Laudo Técnico – Avaliação de Segurança e Governança de Sistema Hospitalar

1. Identificação do Sistema Avaliado

Nome do sistema:

Fabricante / Fornecedor:

Local da instalação:

Data da auditoria:

Versão do sistema:

Entidade auditada:

2. Objetivo do Laudo

Este laudo técnico visa avaliar o sistema [nome do sistema] quanto à conformidade com a Lei Geral de Proteção de Dados (LGPD), às normas de segurança da informação ISO/IEC 27001, ISO 27799, bem como às boas práticas definidas pela SBIS/CFM e outras regulamentações aplicáveis ao setor da saúde.

3. Metodologia Utilizada

A auditoria foi realizada por meio de:
- Entrevistas com responsáveis técnicos e usuários-chave
- Análise documental (políticas, logs, contratos, consentimentos)
- Testes técnicos (scan de vulnerabilidades, análise de logs, checagem de backups)
- Aplicação de checklist estruturado com base nas normas mencionadas

4. Resultados da Auditoria

4.1 Governança e LGPD

✓ O sistema possui política de privacidade implementada e aceita por pacientes e colaboradores.
✗ Falta política formal de retenção e descarte de dados.
✓ Mapeamento de dados sensíveis foi apresentado, com registro de tratamentos.

4.2 Segurança Técnica

✓ Autenticação por login e senha forte, com suporte a MFA.

✗ Ausência de criptografia em dados em repouso.

✓ Log de acessos ativos e auditáveis.

4.3 Continuidade e Incidentes

✗ Plano de resposta a incidentes não testado nos últimos 12 meses.

✓ Backups diários com restauração validada.

4.4 Conformidade Técnica com Padrões de Saúde

✓ Interoperabilidade com CNES e e-SUS utilizando HTTPS e JSON.

✗ Sistema ainda não certificado pela SBIS.

5. Conclusão Técnica

O sistema [nome] apresenta nível satisfatório de conformidade com os principais critérios de segurança da informação e governança de dados, porém requer melhorias urgentes nos seguintes pontos:

- Implementação de criptografia em repouso
- Atualização e teste do plano de resposta a incidentes
- Formalização da política de descarte de dados

6. Recomendações

- Implementar criptografia AES-256 para dados armazenados
- Aplicar testes semestrais de continuidade e resposta a incidentes
- Treinar usuários-chave sobre boas práticas de segurança e LGPD
- Solicitar certificação SBIS caso utilize prontuário eletrônico

7. Responsável Técnico

Nome completo:
Cargo / Função:
Certificações (ex: CISA, ISO 27001 LA, DPO):
Registro Profissional (ex: CREA/SC nº xxxxx):
Local e data:
Assinatura: