# Não note suas senhas

O bom é inimigo do ótimo!!!, eu sempre lembro essa é uma frase que ecoa aos quatro ventos ainda mais quando se trata da questão de segurança da informação.

Abaixo estão mais orientações sobre senhas adaptadas do site da Microsoft.

Altere as senhas nos sistemas de controle quando instala-os - não use as senhas padrão de fábrica.

Não use nomes de família, iniciais ou outras informações pessoais ao criar senhas.

Alterar senhas regularmente - no mínimo, a cada 6 meses.

Use senhas fortes sempre que os dispositivos os suportam.

As senhas fortes são uma combinação de oito ou mais caracteres alfanuméricos, letras maiúsculas e minúsculas e palavras sem sentido.

Memorize senhas sempre que possível. Se você deve anotar uma senha, verifique se ela não é identificada como uma senha e mantê-la bloqueada ou em sua pessoa em todos os momentos.

Não compartilhe senhas, exceto quando o sistema ou as políticas organizacionais o exigem.

Se um fornecedor ou pessoa de serviço precisa acessar seu sistema, não compartilhe sua senha com o indivíduo. Em vez disso, faça com que o indivíduo olhe afastado enquanto você insere suas credenciais de logon.

Se você acredita que sua senha foi comprometida, mude-a o mais rápido possível.

Imediatamente remova os privilégios de acesso sempre que um empregado deixar a empresa.

Se um funcionário não precisa mais de certos privilégios de acesso para executar seu trabalho, remova esses privilégios.

Duplo fator de autenticação

um número crescente de organizações está implementando autenticação de fator duplo (ou fator) para adicionar uma camada de proteção (defesa em profundidade) à segurança. Ao exigir um segundo método de autenticação, além do método padrão de nome de usuário / senha, as organizações implementam uma poderosa contramedida.

Os especialistas em segurança acreditam que a autenticação de dois fatores mais eficiente usa dois dos seguintes tipos de métodos de autenticação:

Algo que você conhece - como uma senha ou PIN.

Algo que você tem - como um crachá de acesso ou um token de segurança.

Algo que você é - como uma impressão digital ou uma varredura da retina.

Uma nota sobre acesso remoto: qualquer dispositivo que se conecte remotamente à rede do sistema corporativo ou de controle oferece uma oportunidade para um adversário ter acesso ao dispositivo e atacar sua rede. Além de usar criptografia e proteção por senha, considere a autenticação de dois fatores para esses dispositivos.