Empresa : CONSULTÓRIO ODONTOLOGICO

Cenário: Realização de atendimento ao cliente, exames/prontuários e dados de pagamento.

Este plano abrange todas as atividades essenciais do consultório, incluindo:

- Atendimento a pacientes.
- Agendamento e gerenciamento de consultas.
- Acesso a prontuários eletrônicos.
- Processamento de pagamentos.
- Comunicação interna e externa.

Principais Riscos

- **Falha de Sistema:** Indisponibilidade do software de gestão.
- **Ataque Cibernético:** Risco de vazamento de dados.
- **Falta de Internet:** Impacto na comunicação e nos serviços online.

Podemos considerar alguns acontecimentos como: ataques cibernéticos, malware, ransoware, phising.
Malvare > rouba informações
Ransoware >bloqueia informações
Phising > obtém dados

- **Normas e boas práticas**

  - LGPD – curso de boas práticas, regulamentos e tratamento de dados

  - Política de acesso – uso de autenticação, pode ser usado o AZURE para criação de AD

- Política de gestão

  Malware -> Impacto ALTO / Probabilidade ALTA
  Ransoware -> Impacto ALTO/ Probabilidade ALTA
  Vazamento de dados -> Impacto ALTO/ Probabilidade ALTA

Soluções:
Treinamentos, manter os sistemas sempre atualizados, criptografia da dados em ataque ransoware isola o sistema, desliga a internet e formata a maquina.
Em caso de de vazamento de dados notificar os pacientes e reforçar segurança. Fazer backup diário em maquinas locais e na nuvem.
Fazer treinamento sobre ameaças e falhas humanas, colocar política de senha segura.

Redundancia de falha na internet

Ter um link secundário para falhas, no caso de duas operadoras de internet.

Procedimentos manuais em papel, como agenda, prontuário em planilha excel, e etc. Em caso de queda em uso, salvar dados locais de forma manual.

Ter roteador failover – (um dispositivo ou configuração de rede que garante a continuidade da conexão à internet ao alternar automaticamente para uma conexão de backup quando a principal falha. Isso é essencial para empresas ou usuários que precisam de alta disponibilidade e não podem sofrer interrupções na internet.)

- Inventário
  Recursos :
  HARDWARE > computador, impressoras, roteador, ponto.
  SOFTWARE > Sistema odontológico, com banco de dados salvando em nuvem.
  REDES > cada maquina tem acesso via lancom switch de conexão.
  DADOS > o sistema trata os dados no back e criptografa e salva no banco, caso precise recuperar, busque pelo ID ou chave primária, sem exposição chamados mostrando os dados, sempre rodando do lado do servidor e o cliente somente gerando as telas.

  PLANO

- O princípio de segurança utilizado no **Plano de Continuidade** está relacionado principalmente à **Disponibilidade - protege o funcionamento do consultório contra falhas inesperadas, garantindo que os serviços continuem disponíveis para os profissionais e pacientes. Isso está diretamente ligado ao princípio da disponibilidade dentro da segurança da informação.**

ARTIGOS :
https://guiaconsultorio.boaconsulta.com/seguranca-da-informacao
https://gestaodesegurancaprivada.com.br/plano-de-seguranca-da-informacao-psi-o-que-como-elaborar-exemplo
https://www.gestaods.com.br/protecao-de-dados-em-clinicas-e-consultorios/
https://www.pixeon.com/blog/praticas-essenciais-para-seguranca-da-informacao-na-area-da-saude/