BioHealth

Systems

FRAMEWORK DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

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

BioHealth
Systems

Nome da empresa: BioHealth Systems
Tipo de documento: Framework do Sistema de Gestão de Segurança da Informação (SGSI)
Data de vigência: 01/01/2026
Framework de Referência: ISO/IEC 27001:2022

BioHealth
Systems

Introdução

Este documento define o modelo de governança de segurança da informação adotado pela BioHealth Systems para proteger seus ativos críticos e garantir a conformidade com as regulamentações de saúde (LGPD).

BioHealth
Systems

Liderança e Comprometimento

A segurança da informação na BioHealth não é apenas uma função técnica, mas uma responsabilidade da alta direção.

- **Aprovação da PSI:** A Política de Segurança da Informação (PSI) é revisada e aprovada anualmente pelo CEO.
- **Recursos:** A organização compromete-se com a alocação de orçamento específico para ferramentas de proteção e treinamento de pessoal.

BioHealth
Systems

Estrutura de Políticas de Segurança

O SGSI da BioHealth é composto por uma estrutura hierárquica de documentos:

- **Política de Segurança da Informação (Diretriz Master):** Regras gerais para todos os colaboradores.
- **Normas Específicas:**
  - Política de Controle de Acesso (Baseada no princípio do "Menor Privilégio").
  - Política de Criptografia (Para dados em repouso e em trânsito).
  - Política de Uso Aceitável (Diretrizes para uso de dispositivos da empresa).
- **Procedimentos (SOPs):** Manuais técnicos passo a passo (ex: Como resetar uma senha).

BioHealth
Systems

Seleção de Controles (Baseado no Anexo A da ISO 27001)

Como resultado da análise de risco (Projeto 3), priorizamos os seguintes domínios de controle:

- **Controles Organizacionais:** Gestão de ativos e segurança no relacionamento com fornecedores.
- **Controles de Pessoas:** Processo de integração (onboarding) com treinamento de conscientização em segurança.
- **Controles Físicos:** Restrição de acesso às salas de servidores e áreas de arquivos médicos.
- **Controles Tecnológicos:** Implementação de Endpoint Detection and Response (EDR) e Gestão de Vulnerabilidades.

BioHealth
Systems

Melhoria Contínua (Ciclo PDCA)

O SGSI opera sob o ciclo PDCA para garantir evolução constante:

- **Plan (Planejar):** Definir objetivos de segurança e avaliar riscos.
- **Do (Fazer):** Implementar as políticas e controles.
- **Check (Verificar):** Realizar auditorias internas e monitorar incidentes.
- **Act (Agir):** Corrigir falhas e atualizar processos com base nos resultados.

BioHealth
Systems

Indicadores de Sucesso (Métricas do SGSI)

- Percentual de colaboradores treinados em segurança (Meta: 100%).
- Tempo médio para detecção de vulnerabilidades críticas.
- Número de incidentes de segurança com impacto financeiro ou legal.

BioHealth
Systems

Isenção de responsabilidade

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