Prefeitura Municipal de Petrolina - PE

Secretário Escolar

NV-017OT-25-PREF-PETROLINA-PE-SECRET
Cód.: 7908428814243

NOVA CONCURSOS

SUMÁRIO

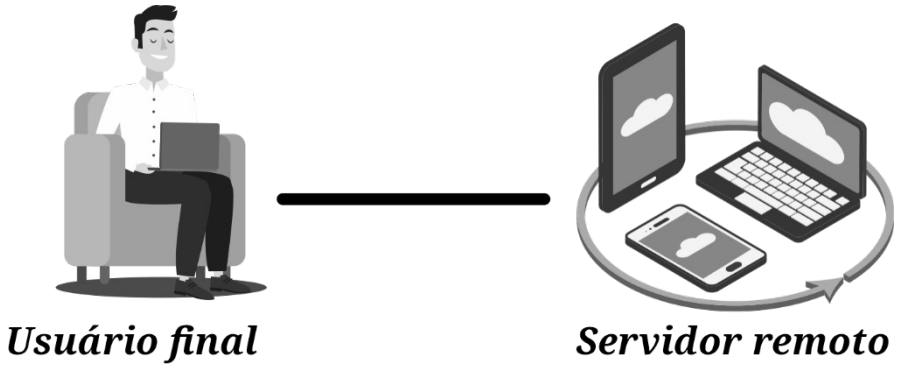
CONHECIMENTOS ESPECÍFICOS

CONCEITOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

O que é segurança da informação? Essa é uma pergunta curta que exige conhecimentos diversos para ser respondida. Neste material, encontraremos as informações necessárias para isso.

As redes de computadores tornaram-se cada vez mais interligadas e complexas. Atualmente, elas integram diversos dispositivos que, talvez, você nem conheça, mas que estão presentes, promovendo a troca de dados entre o seu equipamento e o servidor remoto ao qual você está acessando. No entanto, é sabido que criminosos virtuais podem acessar redes a partir de qualquer lugar do mundo.

Nesse sentido, os profissionais de segurança da informação procuram proteger os dados armazenados e trafegados entre os dispositivos por meio de equipamentos, programas e técnicas direcionadas. Para isso, o treinamento dos usuários também é importante, considerando que eles compreendem o elo mais fraco e vulnerável no que se refere à segurança da informação.

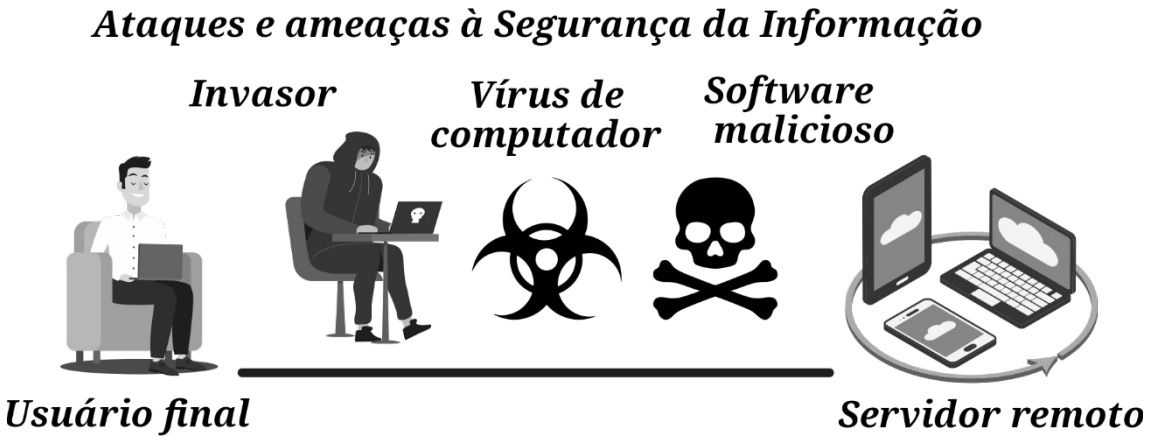


A conexão entre o usuário cliente e o servidor é realizada por diferentes equipamentos, que são transparentes para o usuário final.

