UNIFACIMP-WYDEN
CURSO DE SISTEMAS DE INFORMAÇÃO

PLANO BÁSICO DE SEGURANÇA DA INFORMAÇÃO
MEDCLIN

Aluno 1 – Ilderlan de Jesus Melo
Aluno 2 – Mateus Bizerra da Silva
Aluno 3 – Matheus dos Reis
Aluno 4 – Marcos Antonio Silva Lima

Imperatriz-MA
2025

Sumário

1. Introdução

Este relatório apresenta o Plano Básico de Segurança da Informação desenvolvido para a MedClin, uma clínica médica de médio porte que atua com telemedicina e atendimentos presenciais. A proposta é identificar vulnerabilidades, mapear ameaças, aplicar normas e propor boas práticas, bem como estruturar um plano de continuidade de negócios que assegure a resiliência institucional.

A clínica possui estrutura tecnológica baseada em servidores em nuvem, redes locais, sistemas de prontuário eletrônico e aplicativos móveis. A segurança da informação é crítica para garantir a confidencialidade, integridade e disponibilidade dos dados dos pacientes e dos processos administrativos.

2. Ameaças, Vulnerabilidades e Normas de Segurança

Diversas ameaças e vulnerabilidades foram identificadas: phishing, malware/ransomware, engenharia social, falhas de configuração, acesso indevido, ausência de criptografia, atualizações pendentes, erros humanos, falhas no aplicativo móvel, e ausência de autenticação multifator.

As normas e leis aplicáveis incluem a Lei Geral de Proteção de Dados (LGPD), o Marco Civil da Internet, a norma ISO/IEC 27001, além de políticas internas a serem implementadas.

3. Boas Práticas e Gestão de Risco

Foi realizada uma análise de risco considerando probabilidade e impacto. Com base nisso, foram implementadas políticas como controle de acesso baseado em privilégios mínimos, backup automatizado, atualizações de sistemas em até 72 horas, uso de VPN, autenticação multifator e treinamentos recorrentes para os colaboradores.

Tabela 1 – Exemplos de riscos avaliados:

Risco	Probabilidade	Impacto	Classificação
Phishing	Alta	Alta	Alto
Erro humano	Média	Alta	Médio

4. Plano de Continuidade de Negócio

Os processos críticos identificados incluem acesso ao sistema de prontuário, agendamentos, infraestrutura de rede, comunicação e banco de dados. O PCN prevê estratégias específicas para restaurar cada processo em prazos definidos, mantendo o funcionamento mínimo da operação.

A governança do plano é clara, com papéis definidos para cada tipo de incidente. O coordenador de TI é responsável pela ativação do plano, a secretária-chefe cuida da comunicação com pacientes, e o jurídico garante o cumprimento da LGPD e notificação à ANPD, se necessário.

5. Conclusão

A segurança da informação é essencial para a continuidade e confiabilidade dos serviços prestados pela MedClin. O trabalho identificou riscos, definiu medidas de controle, mapeou normas pertinentes e desenvolveu um plano de continuidade alinhado às melhores práticas. O próximo passo será a implementação e o teste prático de cada medida definida.

6. Referências

CABRAL, R. F.; CAPRINO, E. Fundamentos de Segurança da Informação. São Paulo: Editora Ciência Moderna, 2020.

HINTZBERGEN, J. et al. Fundamentos de Segurança da Informação. Rio de Janeiro: Elsevier, 2019.

STANEK, W. Manual do Administrador de Segurança da Informação. Alta Books, 2020.

BARRETO, A. M.; BRASIL, F. LGPD Comentada. São Paulo: Juspodivm, 2021.

GALVÃO, R. Segurança Cibernética: aspectos técnicos e legais. Brasília: IDP, 2020.

MANOEL, V. Segurança de Sistemas: princípios e práticas. São Paulo: Érica, 2021.

STALLINGS, W. Segurança em Redes de Computadores. São Paulo: Pearson, 2017.

VANCIM, J. L. Segurança da Informação: da teoria à prática. Campinas: Papirus, 2022.