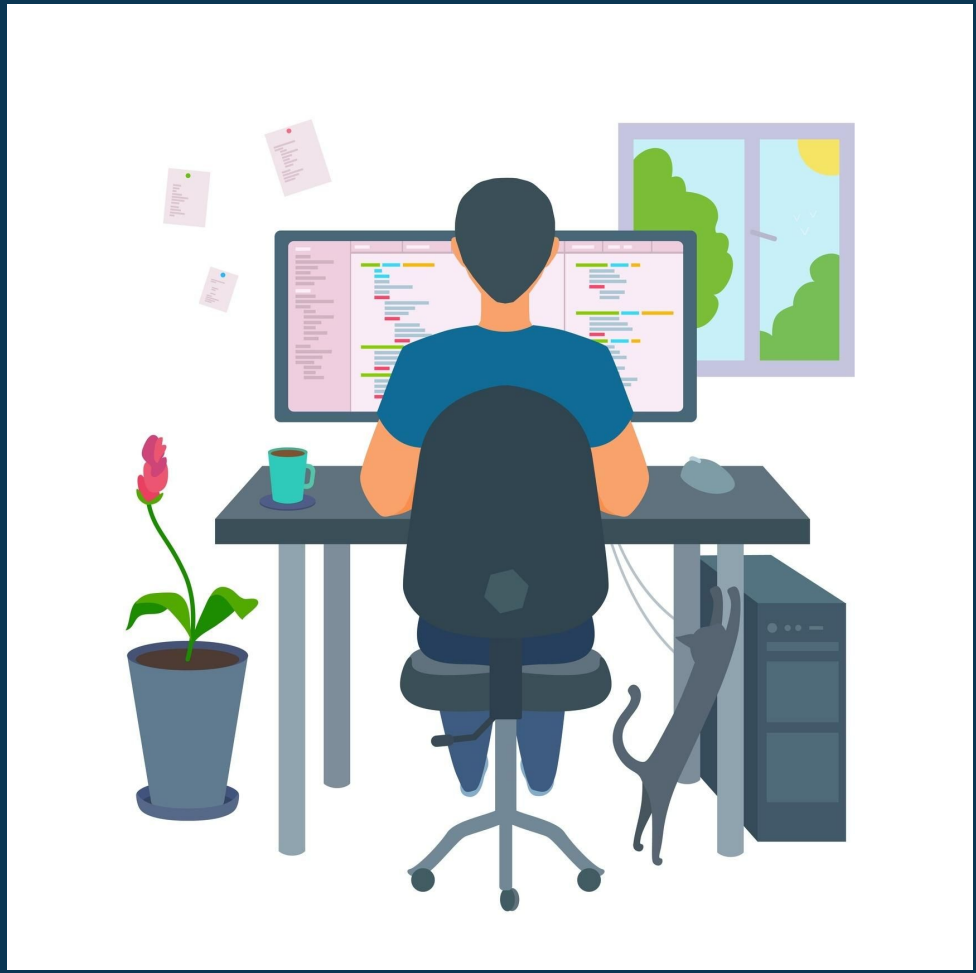
7 INICIATIVAS PARA AUMENTAR A SEGURANÇA NO HOME OFFICE

CentralServer

A maior adesão ao trabalho em home office tem feito as empresas perceberem que não precisam de tantas pessoas trabalhando presencialmente.

A tendência é termos cada vez mais pessoas trabalhando a partir de casa.

CentralServer



Por outro lado, o trabalho remoto é uma oportunidade para os hackers praticarem invasões e roubo de dados.

Como a superfície de ataque aumentou, é possível chegar nos dados da empresa a partir do home office.

Por isso, é crucial garantir que a equipe esteja treinada e com as ferramentas certas para executar rotinas remotamente.