Entre o servidor remoto e o usuário final, as informações solicitadas passarão por vários dispositivos de conexão (roteadores, repetidores de sinal, *switches*, *bridges*, *gateways*) antes de serem apresentadas no dispositivo do usuário.

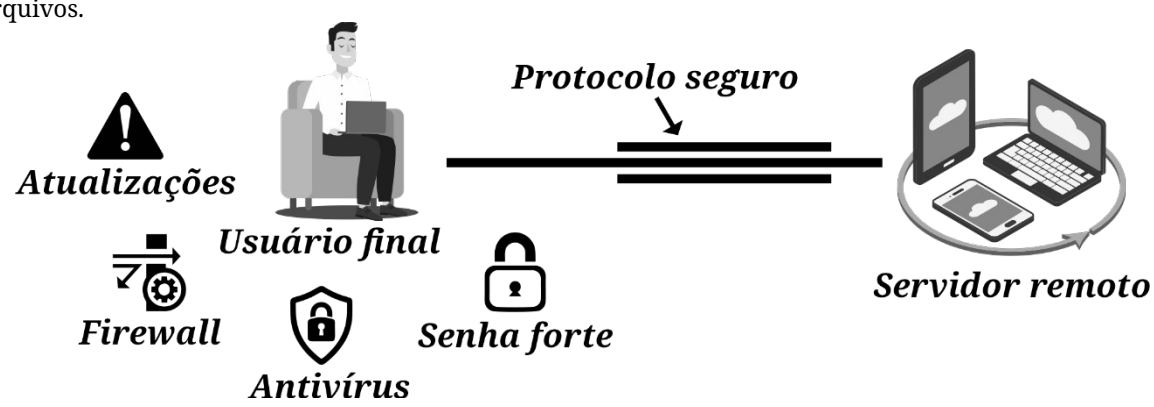
Dica

Paradigma cliente-servidor: nós somos os clientes e acessamos informações em servidores remotos. As redes de computadores, em concursos públicos, são abordadas seguindo esse paradigma. Usamos um cliente web (browser ou navegador) para acessar um servidor web. Usamos um cliente de e-mail para acessar um servidor de e-mail. Usamos um cliente FTP para acessar um servidor FTP.



O tráfego de dados em uma conexão é um ativo interessante para invasores, vírus de computadores e softwares maliciosos.

Invasores tentarão acessar a conexão e capturar os dados trafegados. Os vírus de computador procuram infectar os arquivos e causar danos aos sistemas. Esses softwares maliciosos podem infectar dispositivos e sequestrar arquivos.



Um protocolo seguro protege o tráfego de dados em uma conexão insegura, criptografando as informações que são enviadas e recebidas.

O usuário deverá utilizar um protocolo seguro para acessar os dados, manter o seu dispositivo atualizado e protegido, utilizar uma senha forte de acordo com as políticas de segurança e práticas recomendadas, entre outras ações. Além disso, é necessário utilizar conexões seguras, como as VPNs — *Virtual Private Network* —, para acesso a serviços remotos (computação na nuvem), bem como proteger-se contra ameaças e ataques à segurança da informação, por meio de medidas de proteção no dispositivo, como antivírus, *firewall* e *anti-spyware*.

Iniciaremos nossos estudos sobre segurança da informação com o tópico VPN. Esse recurso é muito importante para a comunicação segura e ganhou destaque nos últimos anos, em razão do trabalho remoto (home office). Empresas e usuários que antes não utilizavam uma conexão remota segura precisaram adaptar-se aos novos tempos. Em concursos, a tendência é que aumente a frequência de questões sobre esse tema, pois ele se popularizou durante a pandemia.

A seguir, conheceremos como é a computação na nuvem, suas características, os tipos de nuvem, os serviços oferecidos e as vantagens e desvantagens. Vale ressaltar que esse tópico já foi bastante abordado em alguns concursos, em provas de diversos cargos.

