPN	El dispositivo se conecta a internet antes de que la VPN arranque	Activar la conexión automática de la app y el modo de bloqueo

Mullvad ofrece en su web una **prueba de conexión** que muestra qué IP y qué DNS ven las webs. Es una buena costumbre pasarla tras instalar o cambiar la configuración.

CAPÍTULO 13

Mullvad Browser y la relación con Tor

Una VPN esconde tu IP, pero tu navegador sigue entregando mucha información sobre ti.

La huella digital del navegador

Cada navegador deja ver detalles como el tamaño de la ventana, las fuentes instaladas, el idioma, la resolución o el tipo de tarjeta gráfica. Combinados, forman una **huella digital** casi única, y una web puede reconocerte con ella sin cookies y aunque cambies de IP. Una VPN no cambia nada de esto.

Mullvad Browser

Mullvad Browser es un navegador libre y gratuito desarrollado por el **Tor Project** a petición de Mullvad. La idea es que los usuarios se parezcan lo máximo posible entre sí, para que tu huella se confunda en una multitud. Lo logra con varias medidas:

- **Huellas parecidas**: todos los usuarios presentan una configuración casi idéntica.
- **Letterboxing**: añade franjas grises alrededor de la página para que los scripts no deduzcan el tamaño exacto de tu ventana.
- **uBlock Origin** incluido, para bloquear rastreadores de terceros.
- **Modo privado por defecto**: no guarda cookies entre sesiones y aísla las cookies de terceros.
- **Sin telemetría**.

Su descripción oficial lo define como un navegador de Tor sin la red Tor. No incluye una VPN: Mullvad recomienda combinarlo con una VPN de confianza, porque el navegador por sí solo no oculta tu IP.

VPN y Tor: no es lo mismo

	VPN (MULLVAD)	RED TOR
Cuántos intermediarios	Uno (o dos con multihop), todos de la misma empresa	Tres relevos operados por voluntarios distintos
En quién confías	En el proveedor	En que los relevos no se pongan de acuerdo
Velocidad	Alta	Menor
Para qué sirve mejor	Uso diario, descargas, vídeo, proteger la red local	Anonimato fuerte en navegación y servicios específicos

Son herramientas distintas y se pueden usar a la vez, pero cada combinación tiene matices. Para el uso diario, la pareja VPN más Mullvad Browser da una protección amplia con poco esfuerzo. Cuando el anonimato es crítico, la red Tor reparte la confianza entre muchos actores independientes y suele ser la opción más adecuada.

Qué fue de Mullvad Leta

Mullvad lanzó en 2023 Leta, un buscador que actuaba como intermediario de privacidad para las búsquedas. Mullvad lo cerró el 27 de noviembre de 2025. Es un recordatorio útil de que los servicios cambian: comprueba siempre qué sigue disponible.

CAPÍTULO 14

Limitaciones y lo que una VPN no puede hacer

Una guía honesta tiene que decir dónde termina la protección.

Hay que confiar en el proveedor

Todo el tráfico pasa por Mullvad. Las auditorías, el código abierto, los servidores sin disco y la redada de 2023 son motivos para confiar, pero no son pruebas definitivas. Una VPN cambia **en quién confías**; no elimina la confianza. Mullvad intenta que confiar en ella sea lo más barato posible, al no saber quién eres.

La correlación de tráfico

Si un adversario puede observar a la vez tu conexión hacia el servidor y la salida del servidor hacia la web, puede comparar el momento y el volumen de los datos y deducir que son la misma comunicación, aunque todo vaya cifrado. Es un ataque muy difícil de ejecutar para un actor corriente, pero posible para quien vigila amplias partes de internet. DAITA y multihop reducen el riesgo, y no lo eliminan.

La huella del navegador y las cuentas

Si inicias sesión en tu correo, tus redes o tu banco, la web sabe quién eres con IP o sin ella. Y si tu navegador tiene una huella única, te reconocen entre sesiones. La VPN no protege de esto, por eso existe Mullvad Browser.

La IP compartida

Muchos usuarios salen a internet por la misma IP de un servidor. Eso te mezcla en una multitud, que es bueno para la privacidad, pero tiene un coste práctico: algunas webs bloquean o limitan las IP de VPN, piden más comprobaciones o impiden el acceso a ciertos servicios. Mullvad no se orienta a desbloquear plataformas de vídeo y lo dice claramente. Tampoco ofrece, desde 2023, la redirección de puertos, que retiró en mayo de 2023.

Los pagos con rastro

Si pagas con tarjeta o transferencia, tu banco o el procesador conoce el pago. Eso no revela qué haces con la VPN, pero sí que eres cliente. Para quien necesita anonimato real, elige efectivo o Monero.

No hay recuperación de cuenta

Si pierdes el número de 16 dígitos, pierdes la cuenta. Es la contrapartida de no guardar datos tuyos.

CAPÍTULO 15

Buenas prácticas

Una VPN bien configurada es mucho más fuerte que una mal usada. Este resumen reúne lo esencial.

1. **Guarda el número de cuenta** en un gestor de contraseñas y no lo compartas.
2. **Elige el método de pago según tu objetivo.** Para anonimato, efectivo o Monero; para comodidad, tarjeta.
3. **Activa los túneles resistentes a la computación cuántica** si no están ya por defecto en tu plataforma.
4. **Mantén activados el kill switch y el modo de bloqueo**, y que la app se conecte sola al arrancar.
5. **Prueba tu conexión** con la herramienta de Mullvad tras instalar y tras cambiar la configuración.
6. **Usa Mullvad Browser** o un navegador reforzado, y no inicies sesión en cuentas personales cuando quieras mantener separada tu identidad.
7. **Usa multihop o DAITA** si tu modelo de amenazas incluye a un observador de red, sabiendo que cuestan velocidad.
8. **Mantén la app al día.** Mullvad publica correcciones y mejoras con frecuencia, y la migración a GotaTun llega por actualización.
9. **No esperes que la VPN lo resuelva todo.** Es una capa dentro de un conjunto: dispositivo seguro, cuentas con autenticación fuerte y cuidado con lo que compartes.

Fuentes

Esta guía se apoya en la web oficial y el blog de Mullvad (páginas "Por qué Mullvad VPN", DAITA, Mullvad Browser y las entradas sobre OpenVPN, GotaTun y Leta), en el análisis de CyberInsider y TechRadar sobre GotaTun y su auditoría, en la cobertura de Ghacks y CyberInsider sobre el registro policial de 2023, en el artículo de AlternativeTo sobre los túneles resistentes a la computación cuántica y en la cobertura de PCWorld y CNET sobre precios y formas de pago.