

O que é realmente uma VPN

Muda quem te pode ver, não se alguém pode.

Para nos entendermos: uma VPN faz com que o teu fornecedor de internet, ou o Wi-Fi de um aeroporto, deixem de ver onde te ligas. Essa informação não desaparece: passa para a empresa da VPN, que agora a vê. O que já viajava cifrado, como o correio ou o banco, ia cifrado também antes. Serve para algumas coisas concretas e costuma ser vendida como se servisse para muito mais.

Durante anos ouvi falar de VPNs e não lhes dei importância, tal como com os antivírus: não uso antivírus, ou quase nunca. Tenho cópias de tudo em três locais, em tempo real, e muito cuidado com o que descarrego, com as ligações em que clico e com as páginas que visito. Não é uma segurança a cem por cento, mas é o que funciona para mim. Um dia vi uma oferta de VPN a pouco mais de dois euros por mês e contratei-a por curiosidade. Funciona bem, mas serviu-me de pouco: por exemplo, para testar um serviço que na altura só abria nos Estados Unidos. Sinto-me mais seguro? Não. Se me oferecerem outra vez a esse preço, talvez renove; se não, não. É apenas a minha experiência, não prova nada. Por isso perguntei a mim próprio o que faz exatamente uma VPN. Foi assim que eu entendi.

Imagina que deitas uma carta no marco do correio com a morada do destinatário bem visível. O carteiro vê para quem a envias, mesmo que não a possa ler se for fechada. Esse carteiro é o teu operador de internet. Uma VPN mete a tua carta dentro de outro envelope, dirigido a um intermediário que a abre e a reenvia. O teu carteiro habitual já não vê a morada real. Apenas vê que escreves àquele intermediário.

Quem controla a rede a partir da qual te ligas, por exemplo o Wi-Fi de um aeroporto, deixa de ver para onde vais. Mas o intermediário vê agora o que o teu operador via, e por vezes mais, porque todo o teu tráfego passa por ele. A vigilância não desaparece: muda de mãos. Daí o nome.

Além disso, quase tudo o que fazes hoje, como abrir o correio ou aceder ao banco, já viaja cifrado até ao servidor de destino graças ao cadeado do navegador. Isso acontece com VPN e sem ela. A VPN acrescenta proteção apenas no primeiro troço, até ao seu próprio servidor. A partir daí o caminho é o habitual.

Por isso há coisas que não te pode prometer, embora por vezes se venda dessa forma. Se iniciaste sessão no teu correio ou no teu banco, esse serviço sabe que és tu, com VPN ou sem ela. Também não garante que ninguém olhe para o teu tráfego: apenas muda quem olha. A empresa dizer que «não guarda registos» é uma promessa, tal como quando uma grande plataforma diz «as tuas mensagens estão cifradas, nós não as lemos». Uma auditoria pode confirmá-lo num determinado momento, mas continua a ser algo que confias que se cumpra, não algo que não possa ser violado por desenho.

E o conteúdo de uma conversa fica igual. Se a tua aplicação de mensagens já cifra de ponta a ponta, a VPN não acrescenta nada. Se não o faz, também não o resolve: protege o percurso da mensagem, não o que a aplicação ou o seu servidor façam com ela ao chegar.

Nada disto a torna inútil. Esconder onde te ligas perante um Wi-Fi público, uma operadora que queira vender esse histórico ou um país que bloqueia um serviço é um trabalho real, e ela fá-lo bem. O marketing, isso sim, costuma prometer mais do que essa camada técnica pode oferecer.

A pergunta que convém fazer, perante uma VPN ou qualquer serviço que prometa proteger-te, não é «está cifrado?». Provavelmente sim, pelo menos num troço. É esta outra: em quem estou a depositar a confiança que retirei a outro? E o que me sobra se essa confiança se revelar injustificada?

Uma VPN, quando faz bem o seu trabalho, apenas muda quem é o intermediário da tua ligação. Uma aplicação como o Solo2, cujas mensagens não passam por nenhum servidor, retira o intermediário da conversa. Não concorrem: resolvem problemas diferentes.

Confundi-las é uma forma muito habitual de alguém se crer mais protegido do que realmente está.

Nota editorial: quando estes Cuadernos nomeiam empresas ou produtos, não é para acusar. Aqueles que os constroem fazem trabalhos que milhões de pessoas usam e apreciam. O que assinalamos é estrutural — o modelo, não a marca. As marcas aparecem como exemplo porque são as que o leitor reconhece.

Fontes e leitura adicional

- O protocolo HTTPS e a cifragem de transporte são normas abertas, documentadas publicamente pela IETF.
- Nesta mesma coleção: «Quando não há ninguém no meio» e «Não és anónimo» desenvolvem, sob outros ângulos, a mesma distinção entre estrutura e promessa.

[← Anterior](#)[Não és anónimo](#)

Leituras recentes

- [Reflexão · 29 de junho de 2026 Não és anónimo](#)
- [Reflexão · 27 de maio de 2026 Lo que una firma no puede arreglar](#)
- [Análise · 26 de maio de 2026 Privacidade real vs aparente: as perguntas que convém fazer-se](#)

Leve este artigo para onde precisar.

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

O arquivo é descarregado no seu dispositivo. A partir daí, pode guardá-lo, importá-lo no Solo2 ou partilhá-lo onde quiser. Cuadernos não decide o destino por si.

Selo de lacre · SHA-256 befe22e1bc1400080ef2c91bd1ea46502dbd89455be85598a14a1060504d632d

[Funcionalidades](#) [Preços](#) [Instalar](#) [Novidades](#) [Blog](#) [Pro](#) [Ajuda](#) [Sobre](#) [Contacto](#)
[Transparência](#) [Verificação](#) [Privacidade](#) [Condições](#) [Cookies](#)

Cuadernos Lacre · Uma publicação da [Menzuri Gestión S.L.](#) ·
escrita por R.Eugenio · editada pela equipa do [Solo2](#).

Este site não utiliza cookies. Tudo o que o teu navegador carrega é escrito ou supervisionado por nós e hospedado em nossos servidores europeus: o contador de visitas anónimo (Umami, auto-hospedado) e o mínimo de JavaScript necessário para o seletor de idioma e a tua preferência de tema claro/escuro, que é guardada no teu próprio dispositivo. Sem recursos de terceiros, sem rastreadores, sem criação de perfis, sem compartilhamento de dados. Se nos quiseres seguir: [RSS](#).