

Qué es realmente una VPN

Cambia quién puede verte, no si alguien puede.

Para entendernos: una VPN hace que tu operador de internet, o el wifi de un aeropuerto, dejen de ver adónde te conectas. Esa información no desaparece, la pasa a la empresa de la VPN, que ahora sí la ve. Lo que ya iba cifrado, como el correo o el banco, iba cifrado también antes. Sirve para unas pocas cosas concretas y suele venderse como si sirviera para muchas más.

Durante años oí hablar de las VPN y no les hice caso, igual que con los antivirus: no uso antivirus, o casi nunca. Tengo copias de todo en tres sitios, en tiempo real, y mucho cuidado con lo que descargo, con los enlaces que pulso y con las webs que visito. No es seguridad al cien por cien, pero es lo que me funciona a mí. Un día vi una oferta de VPN a poco más de dos euros al mes y la contraté por curiosidad. Funciona bien, pero me ha servido para poco: por ejemplo, probar un servicio que entonces solo abría en Estados Unidos. ¿Me siento más seguro? No. Si otra vez me la ofrecen a ese precio, quizá la renueve; si no, no. Es solo mi experiencia, no demuestra nada. Así que me pregunté qué hace exactamente una VPN. Así es como lo he entendido yo.

Imagina que echas una carta al buzón con la dirección del destinatario bien visible. El cartero ve a quién se la envías, aunque no pueda leerla si va cerrada. Ese cartero es tu operador de internet. Una VPN mete tu carta dentro de otro sobre, dirigido a un intermediario que la abre y la reenvía. Tu cartero de siempre ya no ve la dirección real. Solo ve que escribes a ese intermediario.

Quien controla la red desde la que te conectas, por ejemplo el wifi de un aeropuerto, deja de ver adónde vas. Pero el intermediario ve ahora lo que veía tu operador, y a veces más, porque todo tu tráfico pasa por él. La vigilancia no desaparece: cambia de manos. De ahí el nombre.

Además, casi todo lo que haces hoy, como abrir el correo o entrar en el banco, ya viaja cifrado hasta el servidor de destino gracias al candado del navegador. Eso ocurre con VPN y sin ella. La VPN añade protección solo en el primer tramo, hasta su propio servidor. Desde ahí el camino es el de siempre.

Por eso hay cosas que no puede prometerte, aunque a veces se vendan así. Si has iniciado sesión en tu correo o en tu banco, ese servicio sabe que eres tú, con VPN o sin ella. Tampoco garantiza que nadie mire tu tráfico: solo cambia quién mira. Que la empresa diga que «no guarda registros» es una promesa, igual que cuando una gran plataforma dice «tus mensajes están cifrados, no los leemos». Una auditoría puede respaldarla en un momento dado, pero sigue siendo algo que confías en que se cumpla, no algo que no se pueda incumplir por diseño.

Y el contenido de una conversación queda igual. Si tu aplicación de mensajería ya cifra de extremo a extremo, la VPN no suma nada. Si no lo hace, tampoco lo arregla: protege el camino del mensaje, no lo que la aplicación o su servidor hagan con él al llegar.

Nada de esto la hace inútil. Esconder adónde te conectas frente a un wifi público, a un operador que quisiera vender ese historial o a un país que bloquea un servicio es un trabajo real, y lo hace bien. El marketing, eso sí, suele prometer más de lo que esa capa puede dar.

La pregunta que conviene hacerse, con una VPN o con cualquier servicio que promete protegerte, no es «¿está cifrado?». Probablemente sí, al menos un tramo. Es esta otra: ¿en quién estoy depositando la confianza que le he

quitado a otro? ¿Y qué me queda si resulta injustificada?

Una VPN, cuando hace bien su trabajo, solo cambia quién es el intermediario de tu conexión. Una app como Solo2, cuyos mensajes no pasan por ningún servidor, quita al intermediario de la conversación. No compiten: resuelven problemas distintos.

Confundirlas es una forma muy habitual de creerse más protegido de lo que se está.

Nota editorial: cuando este Cuaderno nombra empresas o productos, no es para acusar. Quienes los construyen hacen trabajos que millones de personas usan y aprecian. Lo que señalamos es estructural — el modelo, no la marca. Las marcas aparecen como ejemplo porque son las que el lector reconoce.

Fuentes y lectura adicional

- El protocolo HTTPS y el cifrado de transporte son estándares abiertos, documentados públicamente por la IETF.
- En esta misma colección: «Cuando no hay nadie en medio» y «No eres anónimo» desarrollan, desde otros ángulos, la misma distinción entre estructura y promesa.

[← Anterior](#)[No eres anónimo](#)

Lecturas recientes

- [Reflexión · 29 de junio de 2026](#) [No eres anónimo](#)
- [Reflexión · 27 de mayo de 2026](#) [Lo que una firma no puede arreglar](#)
- [Análisis · 26 de mayo de 2026](#) [Privacidad real vs aparente: las preguntas que conviene hacerse](#)

Llévate este artículo donde lo necesites.

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

El archivo se descarga a tu dispositivo. Desde ahí puedes guardarlo, importarlo a Solo2, o compartirlo donde quieras. Cuadernos no decide el destino por ti.

Sello de lacre · SHA-256 433d6a2ce26e1741352337e73d278952fd95bf016bdf3b51a830ac69ca0806f2

[Características](#) [Precios](#) [Instalar](#) [Novedades](#) [Blog](#) [Pro](#) [Ayuda](#) [Sobre](#) [Contacto](#)
[Transparencia](#) [Verificación](#) [Privacidad](#) [Condiciones](#) [Cookies](#)

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

Esta web no usa cookies. Todo lo que carga tu navegador está escrito o supervisado por nosotros y alojado en nuestros servidores europeos: el contador anónimo de visitas (Umami, autohospedado) y el mínimo JavaScript necesario para el selector de idioma y tu preferencia de tema claro/oscuro, que se guarda en tu propio dispositivo. Sin recursos de empresas externas, sin rastreadores, sin perfilado, sin compartir datos. Si quieres seguirnos: [RSS](#).