É difícil encontrar alguém que nunca tenha sido vítima de computador e softwares maliciosos, não é mesmo? Esse será o terceiro tópico sobre segurança da informação, no qual abordaremos os ataques e ameaças, com destaque para os principais e mais comuns em provas de concursos.

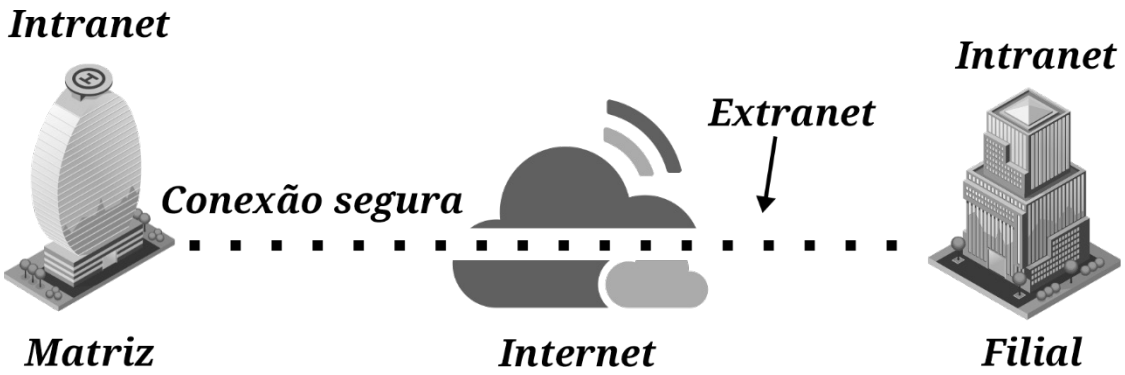
Finalizando o conteúdo de segurança da informação, estudaremos os mecanismos de proteção e defesa contra os ataques e ameaças. Existem equipamentos de proteção, no entanto, em concursos públicos, geralmente, são questionados os **aplicativos para segurança** (antivírus, *firewall*, *anti-spyware* etc.).

Apesar de existirem soluções integradas e avançadas para os problemas de segurança da informação — muitas delas presentes em nossos próprios dispositivos —, nos concursos públicos, costumam ser cobradas as definições oficiais e as configurações padrão dos programas.

NOÇÕES DE REDES PRIVADAS VIRTUAIS (VPN)

As redes privadas virtuais, popularmente identificadas pela sigla VPN, são criadas pelas empresas e usuários para estabelecer uma conexão segura entre dois pontos. Antes de iniciarmos nosso estudo sobre elas, vamos conhecer alguns dos conceitos básicos das redes de computadores, de acordo com as suas características de uso e nível de segurança.

REDE	CARACTERÍSTICAS BÁSICAS
LAN	*Local Area Network* é uma denominação relacionada ao alcance de uma rede, restrita a um prédio ou pequena região
Intranet	É uma rede local (pelo seu alcance, é uma LAN), interna de uma organização, segura, com acesso restrito aos usuários cadastrados no servidor da rede
Extranet	É o acesso remoto seguro de um ambiente inseguro à intranet da organização
Internet	Rede mundial de computadores de acesso público e considerada insegura. A internet é comumente representada por uma nuvem



