

Checklist de Segurança para PMEs

As 24 verificações que separam uma empresa protegida de uma empresa exposta — em 15 minutos de avaliação.

Como usar:

Marque cada item que sua empresa ATENDE hoje. Ao final, some os pontos e consulte a tabela de resultado na última página. Não adivinhe: verifique de fato.

1. Acesso e Identidade

- | | |
|--|------------|
| ☐ A autenticação em dois fatores (MFA) está ativada em e-mail, sistemas de gestão e banco. | CRÍTICO |
| ☐ Não há senhas compartilhadas entre colaboradores. | CRÍTICO |
| ☐ Cada colaborador tem seu próprio usuário e as contas de ex-funcionários são desativadas em até 24h. | CRÍTICO |
| ☐ As senhas são únicas e gerenciadas por um cofre de senhas (não em planilhas ou post-its). | IMPORTANTE |
| ☐ Apenas as pessoas necessárias têm acesso administrativo aos sistemas. | IMPORTANTE |

2. Backups e Recuperação

- | | |
|--|------------|
| ☐ Os backups são automáticos e incluem todos os dados críticos. | CRÍTICO |
| ☐ Existe uma cópia fora da rede (nuvem ou mídia offline/imutável). | CRÍTICO |
| ☐ Um teste de restauração foi feito nos últimos 3 meses — e funcionou. | CRÍTICO |
| ☐ O backup não fica acessível pelas mesmas credenciais da rede principal. | IMPORTANTE |

3. Sistemas Atualizados

- | | |
|--|-------------|
| ☐ Sistemas operacionais e programas estão com as atualizações automáticas ativadas. | CRÍTICO |
| ☐ Os sistemas de gestão (ERP, CRM, emissão de notas) estão em versão suportada pelo fabricante. | IMPORTANTE |
| ☐ Há um inventário atualizado dos computadores, servidores e sistemas da empresa. | RECOMENDADO |

4. Pessoas e Conscientização

- ☐ A equipe recebeu treinamento anti-phishing nos últimos 6 meses. **CRÍTICO**
- ☐ Existe uma orientação clara do que fazer ao receber um e-mail suspeito. **IMPORTANTE**
- ☐ Novo colaborador passa por orientação de segurança no onboarding. **RECOMENDADO**

5. Monitoramento e Proteção

- ☐ Todos os computadores têm antivírus/EDR instalado e ativo. **CRÍTICO**
- ☐ Os alertas de segurança são monitorados (por alguém, dentro ou fora da empresa). **CRÍTICO**
- ☐ O acesso remoto à rede usa VPN/MFA — nunca RDP ou senha simples expostos na internet. **CRÍTICO**
- ☐ O Wi-Fi da empresa tem senha própria, separada da rede de visitantes. **IMPORTANTE**
- ☐ Existe um software de gestão de dispositivos para aplicar políticas de segurança. **RECOMENDADO**

6. Resposta e Conformidade (LGPD)

- ☐ Existe um plano escrito de resposta a incidentes: quem liga para quem, em que ordem. **CRÍTICO**
- ☐ Existe contato de um especialista/parceiro de segurança para acionar em emergência. **IMPORTANTE**
- ☐ A empresa sabe quais dados pessoais coleta, onde estão e por quanto tempo são guardados. **IMPORTANTE**
- ☐ Há política de retenção e descarte seguro de dados e equipamentos. **RECOMENDADO**

Como interpretar seu resultado

0 a 8 itens marcados

ALERTA MÁXIMO: sua empresa está exposta a alto risco de incidente grave. Ataques de ransomware exploram exatamente esses pontos. Recomendamos agir nas verificações CRÍTICAS já nas próximas 2 semanas.

9 a 16 itens marcados

ATENÇÃO: há proteção básica, mas os gaps restantes provavelmente incluem itens críticos. Um único ponto fraco é suficiente para um atacante entrar. Priorize os CRÍTICOS ainda não marcados.

17 a 24 itens marcados

PROTEGIDO: nível acima da média das PMEs. Mantenha os testes de backup, os treinamentos e revise este checklist a cada 6 meses — a ameaça evolui continuamente.

Lembrete importante:

Um checklist marca presença de processos, não eficácia deles. Um backup só é real depois de testado; um MFA só protege se estiver em TODOS os acessos. A avaliação mais confiável é feita por um especialista.

Prefere uma avaliação feita por especialistas?

EA Soluções oferece um diagnóstico gratuito de 30 minutos: identificamos suas vulnerabilidades mais críticas e apresentamos um plano de proteção sob medida para o seu negócio.

AGENDAR DIAGNÓSTICO GRATUITO