# **O Que é SSH e Como Funciona?**

Por: [Andrei L.](https://www.weblink.com.br/blog/author/andrei-longenweblink-com-br/) maio 23, 2019

**SSH** (*Secure Socket Shell*) é um protocolo de rede que permite aos usuários acessar e gerenciar servidores pela internet. Mas ele não se resume apenas a isso. É por isso que, no conteúdo de hoje, você vai aprender mais sobre o que é SSH. Também vai entender como ele funciona e quais ferramentas pode usar para transferir arquivos em segurança pela sua conta de hospedagem.

O que você vai ver:

* [Como Surgiu o Protocolo SSH?](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Como-Surgiu-o-Protocolo-SSH)
* [O Que é SSH e Como Funciona?](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#O-Que-e-SSH-e-Como-Funciona)
* [Para Que Serve o Acesso SSH?](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Para-Que-Serve-o-Acesso-SSH)
* [O Que é Shell?](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#O-Que-e-Shell)
* [Como Funciona o Comando SSH?](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Como-Funciona-o-Comando-SSH)
* [Diferentes Tipos de Criptografia usadas pelo SSH](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Diferentes-Tipos-de-Criptografia-usadas-pelo-SSH)
  + [Criptografia Simétrica](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Criptografia-Simetrica)
  + [Criptografia Assimétrica](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Criptografia-Assimetrica)
  + [Hashing](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Hashing)
* [6 Ferramentas de Cliente SSH para Usar](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#6-Ferramentas-de-Cliente-SSH-para-Usar)
  + [1. Open SSH](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#1-Open-SSH)
  + [2. SmarTTY](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#2-SmarTTY)
  + [3. PuTTy](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#3-PuTTy)
  + [4. Bitvise](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#4-Bitvise)
  + [5. ZOC](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#5-ZOC)
  + [6. XShell](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#6-XShell)
* [Conclusão](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Conclusao)
  + [Artigos Relacionados](https://www.weblink.com.br/blog/tecnologia/acesso-ssh-o-que-e/#Artigos-Relacionados)

## **Como Surgiu o Protocolo SSH?**

O protocolo SSH foi desenvolvido pelo especialista em cibersegurança Tatu Ylonen em 1995. A ideia foi uma resposta a um incidente de hacking na rede de uma universidade da Finlândia.

Um [*sniffer*](https://pt.wikipedia.org/wiki/Analisador_de_pacotes) de senha (um software que rastreia e analisa o tráfego de uma rede) foi instalado em um servidor conectado diretamente ao [*backbone*](https://pt.wikipedia.org/wiki/Backbone) dessa conexão. Quando esse *sniffer* foi descoberto, ele tinha milhares de nomes de usuários e senhas em seu banco de dados. Inclusive de vários deles da empresa de Ylonen.

Esse vazamento fez com que Ylolen se aprofundasse nos estudos sobre criptografia. Então, ele desenvolveu uma solução onde foi possível usar um login remoto pela internet com segurança.

Seus amigos propuseram recursos adicionais, e três meses depois, em julho de 1995, a Ylonen publicou a primeira versão como fonte aberta. Foi assim que surgiu a solução **OpenSSH**. Mais tarde, ele tomou o protocolo de padronização no IETF e projetou o [SSH File Transfer Protocol (SFTP)](https://www.ssh.com/ssh/sftp/).

Atualmente, o protocolo SSH gerencia mais da metade dos servidores web mundiais e praticamente todos os computadores Unix ou Linux.

Especialistas em segurança da informação e de sistemas usam a ferramenta para configurar, gerenciar, monitorar e operar firewalls, roteadores, switches e servidores de redes e ambientes digitais críticos na internet.

## **O Que é SSH e Como Funciona?**

O SSH é um [protocolo de rede](https://www.weblink.com.br/blog/tecnologia/conheca-os-principais-protocolos-de-internet/) para o usuário internet acessar, administrar e modificar remotamente seus servidores. Isso inclui gerenciamento de contas de hospedagem que usam, por exemplo, serviços de [VPS](https://www.weblink.com.br/blog/o-que-e-vps/).

Tudo isso acontece pela rede. Nesta situação, dados, informações, documentos e arquivos são alcançados pelo usuário através de uma comunicação criptografada entre máquinas (o computador do usuário) e servidores (de hospedagem).

O que acontece é que essa comunicação contém um mecanismo de autenticação. Nele, é aplicada uma tecnologia de criptografia avançada que mascara os dados e transações de quem está acessando até o quê exatamente está se querendo acessar.

## **Para Que Serve o Acesso SSH?**

O acesso SSH é usado por administradores de rede para gerenciar sistemas e aplicativos de forma remota. Ou seja, longe do computador ou servidor por onde se está acessando esses sistemas virtuais.

Com o acesso SSH, o usuário pode fazer login em um outro computador por uma rede protegida por criptografia. Desse jeito, ele pode executar comandos, mover e editar arquivos de um local para outro sem riscos de interceptação por agentes maliciosos.

Essa tecnologia oferece uma interface baseada em texto para criar o acesso Shell remoto. Essa interface é o próprio terminal Shell, que executa os comandos digitados e faz a ponte entre a máquina do usuário e o servidor remoto.