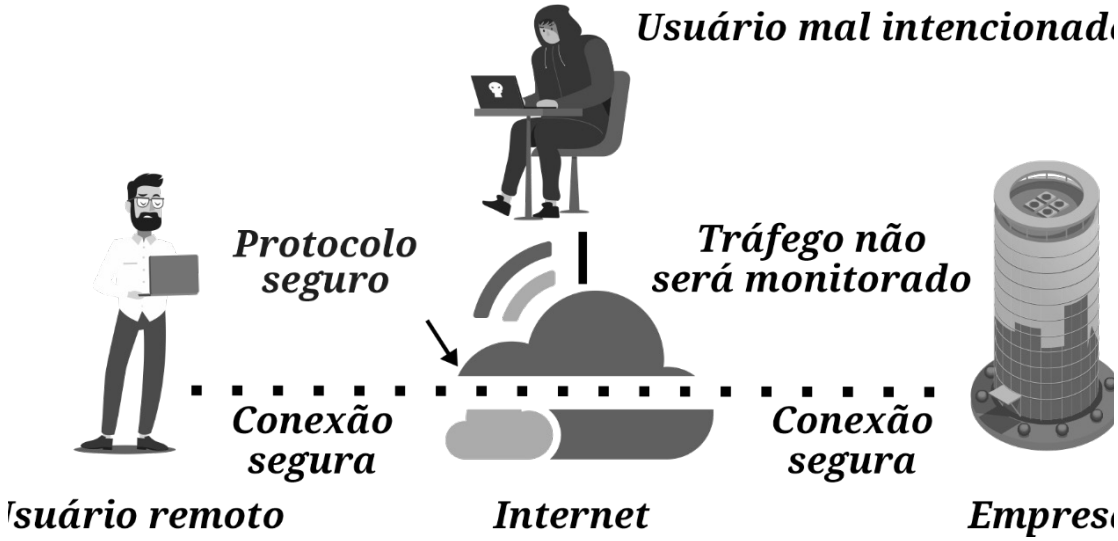
A Extranet é uma conexão segura através de um ambiente inseguro (*internet*) para redes internas protegidas (*Intranet*).

Importante!

Toda intranet é uma LAN, mas nem toda LAN é uma intranet.

Por que usar uma VPN? Porque é importante e necessário. A internet é a rede mundial de computadores que conecta diversos dispositivos entre si utilizando uma estrutura pública e insegura oferecida pelos governos e operadoras de telefonia. O acesso à internet é oferecido para todos e, por isso, os usuários mal-intencionados conseguem interceptar a comunicação de outros usuários, monitorando o tráfego de dados e roubando informações.

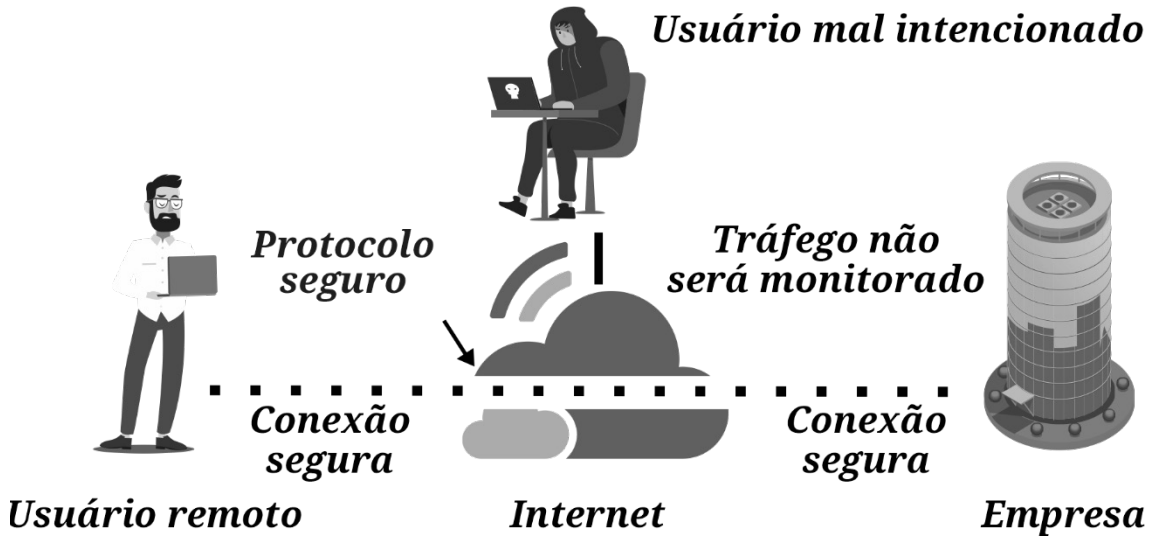
Com uma VPN estabelecida entre os dispositivos, o risco na transmissão é muito pequeno. Lembre-se de que nada é 100% seguro em informática, independentemente da quantidade de sistemas e proteções implementadas.



