**O que são vpns?**

1. **O que é e como funciona uma VPN?**

A VPN é uma ferramenta que possibilita se conectar à Internet de maneira segura e confidencial, e pode ser instalada em dispositivos como computadores, tablets e celulares. Ao acessar a web com o recurso, os dados enviados e recebidos são redirecionados para o servidor criptografados, e assim, não podem ser lidos caso alguém tente interceptá-los.  
Além disso, a identidade do usuário e sua localização também são protegidos porque a VPN oculta o IP pessoal, fornecendo outro endereço para disfarçar a verdadeira origem do acesso. Dessa forma, é possível navegar anonimamente pela web e impedir que as atividades online possam ser rastreadas por terceiros. O recurso ainda permite a conexão remota a servidores em outros países, fazendo parecer que o IP está localizado em uma região diferente.

Alguns usuários ainda utilizam VPN para navegar na Internet como se estivessem em outros países, podendo acessar conteúdos que não estão disponíveis no Brasil, como o catálogo americano da Netflix, Amazon Prime Vídeo e Hulu. Além disso, é possível ter acesso a jogos que ainda não foram lançados no país, porque os servidores de VPNs estão distribuídos no mundo inteiro. No entanto, essas práticas não são recomendadas e podem trazer riscos aos usuários.  
  
**2. Quais são as vantagens de usar VPN?**As vantagens do uso de uma VPN são o aumento da privacidade e a prevenção contra ataques virtuais, mantendo senhas de bancos e de cartão de crédito, por exemplo, longe dos olhos de hackers e criminosos cibernéticos. Também fica mais seguro acessar redes de Wi-Fi públicas como as que são oferecidas nos cafés, shoppings, ônibus e aeroportos.  
No caso das empresas, a VPN contribui para que funcionários acessem informações na rede local da companhia de forma segura, mesmo que estejam fisicamente distantes. A medida contribui para reduzir custos com um possível vazamento de dados sigilosos. Em 2019, o Brasil perdeu mais de R$ 80 bilhões com ataques cibernéticos, estima o levantamento mais recente da União Internacional de Telecomunicações (ITU, na sigla em inglês), órgão da Organização das Nações Unidas (ONU).

**3. Usar VPN é seguro?**A segurança da VPN dependerá da qualidade do serviço prestado pelas empresas que fornecem o recurso. É importante lembrar que, ao optar por uma companhia que oferece a VPN, o usuário está compartilhando seus dados. Ou seja, nenhum serviço oferece 100% de anonimato. Assim, a melhor maneira de acessar uma VPN com segurança é escolher prestadores de serviços que têm credibilidade no mercado e utilizem ferramentas de proteção contra malwares.

## Portanto, o uso de uma VPN não dispensa o usuário de se preocupar com o seu nível de exposição online e de continuar a usar em seus dispositivos outras medidas de seguranças, como o firewall e antivírus. 4. Quais são os riscos de usar VPN?

Alguns serviços gratuitos de VPN podem monitorar as atividades dos usuários e usar seu acesso para redirecionar anúncios de seus próprios produtos ou de outros anunciantes. Geralmente, as empresas costumam deixar explícito em suas políticas de privacidade se coletam dados dos clientes. Existem também diversas denúncias de desvio de banda larga dos usuários e comercialização do perfil de consumo dos clientes.

## Um ponto que também merece atenção é o risco de fraudes, caso haja falha de segurança por parte da empresa escolhida. Um hacker, por exemplo, pode criar uma página falsa fazendo o internauta pensar que está acessando um site oficial e, como os dados trafegam pela VPN, ele pode descobrir senhas e outras informações. 5. Como escolher uma VPN? A maioria das fabricantes de VPN oferecem soluções para desktops e smartphones que podem ser gratuitas ou por meio de pagamento mensal. Em sua maioria, os que são cobrados têm a vantagem de oferecer um limite de uso de dados maior. Também é preciso verificar se as configurações dos equipamentos são compatíveis com o serviço escolhido, alguns celulares, podem travar também dependendo da velocidade da Internet contratada pelo usuário.

## Antes de assinar um serviço de VPN, vale a pena checar a reputação de fornecedores da ferramenta em sites especializados e fóruns de discussão. Outra dica é prestar atenção às políticas de privacidade e os termos do serviço. Existem alternativas grátis como WindScribe, que possui limite de dados até 10 GB por mês e servidores disponíveis em 10 países. Outra opção popular é o TunnelBear, com o limite de 500 MB mensais, e acesso a servidores de 23 países, e o VPN Gate, que tem como diferencial ser um software livre (código aberto) e estar presente em mais de 90 países.