## **O Que é Shell?**

*Shell*, do inglês, significa *concha*, *casca* ou *algo revestido*. No contexto da computação, o Shell é um interceptador de comandos que executa a ligação entre o usuário e o sistema operacional. Também pode ser chamado de painel Shell.

O Shell entende e executa os comandos que o usuário insere por um dispositivo externo (um teclado, por exemplo). O usuário interage com o computador por uma interface específica, inserindo instruções e obtendo respostas na forma de serviços ou funções.

## **Como Funciona o Comando SSH?**

O [comando SSH](https://www.hostinger.com.br/tutoriais/lista-de-comandos-basicos-ssh/) é escrito, por padrão, assim:

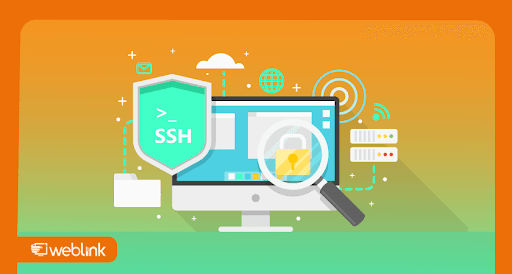
ssh {user}@{host}

Como você pode ver, ele é dividido em três partes. São elas:

* **ssh –** é a indicação do uso do comando SSH, que indica ao sistema que se quer abrir uma conexão criptografada e segura.
* **{user} –** é a conta a qual você deseja se conectar remotamente como usuário *root* (raiz), com direitos completos para mexer em qualquer coisa do sistema.
* **{host} –** é o computador que você quer acessar, inserindo um número de IP ou nome de domínio específico.

Assim que digitar as informações, basta pressionar **ENTER**. Será preciso inserir suas credenciais como nome de usuário e senha de acesso a sua conta.

Novamente, confirme pressionando **ENTER** mais uma vez. Uma janela remota de acesso ao servidor da hospedagem vai aparecer logo na sequência.



## **Diferentes Tipos de Criptografia usadas pelo SSH**

Uma das maiores vantagens de se usar SSH é a sua tecnologia de criptografia. O usuário pode se sentir seguro para acessar servidores, gerenciar e administrar bancos de dados ou informações da sua conta de hospedagem.

Existem 3 tecnologias de criptografia usadas pelo SSH. Confira logo abaixo.

### **Criptografia Simétrica**

A Criptografia Simétrica usa uma chave secreta compartilhada na codificação e decodificação de uma mensagem do cliente e do servidor. Qualquer mensagem ou transferência de arquivos ou documentos são criptografadas nesse processo.

A criação de uma chave simétrica é responsabilidade de uma chave de mudança de um algoritmo. Essa chave nunca é, de fato, transmitida entre o cliente e o servidor. Assim, o compartilhamento de dados é feito de forma independente, sem contato entre as partes.

Na criptografia simétrica, casa sessão SSH é específica, tendo sua própria chave (token) e de forma secreta. Isso exige autenticação prévia do cliente, por meio de uma senha de login, para poder acessar uma máquina externa ou servidor.

### **Criptografia Assimétrica**

A Criptografia Assimétrica usa duas chaves secretas separadas, tanto para a codificação quanto para a descodificação do processo de comunicação entre cliente e servidor. Essas duas chaves são conhecidas como chave-pública e chave-privada. Juntas, elas formam o par pública-privada.

Ao contrário da chave-privada, a chave-pública é aberta, distribuída e compartilhada entre as duas partes. A diferença é que a chave-privada, que funciona da mesma forma como a chave-pública, não pode ser matematicamente entendida pela chave-pública.

A relação entre os dois tipos de chaves é um tanto complexa. A informação ou mensagem é codificada pela chave-pública da máquina, que pode ser apenas decodificada pela chave-privada da mesma máquina.

Isso significa que a chave-pública não pode decodificar suas próprias mensagens. Nem decodificar algo já criptografado pela chave-privada. Assim, qualquer um que quiser descriptografar dados públicos deve, primeiro, possui a chave-privada correspondente.

### **Hashing**

O método de criptografia Hashing envolve o processo de codificação de dados e mensagens, mas nunca a decodificação destas mesmas informações. Por isso, ele também é chamado de *One-Way Hashing* (criptografia de uma só via).

O que acontece é que o hashing gera um valor único, de comprimento fixo para cada entrada e que não mostra nenhuma propensão de que pode ser explorada. Isso faz com que a reversão (decodificação) seja praticamente impossível de acontecer.

O SSH usa *hashes* para autenticar a validade das mensagens. Isso é feito através de códigos de autenticação baseados em Hash (HMCA), que somente o usuário interessado tem acesso. Isso garante que o comando recebido não possa ser manipulado de maneira alguma.

## **6 Ferramentas de Cliente SSH para Usar**

Um cliente SSH estabelece uma conexão segura entre a máquina do usuário a um computador ou servidor através do protocolo SSH.

