

Que é realmente unha VPN

Cambia quen pode verte, non se alguén pode.

Para entendérmonos: unha VPN fai que o teu operador de internet, ou a wifi dun aeroporto, deixen de ver onde te conectas. Esa información non desaparece: pásaa á empresa da VPN, que agora si a ve. O que xa viaxaba cifrado, como o correo ou o banco, tamén ía cifrado antes. Serve para unhas poucas cousas concretas e adoita venderse coma se servise para moitas máis.

Durante anos oín falar das VPN e non lles fixen caso, igual ca cos antivirus: non uso antivirus, ou case nunca. Teño copias de todo en tres sitios, en tempo real, e moito coidado co que descargo, coas ligazóns que premo e coas webs que visito. Non é seguridade ao cen por cento, pero é o que me funciona a min. Un día vin unha oferta de VPN a pouco máis de dous euros ao mes e contrateina por curiosidade. Funciona ben, pero servíume de pouco: por exemplo, probar un servizo que daquela só abría nos Estados Unidos. Síntome máis seguro? Non. Se outra vez ma ofrecen a ese prezo, quizais a renove; se non, non. É só a miña experiencia, non demostra nada. Así que me preguntei que fai exactamente unha VPN. Así é como o entendín eu.

Imaxina que botas unha carta á caixa do correo co enderezo do destinatario ben visible. O carteiro ve a quen lla envías, aínda que non poida lela se vai pechada. Ese carteiro é o teu operador de internet. Unha VPN mete a túa carta dentro doutro sobre, dirixido a un intermediario que a abre e a reenvía. O teu carteiro de sempre xa non ve o enderezo real. Só ve que escribes a ese intermediario.

Quen controla a rede desde a que te conectas, por exemplo a wifi dun aeroporto, deixa de ver onde vas. Pero o intermediario ve agora o que vía o teu operador, e ás veces máis, porque todo o teu tráfico pasa por el. A vixilancia non desaparece: muda de mans. De aí o nome.

Ademais, case todo o que fas hoxe, como abrir o correo ou entrar no banco, xa viaxa cifrado ata o servidor de destino grazas ao cadeado do navegador. Iso ocorre con VPN e sen ela. A VPN engade protección só no primeiro tramo, ata o seu propio servidor. Desde aí o camiño é o de sempre.

Por iso hai cousas que non pode prometerte, aínda que ás veces se vendan así. Se iniciaches sesión no teu correo ou no teu banco, ese servizo sabe que es ti, con VPN ou sen ela. Tampouco garante que ninguén mire o teu tráfico: só cambia quen mira. Que a empresa diga que «non garda rexistros» é unha promesa, igual que cando unha gran plataforma di «as túas mensaxes están cifradas, non as lemos». Unha auditoría pode respaldala nun momento dado, pero segue a ser algo que confías en que se cumpra, non algo que non se poida incumplir por deseño.

E o contido dunha conversa queda igual. Se a túa aplicación de mensaxería xa cifra de extremo a extremo, a VPN non suma nada. Se non o fai, tampouco o arranza: protexe o camiño da mensaxe, non o que a aplicación ou o seu servidor fagan con ela ao chegar.

Nada disto a fai inútil. Agachar onde te conectas fronte a unha wifi pública, a un operador que quixese vender ese historial ou a un país que bloquea un servizo é un traballo real, e faino ben. A mercadotecnia, iso si, adoita prometer máis do que esa capa pode dar.

A pregunta que convén facerse, cunha VPN ou con calquera servizo que promete protexerte, non é «está cifrado?». Probablemente si, polo menos un tramo. É esta outra: en quen estou depositando a confianza que lle quítei a outro? E que me queda se resulta inxustificada?

Unha VPN, cando fai ben o seu traballo, só cambia quen é o intermediario da túa conexión. Unha app como Solo2, cuxas mensaxes non pasan por ningún servidor, quita ao intermediario da conversa. Non compiten: resollen problemas distintos.

Confundilas é un xeito moi habitual de creerse máis protexido do que se está.

Nota editorial: cando estes Cuadernos nomean empresas ou produtos, non é para acusar. Quenes os constrúen fan traballos que millóns de persoas usan e aprecian. O que sinalamos é estrutural — o modelo, non a marca. As marcas aparecen como exemplo porque son as que o lector recoñece.

Fontes e lectura adicional

- O protocolo HTTPS e o cifrado de transporte son estándares abertos, documentados publicamente pola IETF.
- Nesta mesma colección: «Cando non hai ninguén no medio» e «Non es anónimo» desenvolven, desde outros ángulos, a mesma distinción entre estrutura e promesa.

[← AnteriorNon es anónimo](#)

Lecturas recentes

- [Reflexión · 29 de xuño de 2026 Non es anónimo](#)
- [Reflexión · 27 de maio de 2026 O que unha firma non pode arranxar](#)
- [Análise · 26 de maio de 2026 Privacidade real vs aparente: as preguntas que convén facerse](#)

Leva este artigo onde o necesites.

[↓ Markdown](#) [↓ Texto plano](#) [↓ PDF](#)

O arquivo descárgase no teu dispositivo. Desde aí podes gardalo, importalo a Solo2, o compartilo onde queiras. Cuadernos no decide o destino por ti.

Selo de lacre · SHA-256 7029806dccc16077fdebaae958e3db4ef6099306733abd855125fec784bda09e

[Características](#) [Prezos](#) [Instalar](#) [Novidades](#) [Blog](#) [Pro](#) [Axuda](#) [Sobre](#) [Contacto](#)
[Transparencia](#) [Verificación](#) [Privacidade](#) [Condicións](#) [Cookies](#)

Cuadernos Lacre · Unha publicación de [Menzuri Gestión S.L.](#) ·
escrita por R.Eugenio · editada polo equipo de [Solo2](#).

Esta web non usa cookies. Todo o que carga o teu navegador está escrito ou supervisado por nós e aloxado nos nosos servidores europeos: o contador anónimo de visitas (Umami, autohospedado) e o mínimo JavaScript necesario para o selector de idioma e a túa preferencia de tema claro/escuro, que se garda no teu propio dispositivo. Sen recursos de terceiros, sen trackers, sen perfilado, sen compartir datos. Se queres seguirmos: [RSS](#).