**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.

• Falha humana: A falta de conhecimento em segurança digital pode acarretar em vazamento de informações.

**Podemos considerar alguns acontecimentos como: ataques**

**cibernéticos, malware, ransoware, phising.**

**Malvare** > rouba informações

**Ransoware** >bloqueia informações

**Phising** > obtém dados

**Normas e boas práticas**

* **LGPD** (**Lei nº 13.709**, de 14 de agosto de 2018) – Lei Geral de Proteção 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 máquina.**

* Em caso 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.
* Redundância de falha na internet
* Possuir 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 máquina 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.

**A segurança da informação em uma clínica odontológica deve se pautar nos seguintes princípios:**

* **Confidencialidade:** As informações dos pacientes, como históricos médicos, exames e tratamentos realizados, devem ser acessadas exclusivamente por profissionais autorizados. A confidencialidade é essencial para proteger os dados pessoais e garantir a privacidade dos pacientes.
* **Integridade:** A precisão e a consistência dos dados devem ser mantidas, de modo que as informações não sejam alteradas ou corrompidas sem a devida autorização. A integridade é crucial para a continuidade e qualidade do atendimento odontológico.
* **Disponibilidade:** Os sistemas e dados devem estar acessíveis sempre que necessário para os profissionais da clínica, garantindo que a infraestrutura de TI suporte o funcionamento diário da clínica sem interrupções significativas.

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/