**1. FUNCIONAMENTO DA VPN**

Uma VPN (rede privada virtual) é a maneira mais fácil e eficaz para as pessoas protegerem seu tráfego na Internet e esconderem suas identidades online. Ao se conectar a um servidor VPN seguro, seu tráfego de Internet passa por um **túnel criptografado que ninguém pode ver**; incluindo hackers, governos e seu provedor de serviços de Internet.

**Os consumidores usam VPNs** para manter sua actividade online privada e garantir o acesso a sites e serviços que de outra forma poderiam ser restritos.

**As empresas utilizam VPNs** para conectar funcionários distantes como se todos utilizassem a mesma rede local em um escritório central, mas com menos benefícios para os usuários do que com uma VPN pessoal.

**2. BENEFÍCIOS E VANTAGENS DE UMA VPN**

**2.1. Altere sua localização**

Usando uma VPN **muda seu endereço IP**, o número único que o identifica e sua localização no mundo. Com um novo endereço IP, você pode navegar na Internet como se estivesse no Reino Unido, Alemanha, Canadá, Japão ou praticamente em qualquer país, se o serviço VPN tiver servidores lá.

**2.2. Proteja sua privacidade**

Alterar seu endereço IP com uma Rede Privada Virtual ajuda a **esconder sua identidade** de sites, aplicativos e serviços que querem rastreá-lo. As boas VPNs também escondem sua atividade de seu provedor de Internet, operadora móvel e qualquer outra pessoa que possa estar tentando invadir a sua privacidade, graças a uma camada criptografia forte.

**2.3. Aumente sua segurança**

O uso de uma VPN o **protege contra falhas de segurança** de muitas formas, incluindo ataques de sniffing, man-in-the-middle e redes Wi-Fi rogue. Viajantes, trabalhadores remotos e todos os tipos de indivíduos em movimento usam uma VPN sempre que estão em uma rede não confiável como uma rede [Wi-Fi pública gratuita](https://www.expressvpn.com/pt/what-is-vpn/wifi-vpn).

**3. QUANDO DEVO USAR UMA VPN?**

Se a privacidade é importante para você, você deve usar uma VPN **sempre que se conectar à Internet**. Um aplicativo VPN roda em segundo plano no seu dispositivo para que ele não atrapalhe enquanto você usa outros aplicativos, faz streaming de conteúdos e navega na Internet. E você terá paz de espírito sabendo que sua privacidade está sempre protegida.

Mas aqui estão algumas situações nas quais uma VPN é especialmente útil:

**3.1. Viajando**

Explorar o mundo não significa que você tenha que mudar a maneira como você usa a Internet. Uma VPN permite utilizar a Internet como se você ainda estivesse em seu país de origem, não importa a distância que você viaje.

**3.2. Na sua folga**

Desfrute do seu tempo de lazer sem restrições ou outros limites impostos pelo seu provedor de Internet ou rede Wi-Fi local. O que quer que você goste de fazer online, faça-o com tranquilidade.

**3.3. No Wi-Fi público**

A conexão a hotspots [Wi-Fi públicos](https://www.expressvpn.com/pt/what-is-vpn/wifi-vpn), como os de cafés, aeroportos e parques, pode deixar suas informações particulares vulneráveis. O uso de uma VPN em seus dispositivos mantém você seguro através de uma criptografia forte.

**3.4. Ao jogar**

Jogue com amigos em outros países, proteja-se de ataques DDoS e reduza o ping e o lag geral conectando-se a um servidor VPN que está mais próximo do servidor do jogo.

**3.5. Compartilhando arquivos**

O compartilhamento de arquivos P2P geralmente significa que estranhos podem ver seu endereço IP e possivelmente rastrear seus downloads. Uma VPN mantém a privacidade do seu endereço IP, permitindo que você faça downloads com maior anonimato.

**3.6. Fazendo compras**

Algumas lojas online mostram preços diferentes para pessoas de diferentes países. Com uma VPN, você pode encontrar as [melhores ofertas ao redor do mundo](https://www.expressvpn.com/pt/vpn-service/online-shopping-vpn), não importa de onde esteja comprando.

**4. COMO FUNCIONA UMA VPN?**

Para compreender como uma VPN funciona, facilita primeiro entender como a sua conexão de Internet funciona sem uma VPN.

**4.1. Sem uma VPN**

Quando você acessa um site sem VPN, você está sendo conectado a esse site através de seu provedor de serviços de Internet, ou ISP. O ISP atribui a você um **endereço IP único** que pode ser usado para identificá-lo ao site. Como seu provedor está cuidando de todo o seu tráfego, ele pode ver quais sites você visita. E sua actividade pode ser vinculada a você por esse endereço IP único.

