Etapa 3 – Boas Práticas e Gestão de Risco (Detalhada)

a. Identificação e Classificação dos Riscos

Com base nas vulnerabilidades mapeadas na MedClin, os riscos foram analisados conforme sua **probabilidade de ocorrência** e **impacto nos ativos da informação** (dados, sistemas, reputação da clínica). A seguir, uma **matriz de risco** simplificada para ilustrar a análise:

RISCO IDENTIFICADO	PROBABILIDADE	IMPACTO	NÍVEL DE RISCO
Phishing	Alta	Alta	Alto
Malware/Ransomware	Média	Alta	Alto
Engenharia Social	Média	Média	Médio
Acesso indevido a dados	Alta	Alta	Alta
Falhas de configuração (servidores, rede)	Média	Alta	Alto
Atualizações de segurança não aplicadas	Alta	Média	Alto
Ausência de criptografia (em trânsito e repouso)	Média	Alta	Alto
Funcionário mal-intencionado (ameaça interna)	Baixa	Alta	Médio
Falta de autenticação multifator (MFA)	Alta	Alta	Alto
Erro humano (envio incorreto de dados)	Média	Média	Médio

Nota: Nível de risco é classificado como **Alto**, **Médio** ou **Baixo** com base na combinação entre probabilidade e impacto.

b. Políticas de Segurança e Boas Práticas Alinhadas às Normas

Com base nos riscos acima e seguindo normas como **LGPD**, **ISO/IEC 27001** e o **Marco Civil da Internet**, foram definidas as seguintes políticas:

1º **Política de Controle de Acesso**

- Acesso apenas por necessidade (least privilege)
- MFA obrigatória para administradores e médicos
- Bloqueio automático após tentativas de login malsucedidas

2º **Política de Backup e Recuperação**

- Backups automáticos diários e semanais
- Armazenamento em nuvem criptografado
- Testes regulares de restauração de dados

3º **Política de Atualização de Sistemas**

- Atualizações automáticas e monitoramento de falhas
- Patches aplicados no máximo 72h após liberação crítica

4º **Política de Uso de Dispositivos Pessoais (BYOD)**

- Acesso remoto apenas com VPN e dispositivo registrado
- Instalação obrigatória de antivírus corporativo

5º **Política de Educação e Conscientização de Usuários**

- Treinamentos semestrais sobre phishing, proteção de dados e boas práticas
- Simulações de ataques de engenharia social

6º **Política de Segurança no Aplicativo Móvel**

- Validação de segurança nas APIs
- Limitação de permissões do app
- Atualizações forçadas e criptografia local de dados

c. Registro Estruturado e Visual (Recomendação)

- **Tabelas de risco** (como a acima)
- **Fluxogramas** de controle de acesso e resposta a incidentes
- **Matriz de responsabilidade** (ex.: quem monitora, executa, aprova)
- **Gráficos de impacto x probabilidade** para priorização de mitigação