Para auditoria em sistemas voltados à **governança e segurança de dados**, especialmente no contexto de **sistemas hospitalares**, recomenda-se uma abordagem estruturada com base em **normas, frameworks e entidades reguladoras nacionais e internacionais**. A seguir, destaco as principais indicações, metodologias, órgãos e profissionais habilitados para **auditoria e emissão de laudos técnicos** com foco na segurança de dados:

---

1. Normas e frameworks indicados para auditoria de segurança de dados

Normas técnicas e regulamentações

- **LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018)**
  Fundamental para avaliação da conformidade de sistemas hospitalares que tratam dados sensíveis (ex: prontuários eletrônicos, históricos médicos, etc.).
- **Norma ISO/IEC 27001 e 27002**
  Indicadas para auditoria de Sistemas de Gestão de Segurança da Informação (SGSI), estabelecendo controles para proteger confidencialidade, integridade e disponibilidade da informação.
- **Norma ISO 27799:2016**
  Aplicação específica da ISO 27001 para o setor da **saúde**.
- **RDC 302/2005 (Anvisa)**
  Traz diretrizes para gestão da qualidade em laboratórios clínicos, impactando sistemas de informação laboratoriais (LIS).
- **Manual de Certificação SBIS-CFM**
  Normas da **Sociedade Brasileira de Informática em Saúde (SBIS)** e do **Conselho Federal de Medicina (CFM)** para avaliação de sistemas de prontuário eletrônico.

---

2. Instituições e empresas capacitadas para auditoria e laudos técnicos

Empresas especializadas (com atuação na região sul)

- **INCORP Tecnologia** (Chapecó/SC)
  Atua com gestão de TI hospitalar, podendo realizar análise de conformidade e segurança.
- **TNS Nanotecnologia e Sistemas (Xanxerê/SC)**
  Foca em sistemas hospitalares e soluções em gestão e segurança de TI.

- **Horus Engenharia de Software (Florianópolis/SC)**
  Especializada em soluções de segurança da informação, com experiência em auditorias.

Instituições públicas e universidades

- **UNOCHAPECÓ (Laboratório de Tecnologias em Saúde - LTS)**
  Pode emitir parecer técnico/acadêmico para avaliação de sistemas de saúde em parceria com o setor público ou privado.
- **IFSC e UFFS**
  Podem apoiar projetos com pesquisadores em cibersegurança e dados em saúde.

---

3. Etapas de uma auditoria com laudo técnico

Fases da auditoria:

1. **Planejamento e escopo**
   - Levantamento de sistemas envolvidos (ERP hospitalar, PEP, sistemas de imagem, etc.)
   - Identificação de requisitos legais (LGPD, ISO 27799)
2. **Levantamento técnico**
   - Avaliação de infraestrutura (firewall, backups, acesso remoto)
   - Inspeção de logs, controle de acessos, encriptação de dados
3. **Entrevistas e verificação documental**
   - Políticas de segurança, termos de consentimento, registro de incidentes
4. **Teste de segurança (pentest e varreduras automatizadas)**
   - Ferramentas como **OpenVAS**, **Nessus**, **Metasploit**, **OWASP ZAP**
5. **Análise de governança de TI**
   - Avaliação do uso de frameworks como **COBIT 2019**, **ITIL**, **NIST CSF**
6. **Elaboração do laudo técnico**
   - Contendo diagnóstico, riscos, conformidades e recomendações
   - Deve estar assinado por profissional habilitado (ex: engenheiro de computação, auditor de TI ou perito judicial)

---

4. Responsáveis legais por emissão de laudos técnicos

- **Engenheiro da Computação ou Analista de Sistemas com CREA ou CRA**
  Podem assinar laudos em conformidade com as normas técnicas e regulatórias.
- **Profissionais certificados em CISA, ISO 27001 Lead Auditor, DPO**
  Valorizam tecnicamente o laudo.
- **Empresas com CNAE de atividades de auditoria de sistemas ou cibersegurança**
  Podem emitir laudos com validade jurídica.

Considerações específicas para a região Oeste de SC

- A região possui diversos hospitais com sistemas integrados ao **AGHUse (SES-SC)** e a soluções de empresas como a **MV Sistemas**, **TOTVS Saúde**, **Wareline** e **SPDATA**. A auditoria deve considerar a **integração com os sistemas estaduais e federais** (CNES, e-SUS, e-SUS PEC, RNDS).
- **Chapecó**, **Xaxim**, **São Miguel do Oeste**, **Concórdia** e **Maravilha** possuem hospitais com forte atuação no SUS e privados, sendo foco para implementação de políticas robustas de segurança.

Referências técnicas

- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais.
- ABNT NBR ISO/IEC 27001:2022 – Tecnologia da Informação – Sistemas de Gestão de Segurança da Informação.
- ISO 27799:2016 – Health informatics – Information security management in health.
- COBIT 2019 Framework – ISACA.
- Guia de Boas Práticas da SBIS: https://www.sbis.org.br

MODELO DE CHECKLIST TÉCNICO PARA AUDITORIA EM SISTEMA HOSPITALAR

A. Governança e Conformidade com a LGPD

Item	Descrição	Conformidade	Observações
A.1	Existe um Encarregado de Dados (DPO)?	Sim/Não	Nome, cargo
A.2	Há políticas de privacidade e consentimento documentadas e aplicadas?	Sim/Não	URL, anexo
A.3	Realiza-se mapeamento de dados pessoais e sensíveis?	Sim/Não	Data da última revisão
A.4	Existem registros de tratamento de dados (Art. 37 LGPD)?	Sim/Não	Ferramenta usada
A.5	Existe política de retenção e descarte de dados?	Sim/Não	Tempo de retenção

---

B. Segurança Técnica da Informação (ISO 27001 / ISO 27799)

Item	Descrição	Conformidade	Observações
B.1	Os dados estão criptografados em repouso e em trânsito?	Sim/Não	Tipo de criptografia
B.2	Há controle de acesso com autenticação forte (MFA)?	Sim/Não	Aplicações com MFA
B.3	Existe segregação de funções no sistema?	Sim/Não	Perfis de usuários documentados
B.4	Os sistemas mantêm logs auditáveis?	Sim/Não	Retenção de logs
B.5	Backups são realizados periodicamente e testados?	Sim/Não	Frequência e testes
B.6	Existe monitoramento contínuo de vulnerabilidades?	Sim/Não	Ferramentas utilizadas

---

C. Resiliência e Continuidade Operacional

Item	Descrição	Conformidade	Observações
C.1	Há plano de continuidade de negócio (PCN)?	Sim/Não	Último teste realizado
C.2	Existe plano de resposta a incidentes de segurança?	Sim/Não	Responsável pela execução
C.3	Simulações de incidentes são realizadas regularmente?	Sim/Não	Frequência

---

D. Avaliação do Sistema de Informação Hospitalar (ERP, PEP, LIS, PACS)

Item	Descrição	Conformidade	Observações
D.1	O sistema é certificado pela SBIS/CFM (PEP)?	Sim/Não	Nome do sistema
D.2	Permite auditoria de acesso ao prontuário?	Sim/Não	Funcionalidade ativa
D.3	Atende aos requisitos da RDC 302/2005 (se aplicável)?	Sim/Não	Laboratórios conectados
D.4	Interopera com sistemas externos com segurança (CNES, RNDS, e-SUS)?	Sim/Não	Protocolos de segurança

---

TEMPLATE DE LAUDO TÉCNICO – 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 digitalizada ou eletrônica