Usuários mal-intencionados procuram "escutar" uma conexão insegura em busca de dados que possam comprometer a privacidade do usuário ou empresa.

As empresas utilizam softwares de terceiros para estabelecer a conexão segura entre os dispositivos de seus colaboradores. Existem vários softwares que possibilitam a conexão segura, como a área de trabalho remota (Windows) e soluções de empresas de segurança digital (Forticlient VPN, Citrix Metaframe, TeamViewer, LogMeIn etc.).

Os protocolos são padrões de comunicação. Para estabelecer uma conexão segura, protocolos seguros serão usados, criando um túnel seguro entre o emissor e o receptor, por meio de um ambiente vulnerável. Eles procuram encapsular os dados transmitidos para que, em caso de monitoramento, a leitura do conteúdo seja impossível, uma vez que os dados estejam criptografados.



Usuários mal-intencionados não conseguem monitorar o conteúdo de uma conexão que esteja protegida com um protocolo seguro.

TIPO DE VPN	CARACTERÍSTICA
VPN de acesso remoto (VPN *client to site*)	● Um usuário pode conectar-se a uma rede para acessar seus serviços e recursos remotamente ● A conexão é segura e ocorrerá por meio de uma rede pública, como a internet ● Será uma conexão (cliente) para um servidor remoto que aceita várias conexões
VPN site a site	● Dois roteadores estabelecem uma conexão segura para a troca de dados, sendo que um deles opera como cliente VPN e o outro, como servidor VPN ● É o modelo mais usado no âmbito empresarial, para conectar com segurança a rede interna de uma filial com a rede interna de uma matriz ● Serão várias conexões (filial), acessando um servidor remoto que aceita várias conexões (matriz) ● Também conhecida como VPN LAN *to* LAN

Protocolos

Quando uma navegação na internet é realizada, os protocolos transferem os dados de um servidor para o cliente de acordo com o paradigma cliente-servidor. O servidor oferece os dados e provê a conexão e, então, o cliente acessa as informações e solicita serviços.

Em uma conexão, para evitar que os dados sejam acessados por pessoas não autorizadas, protocolos de segurança e proteção poderão ser implementados, utilizando-se de chaves e certificados digitais para a garantia da transferência segura dos dados.

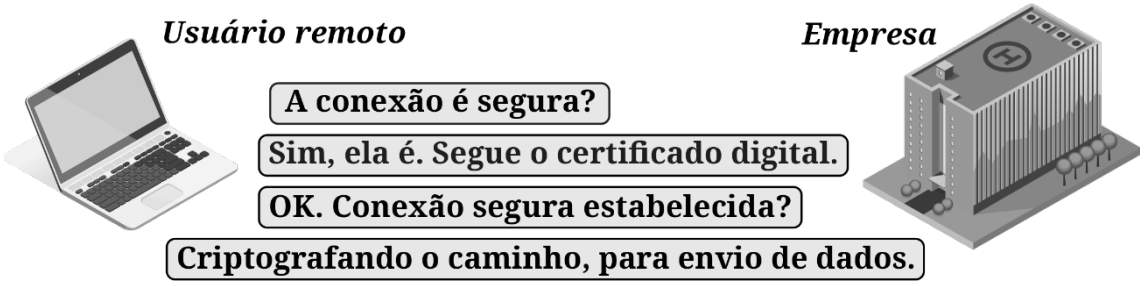
Muitas siglas de protocolos estão relacionadas com este tópico. Confira algumas delas:

