**Documento de Políticas de Segurança da Informação**

Empresa Fictícia: Vida Mais Clínica Integrada

Consultoria em Segurança:

Karla Santos - 825149900

Eduarda Molina - 825154538

Julia Richelly - 825150438

Caio Barbosa – 825154397

**Visão Geral**

Este documento define políticas básicas de segurança da informação para a VidaMais Clínica Integrada, uma pequena clínica com 15 colaboradores, que lida com dados sensíveis de pacientes. O objetivo é proteger essas informações contra acessos não autorizados, perda total ou vazamento de dados .

**Política de Acesso e Controle de Usuários**

Diretrizes

* Todos os funcionários terão usuário e senha individuais para acesso aos sistemas internos (prontuário eletrônico, agendamento e faturamento).
* Os acessos serão concedidos conforme a função: recepção, enfermagem, médicos, administração.
* Contas de ex-funcionários serão desativadas imediatamente após o desligamento.
* Senhas devem ser trocadas a cada 60 dias e não podem ser repetidas nas últimas 3 alterações.
* Acesso a informações de pacientes será registrado em logs de auditoria.
* Sistema bloqueia automaticamente o usuário após 5 tentativas falhas de login.

**Justificativa**

A clínica lida com dados protegidos pela LGPD e deve restringir o acesso a informações sensíveis somente a profissionais autorizados, protegendo a privacidade dos pacientes.

**Política de Uso de Dispositivos Móveis e Redes**

Diretrizes

* É proibido o uso de dispositivos pessoais (celulares, pendrives) para armazenar ou transferir dados de pacientes.
* O Wi-Fi da clínica será dividido em duas redes:
* Rede Interna Segura (apenas para equipamentos da clínica)
* Rede de Visitantes (uso público, sem acesso a sistemas internos)
* Tablets e notebooks da clínica devem possuir:
* Senha de acesso
* Antivírus atualizado
* Bloqueio automático após inatividade de 5 minutos
* Em caso de perda de dispositivo, a equipe de TI será notificada imediatamente para bloqueio remoto (quando aplicável).

**Justificativa**

O uso inadequado de dispositivos e redes pode comprometer dados sensíveis. A separação das redes e o controle dos dispositivos reduzem significativamente o risco de ataque ou vazamento.

**Diretrizes para Resposta a Incidentes de Segurança**

Diretrizes

Todo funcionário deve relatar imediatamente qualquer atividade suspeita ao responsável técnico (ex: e-mails estranhos, lentidão anormal, arquivos desaparecendo).

* Acesso não autorizado a prontuários
* Vírus/ransomware
* Falha de sistema que exponha dados de pacientes
* Em caso de incidente:
* Identificar e conter a ameaça
* Notificar a diretoria e registrar o ocorrido
* Analisar causa e impacto
* Corrigir falhas e prevenir recorrência
* Incidentes relacionados a dados pessoais serão avaliados para possível notificação à ANPD (Autoridade Nacional de Proteção de Dados), conforme a LGPD.

**Justificativa**

Ter um plano claro de resposta minimiza os impactos de ataques e falhas, além de garantir conformidade com as leis e proteger a reputação da clínica.

**Política de Backup e Recuperação de Desastres**

Diretrizes

* O sistema de prontuário eletrônico será backupado automaticamente todos os dias, em horário fora do expediente.
* Os backups serão mantidos:
* Localmente (servidor físico na clínica)
* Em nuvem (servidor criptografado, fora do local)
* Os arquivos de backup terão criptografia e acesso restrito apenas ao responsável técnico.
* Testes de restauração serão realizados a cada 3 meses.
* Em caso de desastre (ex: incêndio, ataque cibernético), o tempo máximo para recuperação será de 24 horas.

**Justificativa**

Em ambientes de saúde, dados dos pacientes são críticos e não podem ser perdidos. Um bom plano de backup garante a continuidade do atendimento mesmo em situações de falha ou emergência.