



MTR
Cyber Sec

Os 10 Maiores Erros de Segurança que as Pequenas Empresas Cometem

Proteja sua empresa contra ataques cibernéticos antes que seja tarde demais.

Author: MTR CYBER SEC



Introdução

40%

Ataques direcionados

Dos ataques cibernéticos são direcionados a pequenas e médias empresas

2

Fatores de risco

Falta de estrutura ou desconhecimento técnico

Você sabia que mais de 40% dos ataques cibernéticos são direcionados a pequenas e médias empresas?

Por falta de estrutura ou desconhecimento técnico, essas empresas acabam se tornando alvos fáceis.

Este guia foi criado para mostrar os erros mais comuns — e como corrigi-los de forma prática.

Erros #1 e #2

Erro #1: Não manter sistemas atualizados

Deixar sistemas, CMS ou plugins desatualizados abre brechas exploradas por hackers.

Correção: Ative atualizações automáticas ou mantenha um cronograma de atualizações mensais.

Erro #2: Usar senhas fracas ou repetidas

Muitas empresas ainda usam senhas como "123456" ou "admin123".

Correção: Use gerenciadores de senha e exija senhas fortes com autenticação em dois fatores (2FA).



Erros #3 e #4

Erro #3: Ausência de backups automáticos

Sem backup, um ransomware pode destruir anos de dados.

Correção: Faça backups automáticos e frequentes, preferencialmente em nuvem + externo.

Erro #4: Falta de firewall ou antivírus corporativo

Muitas empresas ainda usam soluções gratuitas e domésticas.

Correção: Invista em firewall UTM e antivírus com painel de controle centralizado.

Erros #5 e #6



Erro #5: Wi-Fi sem proteção adequada

Redes abertas ou com senha fraca são uma porta de entrada para ataques.

Correção: Use senha WPA2/WPA3, segmente redes (visitantes x internos) e desative WPS.



Erro #6: Não treinar os funcionários

Funcionários clicam em links maliciosos por falta de orientação.

Correção: Faça campanhas de conscientização e simulações de phishing regularmente.



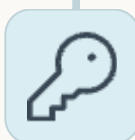
Erros #7 e #8



Erro #7: Aplicativos web sem análise de segurança

Sites e sistemas internos são frequentemente esquecidos.

Correção: Realize testes de intrusão e análises de vulnerabilidade periodicamente.



Erro #8: Compartilhamento de senhas entre colaboradores

Muitos funcionários usando o mesmo login compromete a rastreabilidade.

Correção: Crie logins individuais com permissões específicas por função.

Erros #9 e #10

1

Erro #9: Não ter política de segurança interna

Sem regras claras, colaboradores não sabem como agir.

Correção: Desenvolva uma política de segurança da informação e treine a equipe.

2

Erro #10: Ignorar a LGPD

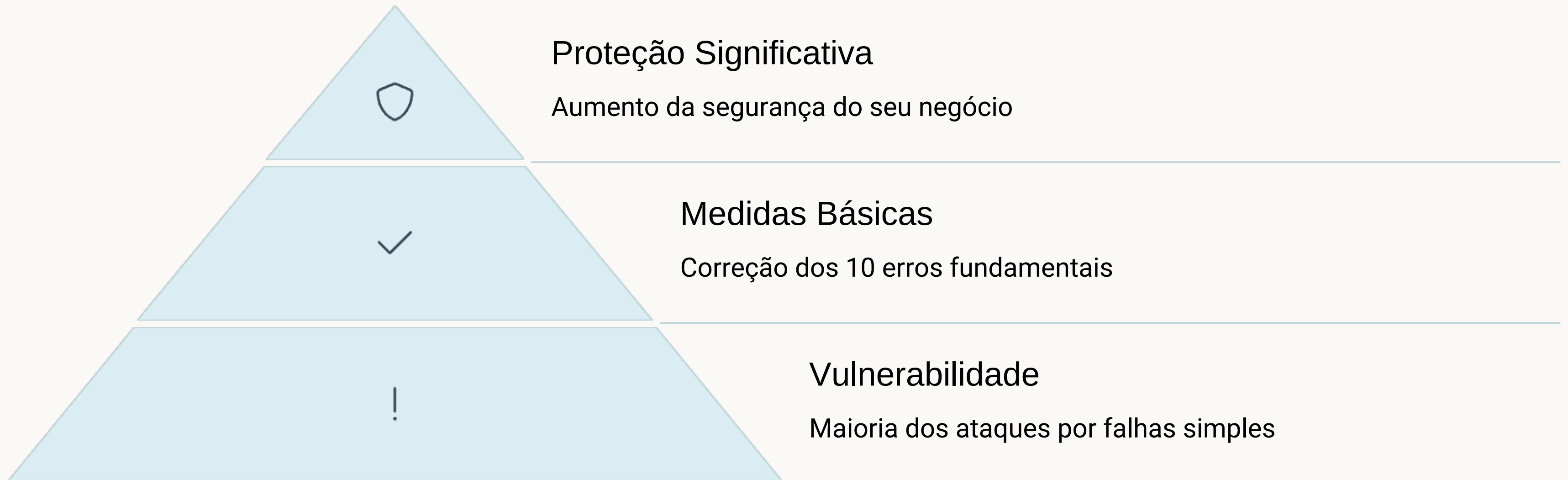
Deixar dados pessoais expostos pode gerar multas severas.

Correção: Adeque seus processos à Lei Geral de Proteção de Dados com apoio profissional.



LGPD
LEI GERAL
DE PROTEÇÃO
DE DADOS

Conclusão



A maioria dos ataques ocorre porque as medidas básicas de segurança não foram aplicadas.

Corrigir esses 10 erros pode aumentar significativamente a proteção do seu negócio.

Quer saber se sua empresa está segura?

Solicite agora um Pentest com um especialista da MTR Cyber Sec e descubra se você está vulnerável a ataques.

 Fale conosco pelo WhatsApp (62) 99651-9273

 Ou envie um e-mail para: contato@mtrcybersec.com.br

 <https://www.mtrcybersec.com.br>