PROTOCOLO	SIGNIFICADO	CARACTERÍSTICAS	SEGURO?
GRE	*Generic Routing Encapsulation*	Desenvolvido pela CISCO, prioriza a velocidade	Não
SSL	*Secure Sockets Layer*	Camada adicional de segurança para a conexão	Sim
TLS	*Transport Layer Security*	Camada de transporte seguro para a conexão	Sim
SSH	*Secure Shell*	Orientar o servidor para criação de uma conexão segura com o cliente	Sim
IPsec	*IP Security Protocol*	Extensão do protocolo IP para suprir a falta de segurança de informações que trafegam em uma rede pública	Sim
Telnet	–	Protocolo para facilitar a comunicação bidirecional, baseada em texto interativo (comandos), usando uma conexão de terminal virtual	Não

PROTOCOLO	SIGNIFICADO	CARACTERÍSTICAS	SEGURO?
L2TP	*Layer 2 Tunnelling Protocol*	Atualização dos protocolos L2F (Protocolo de Encaminhamento da Camada 2) e PPTP (Protocolo de Tunelamento Ponto a Ponto)	Não
PPTP	*Point-to-Point Tunneling Protocol*	O PPTP adiciona um canal seguro ao TCP e utiliza um túnel GRE Algumas questões o apresentam com a sigla PPP	Sim
OpenVPN	VPN de Código aberto	Criar conexões ponto a ponto (*point-to-point*) e site a site (*site-to-site*) usando um protocolo personalizado baseado no TLS e SSL	Sim

Atenção! Protocolos seguros costumam mostrar a **letra S** na sua sigla, como em HTTPS.

Um protocolo seguro procura estabelecer uma conexão segura entre os dispositivos, possibilitando a troca de informações. Antes do envio de dados, a conexão segura será negociada entre os dispositivos e aprovada após a confirmação do certificado digital.



A criptografia é usada para garantir a autenticidade e a integridade das conexões.

A conexão remota poderá ser uma simples conexão direta entre os dispositivos (ponto a ponto, túnel de conexão, sem criptografia dos dados trafegados) ou uma conexão entre os dispositivos com segurança, utilizando protocolos seguros para criptografar o conteúdo trafegado no túnel de conexão.

Programas

Após conhecer as definições de uma VPN e os protocolos que podem ser utilizados, é comum surgir uma dúvida: quais são os programas que usamos para transformar o nosso dispositivo em um cliente VPN?

A resposta é: depende. Cada dispositivo possui um sistema operacional e, de acordo com a origem (cliente) e o destino (servidor), existem programas mais adequados para cada cenário.

ORIGEM (CLIENTE)	DESTINO (SERVIDOR)	EXEMPLO DE PROGRAMA PARA VPN
Windows	Windows	Área de trabalho remota
Windows	Linux	PuTTy
Linux	Windows	OpenVPN
Linux	Linux	*Network-Manager*

A utilização de um software de VPN, com o objetivo de acessar a rede interna de uma organização (no modelo VPN *client to site*), implementa segurança aos dados trafegados na forma de criptografia para garantir a autenticidade e a integridade das conexões. No entanto, onde a VPN será "iniciada"?

Nas redes de computadores, o firewall é um item especialmente importante em relação à segurança da informação. Ele é um filtro de portas TCP (Protocolo de Controle de Transmissão), que permite ou bloqueia o tráfego de dados. Logo, se uma conexão deseja enviar e receber dados, precisa ter a porta correspondente liberada em ambos os lados, tanto no cliente como no servidor.

Se existe um firewall na rede, a VPN poderá ser instalada (e configurada) no firewall (mais comum), em frente ao firewall (para autenticar o que está chegando), atrás do firewall (para autenticar o que chegou), paralelamente ao firewall (para acompanhar o envio e recebimento dos pacotes) ou na interface dedicada do firewall (na conexão VPN *site-to-site*, para atender a vários dispositivos da rede).

No Windows 10, a definição da VPN poderá ser realizada por meio da Central de Ações (atalho de teclado Windows + A) ou nas Configurações → Rede e Internet → VPN. O acesso home office é um tipo de conexão externa que deverá utilizar uma VPN para proteger os dados trafegados com o uso de criptografia implementada por protocolos seguros.