Segurança em Foco

CPSI - Comissão Permanente de Segurança da Informação
SSI - Seção de Segurança da Informação
ASCOM - Assessoria de Comunicação Social e Cerimonial

Soluções para Acesso Remoto

Edição nº29
Março/2023

É inegável que a tecnologia para o trabalho remoto e teletrabalho vem ganhando cada vez mais espaço no mundo contemporâneo e um dos pontos mais importantes é a de garantir que todos os servidores tenham acesso às informações necessárias para realizar as suas atribuições. Para não ameaçar os servidores da instituição com conexões duvidosas, a solução é escolher como realizar esse acesso sem colocar as informações corporativas em risco. O TRE está implantando uma ferramenta segura e confiável para viabilizar o acesso remoto, o VDI - *Virtual Desktop Infrastructure*.

O que é VDI *(Virtual Desktop Infrastructure)*?

O *Virtual Desktop Infrastructure* (VDI), consiste numa tecnologia que permite a criação de *desktops* virtuais (estações de trabalho remotas) em uma máquina servidora central para, em seguida, ser acessados por usuários por meio de dispositivos conectados à Internet, como *laptops, tablets* e *smartphones*.

A partir de tais dispositivos, o usuário tem acesso a uma área de trabalho remota, com o sistema operacional e demais recursos corporativos, como os serviços da intranet, sem precisar instalar nada.

Segurança da informação: 8 cuidados para o trabalho remoto

- **Seguir diretrizes da instituição:** naturalmente, a gestão deve guiar a equipe e implementar algumas diretrizes e bons hábitos básicos de segurança. Assim, com a definição e a organização das questões internas, os usuários ficam informados sobre como será a rotina e quais práticas de proteção serão adotadas pela instituição. Isso também é importante para entender como se comportar no ambiente virtual de acordo com as expectativas dos gestores.

- **Só utilizar softwares e aplicativos instalados pelo TI da instituição:** mesmo antes do *home office,* softwares e aplicativos de TI já eram parte importante do cotidiano organizacional das instituições. Isso porque as ferramentas permitem realizar operações no departamento financeiro, de logística, de RH, e de clientes e fornecedores, de maneira totalmente segura e ágil. Para que as atividades continuem ocorrendo a distância, os usuários devem se adaptar, utilizando apenas os programas instalados pelo setor de tecnologia da corporação.

- **Atualizar sistemas e softwares:** outro cuidado imprescindível é instalar apenas sistemas e softwares originais no computador e mantê-los sempre atualizados. Com frequência, os programas são atualizados pelos desenvolvedores para evitar riscos de vazamentos de dados ou possíveis brechas para hackers invadirem as informações corporativas. No entanto, é necessário ter bastante atenção no momento da atualização, verificando se a fonte de notificação é, de fato, confiável.

- **Realizar backup regularmente:** fazer o backup regularmente mantém o negócio protegido contra imprevistos. Por isso, é fundamental que a equipe tenha uma rotina de armazenamento de cópias de segurança dos dados. O mais indicado é contar com sistemas em nuvem que mantém um backup a cada alteração, o que garante maior eficiência e proteção no processo de compartilhamento.

- **Usar senhas fortes:** o mais indicado é utilizar sempre senhas fortes e mecanismos de autenticação, garantindo segurança e impedindo que hackers acessem as contas da empresa. Também é importante evitar salvar as senhas automaticamente no computador e no navegador. O ideal é que, a cada acesso, a senha seja digitada, fazendo disso um hábito de proteção a mais para a manutenção da integridade dos dados.

- **Controlar o acesso aos sistemas corporativos:** outra dica fundamental é controlar ao máximo o acesso aos sistemas corporativos, sempre fazendo a ação por meio de uma conexão de rede segura. Portanto, é importante verificar se o roteador da casa está com as configurações atualizadas e com uma senha forte. A gestão ainda pode incentivar os usuários a utilizarem uma rede privada virtual *(VPN)*, que garante a criptografia no momento de trocar as informações relativas ao negócio.

- **Não acessar links suspeitos:** caso o usuário se depare com links suspeitos, o mais indicado é excluir a mensagem o quanto antes e reportar o problema ao departamento de TI da empresa. Ataques cibernéticos, e-mails, entre outros tipos de ameaças ocorrem diariamente e representam riscos reais para a integridade e o sigilo dos dados corporativos. Por isso, é preciso ficar atento. Caso haja qualquer tipo de notificação estranha, o melhor é não acessar os links recebidos.

- **Instalar um bom antivírus:** os antivírus são softwares específicos para verificar se os dispositivos estão ou não contaminados e, ainda, se o sistema operacional está atualizado. Além disso, os antivírus realizam atualizações que corrigem problemas técnicos – responsáveis, muitas vezes, por causar vulnerabilidade nos computadores e na rede de internet. Portanto, ter um bom antivírus instalado é essencial para exercer as atividades em formato *home office*.

É preciso ter em mente que as medidas citadas são de extrema importância para manter a segurança da informação, uma vez que todos os cuidados garantirão uma maior proteção para a instituição. Com isso, os gestores podem ficar mais tranquilos, tendo a certeza de que os usuários cuidarão da melhor forma da integridade dos dados do negócio.

Fique ligado: no próximo mês, falaremos sobre ***Como localizar remotamente o celular?***

Tribunal Regional Eleitoral - RN