Assim, o usuário consegue se conectar ao seu serviço de hospedagem, seja pelo computador ou serviço na nuvem, sem correr riscos de conexão ou sofrer ataques maliciosos da web.

Abaixo, trazemos 6 sugestões de programa SSH para conhecer.

### **1.** [**Open SSH**](https://www.openssh.com/)

****

O **OpenSSH** é um dos principais clientes para realizar login remoto com o protocolo SSH. Ele faz a criptografia de todo o tráfego recebido para eliminar a espionagem, o sequestro de dados, de conexão e outros tipos de ataques.

O OpenSSH oferece um grande conjunto de recursos de filtragem segura, além de métodos de autenticação e opções de configuração sofisticadas. Ele é desenvolvido por especialistas do [OpenBSD Project](https://www.openbsd.org/donations.html) e é disponibilizado sob uma licença de estilo BSD.

### **2.** [**SmarTTY**](https://sysprogs.com/SmarTTY/)

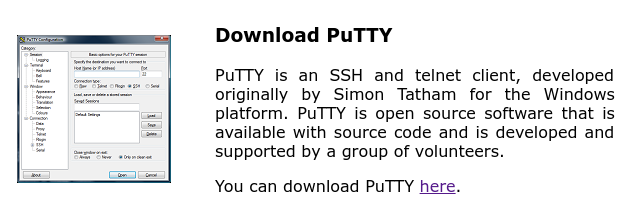
****

O **SmarTTY** é um cliente SSH com várias tabulações. E permite copiar arquivos e diretórios com SCP (*Secure Copy Protocol*) em tempo rea. Também traz a possibilidade de editar arquivos no próprio localhost.

Além disso, a ferramenta ainda possibilita:

* Abrir múltiplas abas em uma única sessão;
* Transferir arquivos e diretórios inteiros;
* Executar aplicativos gráficos sem perdas de desempenho.

### **3.** [**PuTTy**](https://www.putty.org/)

****

O **PuTTy** é um cliente SSH para a plataforma Windows e Unix (Linux e suas distribuições). Ele é um software de código aberto desenvolvido e constantemente atualizado por um grupo de especialistas voluntários.

O PuTTY é um dos mais populares clientes SSH. Ele cria uma espécie de túnel encriptado de comunicação entre servidores, garantindo a segurança e o anonimato das conexões.

Com o Putty, o usuário pode acessar e gerenciar seu servidor ou hospedagem remotamente. Com isso, é possível instalar, editar ou remover aplicações de acordo com as preferências de uso.

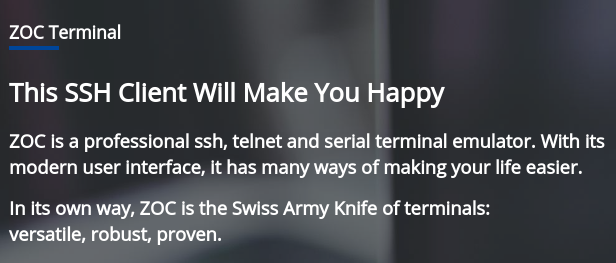
### **4.** [**Bitvise**](https://www.bitvise.com/)

****

O Bitvise é uma ferramenta SSH bastante popular, principalmente entre usuários do Windows. Ela tem suporte às versões de 32 bits e 64 bits do sistema operacional da Microsoft.

O Bitviseé gratuito a qualquer usuário, inclusive para uso comercial. Ele também conta um serviço próprio de transferência de arquivos com criptografia avançado de segurança (*SFTP* – *Secure File Transfer Protocol*).

### **5.** [**ZOC**](https://www.emtec.com/zoc/)

****

Mais voltado para desenvolvedores profissionais, o ZOC é um cliente SSH e emulador de terminal especializado para Windows e MacOS.

Ele conta com uma grande variedade de recursos, sendo uma alternativa confiável para estabelecer conexões seguras pelo terminal Shell.

O ZOC é baseado no OpenSSH. Isso significa que a ferramenta suporta trocas seguras de informações e dados por criptografia de chaves. Tudo acontece pelo protocolo SSH.

A diferença do ZOC para o OpenSSH é que aquele possui uma aba interativa de interface do usuário. Ele apresenta abas modernas, um diretório host com recursos completos e uma variedade de scripts.

### **6.** [**XShell**](https://www.netsarang.com/en/xshell/)

****

O XShell é um dos clientes SSH mais poderosos e versáteis que existem. Isso porque ele é compatível com uma variedade de protocolos de comunicação e transferência de dados e arquivos. Entre eles SSH, SFTP, Telnet, RLogin e Serial.

Por conta disso, a ferramenta se destaca mais na sua versão paga, que tem mais recursos do que a edição gratuita. Isso inclui ambiente de abas interativas, direcionamento dinâmico de portas e gerenciamento de contas com camadas extras de proteção criptografada.

## **Conclusão**

Segurança é indispensável em qualquer projeto na internet. Com o SSH, o usuário tem vantagens com as tecnologias de criptografia, que garantem acesso remoto a computadores e servidores de qualquer lugar sem comprometer a proteção de dados e nem de desempenho. Só se lembre de guardar suas credenciais de acesso ao SSH.