**4.2. Com uma VPN**

Quando você se conecta à Internet com uma VPN, o aplicativo VPN em seu dispositivo (também chamado de **cliente VPN**) estabelece uma conexão segura com um **servidor VPN**. Seu tráfego ainda passa pelo seu provedor, mas seu provedor não pode mais ler seus dados ou ver seu destino final. Os sites que você visita não podem mais ver seu endereço IP original, apenas o endereço IP do servidor VPN, que é compartilhado por muitos outros usuários e muda regularmente.

**5. CONCEITOS-CHAVE RELACIONADOS À VPN PARA SEU FUNCIONAMENTO E OS BENEFÍCIOS QUE ELA PROPORCIONA**

**5.1. Proxying**

O servidor VPN actua como um **proxy**, ou stand-in, para sua atividade na internet: Em vez de seu endereço IP e localização reais, os sites que você visita só verão o endereço IP e a localização do servidor VPN, o que o torna mais anônimo na Internet.

**5.2. Autenticação**

Estabelecer uma conexão segura é um problema complicado resolvido por uma matemática inteligente em um processo chamado **autenticação**.

Uma vez autenticados, o cliente VPN e o servidor VPN podem ter certeza de que estão conversando um com o outro e com ninguém mais.

**5.3. Tunelamento**

As VPNs também protegem a conexão entre cliente e servidor com tunelamento e criptografia.

O tunelamento é um processo pelo qual cada pacote de dados é **encapsulado** dentro de outro pacote de dados. Isto torna a leitura mais difícil para terceiros.

**5.4. Criptografia**

Os dados dentro do túnel também são **criptografados** de tal forma que somente o destinatário pretendido pode descriptografá-los. Isto mantém o conteúdo de seu tráfego na Internet completamente escondido, mesmo de seu provedor de serviços de Internet.

**6. PROTOCOLOS VPN**

Os protocolos VPN são os **métodos** pelos quais seu dispositivo se conecta ao servidor VPN. Alguns protocolos são melhores para a **velocidade**, outros são melhores para a **segurança** e alguns simplesmente funcionam melhor sob certas condições de rede.

**O ExpressVPN é uma das VPNs mais seguras e velozes disponíveis**, mas sua única desvantagem sempre foi o preço. [**Ele sempre oferece descontos**](https://pt.vpnmentor.com/?Track_link=MjY0MjR8&vid=26424&target=ShortCodeAffiliateLink_26424_vendor_263954&pageid=26424&type=vendor&org_referer=https://pt.vpnmentor.com/reviews/expressvpn/?exp_id=1196&exp_var=0&reviews_ftc_no_ratings_all=0&ve=1&pageview_id=1|LI8F7PSTK711Q&clickout_id=1|LI8F7PSTK711Q|1|26424) que o tornam mais acessível, mas há outras VPNs decentes oferecendo recursos de segurança similares por preços muito menores.

Além de oferecer um conjunto padrão de protocolos, a ExpressVPN desenvolveu o [Lightway](https://www.expressvpn.com/pt/lightway) para superá-los em velocidade, confiabilidade e segurança. Experimente agora mesmo. [Saiba mais sobre o Lightway](https://www.expressvpn.com/pt/blog/lightway-protocol-beta/).

A ExpressVPN escolhe automaticamente o melhor protocolo para sua rede, mas você também pode escolher um manualmente.

Os protocolos VPN populares em uso hoje em dia incluem:

﻿6.1. OpenVPN

﻿6.2. IKEv2

6.3. L2TP / IPsec

﻿6.4. PPTP

﻿6.5. WireGuard

6.6. SSTP

**7. TIPOS DE VPN**

**7.1. VPN Comercial**

Uma VPN comercial, também chamada de VPN pessoal ou VPN de consumo, é um serviço privado oferecido diretamente aos usuários, geralmente mediante o pagamento de uma taxa.

A ExpressVPN é este tipo de serviço de VPN, pois atende diretamente às necessidades de privacidade de seus clientes.

**7.2. VPN Corporativa**

Uma VPN corporativa, também chamada de VPN empresarial, permite que os funcionários remotos de uma organização se conectem com segurança à Internet como se estivessem fisicamente presentes no escritório.

Ao contrário das VPNs comerciais, no entanto, as VPNs corporativas são destinadas a proteger a privacidade da empresa e não necessariamente do indivíduo.

