***Estabelecer níveis de acesso aos usuários***

O erro mais comum entre as empresas é o fator do “Erro Humano” que vem em múltiplas formas. Neste caso a permissão dos usuários, uma das formas de minimizar riscos é estabelecer níveis de acesso aos usuários. Colaboradores de determinada área não precisam ter acesso a documentos que não concernem às suas funções.

Outro ponto importante é que, dessa maneira, as informações estratégicas e que geram vantagem competitiva ficarão disponíveis apenas para aqueles que realmente necessitam dela. Logo, as chances de vazamentos de documentos confidenciais são menores e todos os dados da empresa ficam mais protegidos. Isso também força uma melhor organização de documentos e arquivos, o que pode auxiliar na produtividade dos setores.

### *Proteja as conexões wi-fi*

As conexões wi-fi abertas permitem que os dados fiquem expostos a todos os tipos de malware e ações criminosas. E então temos um protocolo de ações a serem tomadas para estabelecer a segurança da empresa.

1. Inserir uma senha de acesso para cada usuário, o que permite rastrear as entradas na rede e identificar de onde surgiu um determinado roubo de dados por esse meio;
2. Tenha uma senha forte de acesso;
3. Realize as configurações de criptografia de rede;
4. Mantenha os firewalls ativos e atualizados;
5. Desative acessos remotos e serviços desnecessários.

### *Realize backup constante e eficiente*

Apesar de não ajudar a se proteger, o backup constante é sempre necessário para manter a empresa em casos de crise e outros problemas drásticos, como um ataque de sequestro de dados (Ransomware) e dentre outras ameaças, como dados sendo corrompidos.

### *Mantenha os sistemas atualizados*

As atualizações são importantes para resolver falhas de segurança que sejam conhecidas pelos hackers, sendo um grande motivo pelo qual softwares de hoje em dia estão sempre em constante atualização. Os pontos de vulnerabilidade são:

Firewalls e outros mecanismos/softwares de segurança e supervisão;

Sistemas operacionais;

Drives, Firmwares, entre outros.

### *Treine os funcionários para condutas seguras*

Condutas inadequadas de funcionários são um dos principais problemas (Como já estabelecido a cima) com segurança das redes. Ações que fujam dos protocolos de segurança podem abrir brecha para instalação de malwares.

Reuniões, MiniCursos e “Hands on training” são maneiras efetivas de manter suas equipes de funcionários bem atualizadas sobre o comportamento online de seus usuários.