Checklist de Saúde do Servidor

Servidor não avisa antes de parar. Quem avisa é quem está olhando.

Vale para o servidor, o NAS (a "caixinha" de arquivos na rede) ou aquele **computador que fica ligado** com o sistema e as pastas da empresa. Marque só o que você **confirmou com os próprios olhos**. Cada caixa em branco é um ponto a resolver.

1 Onde ele fica

- [ ] Fica num **local ventilado**, com as saídas de ar livres de poeira.
  Nada de embaixo da mesa, em armário abafado ou no depósito quente.
- [ ] Está **protegido de água**: fora do chão, longe de janela, pia e ar-condicionado pingando.
- [ ] **Acesso físico restrito**: sala ou rack com chave. Quem chega nele pode desligar, levar ou plugar algo.

2 Energia

- [ ] Está ligado num **nobreak** com carga suficiente para ele **desligar com segurança** numa queda de luz.
  Desligar "no tranco" pode corromper o banco de dados e os arquivos abertos.
- [ ] O **desligamento é automático** quando a bateria está acabando.
  Exige o cabo (USB ou rede) entre nobreak e servidor e o programa configurado.
- [ ] A **bateria do nobreak é testada** e trocada no prazo do fabricante. Bateria velha segura bem menos.
- [ ] Última troca da bateria: ____/____/_____

3 Discos

- [ ] O **espaço livre é acompanhado** e há um **alerta antes de encher**. Disco cheio para o sistema e o banco de dados.
- [ ] A **saúde dos discos (SMART)** é verificada.
  SMART é o autodiagnóstico do disco: aponta desgaste antes da falha (não todas).
- [ ] Se tem **RAID**, chega um **aviso quando um disco falha**, e ele é trocado logo.
  RAID = discos que se espelham: se um queima, o servidor segue. Mas o que for apagado ou travado por vírus some em todos. **RAID não é backup.**

4 Atualizações e acesso

- [ ] O sistema está **recebendo atualizações de segurança** e ainda tem suporte do fabricante.
  Ex.: Windows Server 2012 e 2012 R2 não recebem mais atualizações desde outubro de 2023.
- [ ] **Antivírus ou EDR ativo** e atualizado.
  EDR = proteção que também vigia comportamento suspeito.
- [ ] **Cada pessoa tem sua senha de administrador**, forte e só dela. Nada de senha compartilhada.
- [ ] **Área de trabalho remota não fica aberta na internet.** Acesso de fora só por VPN, com verificação em duas etapas.
  Acesso remoto exposto é porta de entrada comum de ransomware.

5 Quem está olhando

equipamento sem vigia só é notado quando para

- [ ] Existe **monitoramento** que vigia disco, temperatura, serviços parados e servidor fora do ar.
- [ ] O alerta **chega a uma pessoa** que lê, não a uma tela que ninguém olha.
- [ ] O aviso funciona **fora do horário comercial**, em fim de semana e feriado.
- [ ] Há **um responsável definido** (pessoa ou fornecedor), com nome, telefone e acesso ao servidor.
- [ ] As **senhas e o passo a passo** estão anotados em local seguro, não só na cabeça de uma pessoa.
- [ ] E o backup? Tem checklist próprio: **maisseg.net.br/materiais/checklist-backup.pdf**

TESTE DE 5 MIN

Se o servidor parar agora, quem fica sabendo primeiro?

1. Seja sincero: **o técnico**, por um alerta, ou **o cliente no balcão**?
2. Abra o servidor e veja **quanto espaço livre** sobra no disco principal.
3. Confira a data da **última atualização de segurança** instalada.

Se foi "o cliente", se o disco está quase cheio ou ninguém sabe a data, o seu servidor precisa de atenção agora, não depois que parar.