

Què és realment una VPN

Canvia qui et pot veure, no si algú pot.

Per entendre'ns: una VPN fa que el teu proveïdor d'internet, o la Wi-Fi d'un aeroport, deixin de veure on et connectes. Aquesta informació no desapareix: la passa a l'empresa de la VPN, que ara sí que la veu. El que ja viatjava xifrat, com el correu o el banc, ja anava xifrat abans. Serveix per a unes quantes coses concretes i se sol vendre com si servís per a molt més.

Durant anys vaig sentir parlar de les VPN i no en vaig fer cas, igual que amb els antivirus: no faig servir antivirus, o gairebé mai. Tinc còpies de tot en tres llocs, en temps real, i molt de compte amb el que descarrego, amb els enllaços on clico i amb els webs que visito. No és seguretat al cent per cent, però és el que em funciona a mi. Un dia vaig veure una oferta de VPN a poc més de dos euros al mes i la vaig contractar per curiositat. Funciona bé, però m'ha servit de poc: per exemple, provar un servei que aleshores només funcionava als Estats Units. Em sento més segur? No. Si me la tornen a oferir a aquest preu, potser la renovaré; si no, no. És només la meva experiència, no demostra res. Així que em vaig preguntar què fa exactament una VPN. Així és com ho he entès jo.

Imagina que tires una carta a la bústia amb l'adreça del destinatari ben visible. El carter veu a qui la envies, encara que no pugui llegir-la si va tancada. Aquest carter és el teu operador d'internet. Una VPN fica la teva carta dins d'un altre sobre, dirigit a un intermediari que l'obre i la reenvia. El teu carter de sempre ja no veu l'adreça real. Només veu que escrius a aquell intermediari.

Qui controla la xarxa des d'on et connectes, per exemple la Wi-Fi d'un aeroport, deixa de veure on vas. Però l'intermediari veu ara el que veia el teu operador, i de vegades més, perquè tot el teu trànsit passa per ell. La vigilància no desapareix: canvia de mans. D'aquí el nom.

A més, gairebé tot el que fas avui, com obrir el correu o entrar al banc, ja viatja xifrat fins al servidor de destinació gràcies al cademat del navegador. Això passa amb VPN i sense. La VPN afegeix protecció només en el primer tram, fins al seu propi servidor. Des d'allà el camí és el de sempre.

Per això hi ha coses que no et pot prometre, encara que de vegades es vengui així. Si has iniciat sessió al teu correu o al teu banc, aquest servei sap que ets tu, amb VPN o sense. Tampoc garanteix que ningú miri el teu trànsit: només canvia qui mira. Que l'empresa digui que «no guarda registres» és una promesa, igual que quan una gran plataforma diu «els teus missatges estan xifrats, no els llegim». Una auditoria pot avalar-ho en un moment donat, però continua sent una cosa que confies que es compleixi, no una cosa que no es pugui incomplir per disseny.

I el contingut d'una conversa queda igual. Si la teva aplicació de missatgeria ja xifra d'extrem a extrem, la VPN no hi suma res. Si no ho fa, tampoc ho arregla: protegeix el camí del missatge, no el que l'aplicació o el seu servidor en facin en arribar.

Res d'això no la fa inútil. Amagar on et connectes davant d'una Wi-Fi pública, d'un operador que vulgui vendre aquest historial o d'un país que bloqueja un servei és una feina real, i la fa bé. El màrqueting, això sí, sol prometre més del que aquesta capa tècnica pot donar.

La pregunta que convé fer-se, amb una VPN o amb qualsevol servei que promet protegir-te, no és «està xifrat?». Probablement sí, almenys un tram. És aquesta altra: en qui estic dipositant la confiança que he tret a un altre? I què em queda si resulta injustificada?

Una VPN, quan fa bé la seva feina, només canvia qui és l'intermediari de la teva connexió. Una aplicació com Solo2, els missatges de la qual no passen per cap servidor, treu l'intermediari de la conversa. No competeixen: resolen problemes diferents.

Confondre-les és una manera molt habitual de creure's més protegit del que realment s'està.

Nota editorial: quan aquests Cuadernos nomenen empreses o productes, no és per acusar. Els qui els construeixen fan treballs que milions de persones usen i aprecien. El que assenyalen és estructural — el model, no la marca. Les marques apareixen com a exemple perquè són les que el lector reconeix.

Fonts i lectura adicional

- El protocol HTTPS i el xifratge de transport són estàndards oberts, documentats públicament per la IETF.
- En aquesta mateixa col·lecció: «Quan no hi ha ningú al mig» i «No ets anònim» desenvolupen, des d'altres angles, la mateixa distinció entre estructura i promesa.

[← Anterior](#)[No ets anònim](#)

Lectures recents

- [Reflexió · 29 de juny del 2026](#) [No ets anònim](#)
- [Reflexió · 27 de maig del 2026](#) [El que una signatura no pot arreglar](#)
- [Anàlisi · 26 de maig del 2026](#) [Privadesa real vs aparent: les preguntes que convé fer-se](#)

Emporta't aquest article on el necessitis.

[↓ Markdown](#) [↓ Text pla](#) [↓ PDF](#)

L'arxiu es descarrega al teu dispositiu. Des d'allà pots guardar-lo, importar-lo a Solo2, o compartir-lo on vulguis. Cuadernos no decideix el destí per tu.

Segell de lacre · SHA-256 33e849f0a465d43bd72fb512e8fe3b2e3fbf148d7266013f9a4340171cb1dbc3

[Característiques](#) [Preus](#) [Instal·lar](#) [Novetats](#) [Blog](#) [Pro](#) [Ajuda](#) [Sobre](#) [Contacte](#)
[Transparència](#) [Verificació](#) [Privacitat](#) [Condicions](#) [Galetes](#)

Cuadernos Lacre · Una publicació de [Menzuri Gestión S.L.](#) ·
escrita per R.Eugenio · editada per l'equip de [Solo2](#).

Aquest web no utilitza galetes. Tot el que carrega el teu navegador està escrit o supervisat per nosaltres i allotjat als nostres servidors europeus: el comptador anònim de visites (Umami, autoallotjat) i el mínim JavaScript necessari per al selector d'idioma i la teva preferència de tema clar/fosc, que es desa al teu propi dispositiu. Sense recursos de tercers, sense traquejadors, sense perfilat, sense compartir dades. Si vols seguir-nos: [RSS](#).