**7.3. VPN de configuração pessoal**

Alguns especialistas em tecnologia e pessoas que gostam de fazer as coisas independentemente optam por montar sua própria VPN usando seu próprio equipamento.  
  
As VPNs de configuração pessoais, no entanto, não oferecem a protecção de endereços IP compartilhados, localização de servidores em vários países, ou muitas outras características desfrutadas por usuários de VPNs comerciais.

Existe quatro componentes básicos para a implementação de uma VPN baseada na Internet: a Internet, gateways seguros, servidores com políticas de segurança e certificados de autenticidade.

Para começar, você vai precisar de um cliente VPN, um servidor VPN e um roteador de VPN. O cliente, disponível para download, conecta você a servidores em todo o mundo, para que os funcionários possam acessar a rede da sua empresa de pequeno porte em qualquer lugar.

**Como as VPNs funcionam?**

Sua VPN **redireciona todo o seu tráfego de internet através de um de seus servidores,** onde ele é criptografado. Por exemplo, você pode estar no Brasil e se conectar a um servidor nos EUA. A VPN enviará seu tráfego do Brasil para os EUA, totalmente criptografado. Por ele estar criptografado, seu provedor de internet não poderá mais ver sua atividade online e seus locais acessados, ou mesmo rastreá-lo.

Em seguida, **seu servidor VPN encaminhará seu tráfego para o site que você está acessando**. O site verá o servidor VPN como a origem do seu tráfego, em vez do seu dispositivo. Isso significa que ele também **vê o endereço IP do seu servidor VPN, em vez do seu IP.** As **[melhores VPNs](https://tr.vpn-mentors.com/" \t "_blank)** usam milhares de servidores e atualizam seus endereços IP regularmente, para que os sites não tenham tempo suficiente de bloqueá-los. E isso significa que você permanece totalmente privado e indetectável.

**Como uma VPN garante minha privacidade?**

As VPNs se encarregam de muitas informações confidenciais, portanto, **elas devem contar com políticas de privacidade robustas e medidas de segurança sólidas.**Alguns recursos de segurança parecem idênticos, mas têm funções muito diferentes.

Por exemplo, apesar da crença popular, os **vazamentos de DNS e IP**não são a mesma coisa. Informar-se é essencial. Além disso, algumas VPNs não são confiáveis, portanto, é importante tomar cuidado para escolher uma opção que seja confiável e segura.

As VPNs confiáveis oferecem diversos recursos de proteção à privacidade, como:

**Política antilogs (no-logs policy)**

**Políticas antilogs robustas impedem que provedores de VPN registrem suas atividades de navegação.** Se elas não registram suas informações, não são capazes de divulgá-las para agências de vigilância governamental, mesmo que sejam solicitadas a fazê-lo. Isso também significa que, caso a VPN seja comprometida, hackers não poderão obter nenhuma de suas informações a partir dos servidores VPN.

**Proteção contra vazamento de DNS (DNS leak protection)**

Sempre que você acessa um site, seu computador envia uma solicitação a um servidor DNS para saber o endereço IP do site. Normalmente, essa solicitação chega aos servidores DNS do seu provedor de internet, revelando suas atividades de navegação para ele.

Quando você está conectado a uma VPN, suas solicitações de DNS são redirecionadas para os servidores DNS da sua VPN. Às vezes, no entanto, seu dispositivo pode redirecionar suas solicitações de volta ao seu provedor de internet sem que você saiba. Em termos simples, a proteção contra vazamento de DNS impede que isso aconteça.

**Proteção contra vazamento de IPv6 (IPv6 leak protection)**

Embora o IPv6 esteja disponível atualmente, quase todas as VPNs ainda usam endereços IPv4. Isso gera potencial para uma grave violação de segurança.

Caso seu provedor de internet ofereça suporte a IPv6 e você acesse um site que também seja compatível com ele, seu tráfego para esse site será redirecionado através do seu provedor de internet, e não da sua VPN. Isso revelará suas atividades ao seu provedor — e sua localização real para o site.

**VPNs confiáveis desativam o tráfego IPv6 para proteger você desses vazamentos.** Você ainda poderá acessar sites com IPv6 habilitado, mas o fará usando um endereço IPv4.

**2 MELHORES VPNS PARA INICIANTES**

Tenho usado VPNs há anos e já testei minha cota de serviços pouco confiáveis e obscuros. Durante minha missão para me proteger online, também encontrei alguns serviços excelentes que recomendo com louvor.

