BioHealth

Systems

METODOLOGIA E PLANO DE GESTÃO DE RISCOS DE TI

"Este documento é uma versão simplificada para fins de demonstração de portfólio técnico, focando na estrutura estratégica e alinhamento com os frameworks COBIT e ISO."

Nome da empresa: BioHealth Systems

Tipo de documento: Metodologia e Plano de Gestão de Riscos de TI

Data de vigência: 01/01/2026

Framework de Referência: ISO/IEC 27005 e ISO 31000

BioHealth
Systems

Processo de Avaliação de Riscos (Risk Assessment)

Seguimos o fluxo da ISO 27005:

- **Identificação:** Mapeamento de ativos (Ex: Prontuário Eletrônico, Servidores Cloud), ameaças (Ex: Ransomware) e vulnerabilidades (Ex: Sistemas desatualizados).
- **Análise:** Determinação da Probabilidade (P) e do Impacto (I).
- **Avaliação:** Cálculo do Nível de Risco ($R = P \times I$).

BioHealth
Systems

Critérios de Impacto (Exemplo de Matriz)

Para a BioHealth, o impacto é medido em quatro dimensões:

- **Operacional:** Interrupção de cirurgias ou exames.
- **Legal/Compliance:** Multas da ANPD (LGPD).
- **Reputacional:** Perda de confiança dos pacientes.
- **Financeiro:** Perda de receita e custos de remediação.

Amostra do Registro de Riscos (Risk Register)

Abaixo, uma simulação de como os riscos são priorizados:

ID	Ameaça	Impacto Potencial	P	I	Nível	Estratégia de Tratamento
R-01	Ataque de Ransomware	Indisponibilidade de Prontuários	4	5	20 (Crítico)	Mitigar: Implementar backups offline e MFA.
R-02	Vazamento de Dados	Multas LGPD e Exposição de Pacientes	3	5	15 (Alto)	Mitigar: Criptografia de banco de dados
R-03	Falha de Energia (Data Center)	Queda temporária de sistemas locais	2	4	8 (Médio)	Transferir: Migrar carga para nuvem (SaaS).

BioHealth
Systems

Matriz de Calor (Heat Map)

Os riscos são plotados em uma matriz 5x5:

- **Área Vermelha (15-25):** Requer ação imediata e reporte ao Comitê Executivo.
- **Área Laranja (8-14):** Ações planejadas para o próximo trimestre.
- **Área Amarela (1-7):** Risco aceito ou monitorado.

BioHealth
Systems

Monitoramento Contínuo

Os riscos não são estáticos. A BioHealth realiza revisões semestrais ou sempre que houver mudanças significativas na infraestrutura de TI.

BioHealth
Systems

Isenção de responsabilidade

Este documento representa um caso fictício desenvolvido para fins profissionais e educacionais e não reflete nenhuma organização real.