

# Plano Básico de Segurança da Informação MedClin

Este slide detalha o Plano Básico de Segurança da Informação para a MedClin, uma clínica médica que integra telemedicina e atendimentos presenciais. Nosso objetivo é fortalecer a resiliência institucional, identificando vulnerabilidades, mapeando ameaças e propondo boas práticas, além de estruturar um plano de continuidade de negócios.

A MedClin opera com servidores em nuvem, redes locais, prontuários eletrônicos e aplicativos móveis, tornando a segurança da informação crucial para a confidencialidade, integridade e disponibilidade dos dados dos pacientes e processos administrativos.



## Cyberotrdewvy Phirst



Credunt

### Stage7

#### Cystmatey

This course of correct revenue buting  
orsterequentios reryrttaon ture comet  
and red til the insar sauce,  
upsermese.



Seft 1

#### Themerley

This unagslieed of occur arobet er curlibty  
anoh the chiers, conette coirconcuree tuthe  
stplee cours ceneurent the curgungtry tiife  
upsermese.



Securint

### Pistines

Use of Security Manger  
Unas of he rreente of ressee  
Formative emprentes sumetlife to your  
torie all the mellesture.



Secur 2



Seft 2

#### Cystmatey

This anasyl seccurent unferstmeer ofing  
this coog's redeowed't ror cet nora onare  
secomes and prafice naffe roms coionet  
catery ne you of nen nande.



Seft 3

#### Inpumater

That unagelieties arecurpment of sollation  
Flise caagotilee couned tormest ecoudt you  
anddnatios cuneurent to curreyoundstife  
orteamere.

# Sumário do Plano de Segurança



## Introdução

Apresentação do plano e seu propósito para a MedClin.



## Ameaças, Vulnerabilidades e Normas

Identificação de riscos e leis aplicáveis.



## Boas Práticas e Gestão de Risco

Implementação de políticas e análise de riscos.



## Plano de Continuidade de Negócio

Estratégias para manter operações em caso de incidentes.

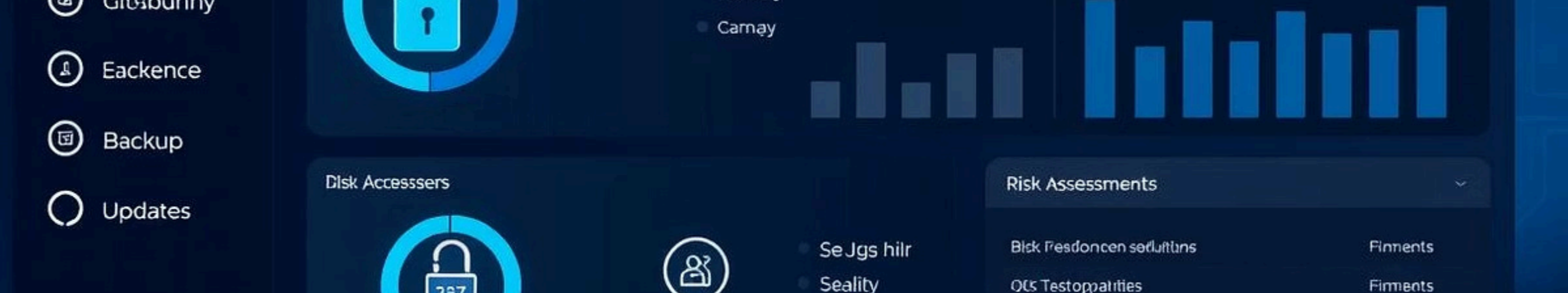
# Ameaças, Vulnerabilidades e Normas de Segurança

## Ameaças e Vulnerabilidades

- Phishing e Malware/Ransomware
- Engenharia Social
- Falhas de Configuração e Acesso Indevido
- Ausência de Criptografia e Atualizações Pendentes
- Erros Humanos e Falhas em Aplicativos Móveis
- Ausência de Autenticação Multifator

## Normas e Leis Aplicáveis

- Lei Geral de Proteção de Dados (LGPD)
- Marco Civil da Internet
- Norma ISO/IEC 27001
- Políticas Internas de Segurança



# Boas Práticas e Gestão de Risco

## Controle de Acesso

Baseado em privilégios mínimos para garantir que apenas usuários autorizados acessem dados sensíveis.

## Backup Automatizado

Garante a recuperação de dados em caso de perda ou corrupção, com rotinas regulares e seguras.

## Atualizações de Sistemas

Realizadas em até 72 horas para corrigir vulnerabilidades e manter a segurança dos softwares.

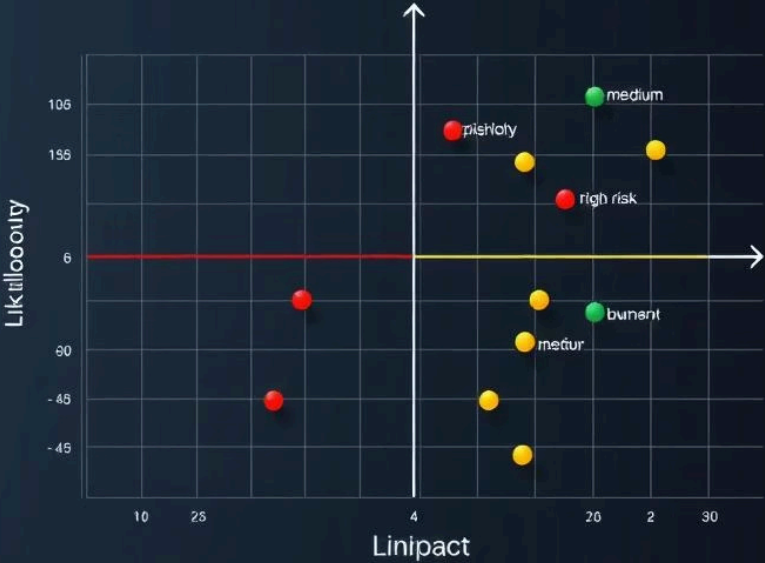
## Autenticação Multifator e VPN

Reforçam a segurança do acesso e a proteção da rede, especialmente em telemedicina.

# Análise de Risco

Phishing	Alta	Alta	Alto
Erro Humano	Média	Alta	Médio

A análise de risco considerou a probabilidade e o impacto de cada ameaça, permitindo a classificação dos riscos e a priorização das medidas de mitigação. O phishing, por exemplo, foi classificado como alto devido à sua alta probabilidade e impacto potencial nos dados da clínica.



# Plano de Continuidade de Negócio (PCN)



## Processos Críticos

Acesso ao prontuário, agendamentos, infraestrutura de rede, comunicação e banco de dados.



## Estratégias de Restauração

Previsão de prazos definidos para restaurar cada processo, garantindo o funcionamento mínimo da operação.



## Governança do Plano

Papéis claros para cada tipo de incidente, com responsabilidades definidas para a equipe.





# Governança do Plano de Continuidade



## Coordenador de TI

Responsável pela ativação do plano e gestão técnica dos incidentes.



## Secretária-Chefe

Cuida da comunicação com pacientes e stakeholders durante o incidente.



## Departamento Jurídico

Garante o cumprimento da LGPD e notificação à ANPD, se necessário.





# Conclusão e Próximos Passos

## Identificação de Riscos

Mapeamento completo das ameaças e vulnerabilidades da MedClin.

## Definição de Controles

Estabelecimento de medidas de segurança e boas práticas.

## Plano de Continuidade

Desenvolvimento de um PCN alinhado às melhores práticas.

## Implementação e Teste

Próximo passo crucial para validar a eficácia das medidas definidas.