[**1. ExpressVPN – seguro, rápido e flexível**](https://pt.vpn-mentors.com/?Track_link=MjY0MjR8&dl=what_is_vpn&vid=26424&target=ShortCodeAffiliateLink_1079017_popular_295363&pageid=1079017&type=popular&org_referer=https://pt.vpn-mentors.com/popular/o-que-e-vpn-e-por-que-voce-precisa-de-uma/?keyword=vpn%20o%20que%20%c3%a9&geo=1032063&device=&ad=569676414633&cq_src=google_ads&cq_cmp=759248779&cq_term=vpn%20o%20que%20%c3%a9&cq_plac=&cq_net=g&cq_plt=gp&gclid=cj0kcqjw98ujbhcgarisad7qeahe1lsm1xjtwipnphkziywpxcmzs-tkmjlwfiexv16oj5_sb1kaouwaaqmoealw_wcb&ve=1&pageview_id=1|LI8GDGMNFTW1N&clickout_id=1|LI8GDGMNFTW1N|1|26424)

O [ExpressVPN](https://pt.vpn-mentors.com/?Track_link=MjY0MjR8&dl=what_is_vpn&vid=26424&target=ShortCodeAffiliateLink_1079017_popular_295364&pageid=1079017&type=popular&org_referer=https://pt.vpn-mentors.com/popular/o-que-e-vpn-e-por-que-voce-precisa-de-uma/?keyword=vpn%20o%20que%20%c3%a9&geo=1032063&device=&ad=569676414633&cq_src=google_ads&cq_cmp=759248779&cq_term=vpn%20o%20que%20%c3%a9&cq_plac=&cq_net=g&cq_plt=gp&gclid=cj0kcqjw98ujbhcgarisad7qeahe1lsm1xjtwipnphkziywpxcmzs-tkmjlwfiexv16oj5_sb1kaouwaaqmoealw_wcb&ve=1&pageview_id=1|LI8GDGMNFTW1N&clickout_id=1|LI8GDGMNFTW1N|1|26424" \t "_blank) oferece o recurso de tunelamento dividido (split tunneling), que é essencial se você trabalha em home office com dispositivos wireless.

O tunelamento dividido permite escolher quais atividades serão retransmitidas através da sua VPN, e quais utilizarão seu endereço IP local. Usei o recurso para permanecer conectado aos meus dispositivos na rede, como minha impressora wireless, ao mesmo tempo mantendo meu tráfego de internet seguro.

Os servidores do ExpressVPN são otimizados para altas velocidades, portanto, você não enfrentará problemas enquanto navega ou usa a web em geral.

E ele também é rápido. Testei os servidores do ExpressVPN para conferir seu desempenho. Desta vez, minha velocidade de base foi a seguinte: 3 ms de ping, 22.13 Mbps de download e 17.13 Mbps de upload.

[**2. CyberGhost – otimizado, seguro e confiável**](https://pt.vpn-mentors.com/?Track_link=MTI0NTJ8&dl=what_is_vpn&vid=12452&target=ShortCodeAffiliateLink_1079017_popular_295366&pageid=1079017&type=popular&pageview_id=1|LI8GDGMNFTW1N&clickout_id=1|LI8GDGMNFTW1N|1|12452)

O [CyberGhost](https://pt.vpn-mentors.com/?Track_link=MTI0NTJ8&dl=what_is_vpn&vid=12452&target=ShortCodeAffiliateLink_1079017_popular_295367&pageid=1079017&type=popular&pageview_id=1|LI8GDGMNFTW1N&clickout_id=1|LI8GDGMNFTW1N|1|12452" \t "_blank) é uma ótima opção se você é iniciante no mundo das VPNs, pois seus apps são muito simples de instalar e usar. Não precisei alterar nenhuma configuração antes de me conectar: basta instalar, fazer login e pronto!

Mas não se engane – ele também é altamente customizável. Escondido no menu de configurações avançadas, descobri que é possível alterar seu DNS, trocar de protocolo e configurar regras customizadas.

O CyberGhost opera uma enorme rede. Há mais de 9.388 servidores em 91 países. Testei-o durante férias recentes e descobri que isso é muito útil, pois sempre havia um servidor local rápido próximo de onde eu estava ficando. Não precisei sofrer com quedas de velocidade ao me conectar a uma localização distante. Meus colegas reportaram resultados similares.

Decidi testar o CyberGhost novamente ao chegar em casa. Minha velocidade de base era a seguinte: 37 ms de ping, 19.22 Mbps de download e 17.24 Mbps de upload.