Etapa 2 – Ameaças, Vulnerabilidades e Normas de Segurança

a. Mapeamento de Ameaças e Vulnerabilidades

A seguir são apresentadas as principais ameaças e vulnerabilidades identificadas no ambiente operacional da **MedClin**, uma clínica médica de médio porte que lida com dados sensíveis de pacientes por meio de sistemas informatizados, servidores em nuvem.

Principais ameaças e vulnerabilidades mapeadas:

- **Phishing**
  Tentativas de enganar colaboradores por meio de e-mails ou mensagens falsas, com o objetivo de capturar credenciais de acesso ou informações confidenciais de pacientes.

- **Malware e Ransomware**
  Risco de infecção por softwares maliciosos que podem comprometer sistemas ou criptografar dados importantes como prontuários eletrônicos.

- **Engenharia Social**
  Manipulação psicológica de funcionários para que forneçam acesso a sistemas internos da clínica.

- **Acesso Indevido**
  Falta de controle de permissões pode permitir que usuários sem autorização acessem dados sensíveis de pacientes ou informações administrativas.

- **Falhas de Configuração**
  Configurações incorretas de servidores, roteadores ou firewalls podem expor serviços da clínica à internet de forma insegura.

- **Ausência de Criptografia**
  Dados armazenados ou transmitidos sem criptografia aumentam o risco de interceptação e vazamento de informações sensíveis.

- **Atualizações e Patches Não Aplicados Regularmente**
  Atrasos na aplicação de atualizações de segurança deixam sistemas vulneráveis a ataques conhecidos.

- **Erro Humano**
  Envio incorreto de informações, como resultados de exames para pacientes errados, representa risco frequente e crítico.

- **Funcionários Mal-Intencionados (Ameaça Interna)**
  Colaboradores que, por insatisfação ou interesses pessoais, podem deliberadamente causar danos ou vazamento de dados.

- **Falta de Autenticação Multifator (MFA)**
  A ausência de autenticação adicional nos acessos administrativos e médicos compromete a segurança de contas com privilégios elevados.

b. Normas, Leis e Regulamentações Pertinentes

A MedClin está sujeita a diversas normas legais e regulamentações, tanto nacionais quanto internacionais, que visam proteger os dados e garantir boas práticas de segurança da informação. A seguir, as principais diretrizes aplicáveis:

- **LGPD (Lei Geral de Proteção de Dados – Brasil)**
  Legislação que regula o tratamento de dados pessoais no Brasil, exigindo medidas técnicas e organizacionais para garantir segurança, privacidade e transparência no uso das informações.

- **Marco Civil da Internet**
  Estabelece princípios, garantias e direitos para o uso da internet no Brasil, incluindo proteção de dados, privacidade e responsabilidade na guarda de registros de acesso.

- **ISO/IEC 27001**
  Norma internacional que define padrões para a implantação e gestão de um Sistema de Gestão de Segurança da Informação (SGSI), assegurando a confidencialidade, integridade e disponibilidade das informações.

- **Políticas Internas da MedClin (em desenvolvimento)**
  A clínica pretende implementar diretrizes internas específicas que regulem o uso de senhas, acesso remoto, backup de dados, uso de dispositivos pessoais (BYOD), plano de resposta a incidentes e capacitação de usuários.