CentralServer

Conheça as 7 iniciativas que você deve tomar para tornar o home office mais seguro

CentralServer

1. Treinar a equipe
2. Proteger as senhas
3. Investir em antivírus
4. Controlar os arquivos
5. Usar sistemas na nuvem
6. Usar VPN
7. Fazer backups regulares

1. Treinar a equipe para não cair no phishing

Os hackers usam emails forjados e fake news para levar as pessoas a baixar programas maliciosos ou visitar sites que roubam credenciais de acesso.

Treine os colaboradores para verificar o remetente das mensagens e o destino dos links contidos nelas.

Hoje em dia, é fácil descobrir os nomes das pessoas que trabalham em uma empresa através das redes sociais. Por isso, a equipe deve estar atenta a pedidos de trocas de senhas ou permissões de acesso.

CentralServer

1. Treinar a equipe para identificar sites falsos

CentralServer

Outro cuidado importante é verificar se o endereço mostrado no navegador começa com "https://" e se o certificado seguro é válido.

Na dúvida, é possível confirmar a informação clicando no ícone de cadeado da barra de endereços do navegador.

2. Proteger as senhas

Forneça um cofre de senhas para cada colaborador guardar as suas credenciais. Isso permitirá o uso de senhas complexas e específicas para casa sistema.

Torne obrigatório o uso de autenticação de dois fatores (2FA) como uma camada extra de proteção.

CentralServer

3. Investir em antivírus

CentralServer

Escolha uma solução de segurança forte e confiável.

Configure o antivírus para baixar e instalar atualizações automaticamente.

Ative as funções de anti-phishing e anti-ransomware para evitar esses tipos de ataques.

4. Controlar os arquivos

Use uma suíte como o Microsoft 365 para facilitar a colaboração da equipe e permitir o compartilhamento seguro de documentos.

Defina a política de compartilhamento externo e controle os dispositivos que podem acessar os arquivos.

CentralServer

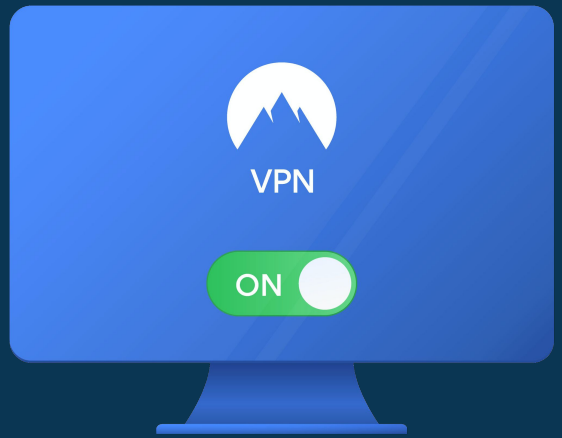
5. Usar sistemas na nuvem

A nuvem aumenta a segurança do trabalho remoto pois permite a configuração de políticas de acesso dos colaboradores aos sistemas da empresa.

Conceda ou remova as permissões rapidamente, ganhando agilidade na gestão da segurança da informação.

CentralServer

6. Usar VPN



CentralServer

Configure uma rede privada virtual (VPN) para elevar a segurança das conexões feitas de casa o escritório ou para a nuvem.

Conexões via VPN são criptografadas, o que protege o tráfego de informações e dificulta a ocorrência de invasões.

7. Fazer backups regulares

CentralServer

Faça backup dos dados importantes para ter uma salvaguarda em caso de perda ou roubo.

Se tiver recursos na nuvem, faça também backup dos servidores virtuais para ter uma proteção extra e facilitar o processo de restauração.

Ajudamos você a implantar um home office seguro

Nossa Missão é fornecer serviços gerenciados de computação em nuvem para apoiar o crescimento do seu negócio.

Trabalhamos para entender as suas necessidades e criar soluções personalizadas. Atuamos na fase de implantação e seguimos apoiando para que você possa se concentrar nos seus objetivos enquanto usa a nuvem.

Fale conosco e transforme a TI da sua empresa em um recurso estratégico.

SEU NEGÓCIO NA NUVEM. SIMPLES ASSIM.

CentralServer