Checklist de Acesso Remoto Seguro (VPN)

Porta aberta na internet é convite. Robôs procuram por ela o dia inteiro, testando senhas sem parar.

Como usar: marque só o que você **confirmou com os próprios olhos** (ou viu a sua equipe de TI mostrar). "Acho que sim" não vale. Cada caixa em branco é um ponto a resolver.

1 Como se entra de fora

VPN é um túnel protegido por criptografia: quem está fora só entra na rede da empresa depois de provar quem é.

- [ ] **Nenhuma área de trabalho remota** (RDP, porta 3389) aberta direto na internet.
  RDP é o recurso do Windows para controlar outro computador. Exposto, vira alvo de tentativas de senha.
- [ ] **Câmeras e gravador (DVR/NVR) sem porta aberta** no roteador.
  Para ver de fora, use a VPN ou o app oficial do fabricante.
- [ ] Acesso aos sistemas **só pela VPN**. AnyDesk, TeamViewer e similares só onde for preciso, com duas etapas.
- [ ] Existe uma **lista escrita de quem tem acesso** de fora, e para quê.

2 Quem entra

- [ ] **Um usuário por pessoa.** Nada de login "admin" ou "vpn" usado por várias pessoas.
  Com login compartilhado, não dá para saber quem fez o quê, nem tirar o acesso de uma pessoa só.
- [ ] **Senha forte e só dela**: longa (uma frase é ótimo) e que não é usada em nenhum outro site ou sistema.
- [ ] **Verificação em duas etapas** ligada na VPN.
  Além da senha, pede um código ou confirmação no celular. Se a senha vazar, sozinha ela não abre a porta.
- [ ] O acesso é **desligado no mesmo dia** em que alguém sai da empresa. Vale também para fornecedor que terminou o serviço.

3 Equipamento

Firmware é o sistema interno do roteador/firewall. Atualizar fecha falhas que invasores já conhecem.

- [ ] Roteador/firewall com **firmware atualizado** e ainda recebendo atualizações do fabricante.
- [ ] **Senha padrão de fábrica trocada** no roteador, firewall, câmeras e DVR.
  Elas estão nos manuais, publicados na internet.
- [ ] O **painel de configuração** do roteador não pode ser aberto pela internet.
- [ ] VPN em **protocolo atual**: WireGuard, IPsec/IKEv2 ou OpenVPN.
  Evite PPTP: é antigo e a proteção dele pode ser quebrada.

4 O que a VPN deixa ver

- [ ] Cada pessoa acessa **só o que precisa** (ex.: o sistema financeiro), não a rede inteira.
  Se um computador de fora for invadido, o estrago fica limitado.
- [ ] **Fornecedores** têm acesso separado, limitado ao que atendem e com data para acabar.
- [ ] O computador que conecta de casa tem **sistema atualizado e antivírus ligado**.
- [ ] De preferência, é um **notebook da empresa**, não o computador que a família toda usa.

5 Registro

sem registro, ninguém sabe o que aconteceu

Log é o registro automático de quem entrou, de onde e a que horas.

- [ ] A VPN **guarda o log** de cada acesso (usuário, horário, de onde veio) por **semanas ou meses**.
- [ ] **Várias senhas erradas seguidas** bloqueiam o login e **geram alerta** para quem de fato lê.
- [ ] Alguém confere acessos em **horário estranho** (madrugada, feriado).
- [ ] Última revisão da lista de acessos: ____/____/_____

TESTE DE 5 MIN

Liste quem tem acesso de fora hoje.

1. Peça a lista de **todos os usuários** da VPN e do acesso remoto, inclusive fornecedores.
2. Ao lado de cada nome, anote quem é a pessoa e se ela **ainda trabalha** com vocês.
3. Procure logins genéricos, como "admin", "vpn", "suporte" ou "recepcao".

Se tem gente que já saiu da empresa, ou login "admin" compartilhado, o acesso precisa de atenção agora, não depois do problema.

Quer que a gente confira o seu?
Chama no WhatsApp: (32) 98809-6395