Relatório de Auditoria de Segurança da Informação

Hospital YSL – Pouso Alegre

Avaliação de Conformidade LGPD e Normas ISO

Objetivo e Escopo da Auditoria

Objetivo Principal

Avaliar conformidade das práticas de segurança contra políticas internas e obrigações legais (LGPD)

Escopo de Análise

Todos colaboradores, fornecedores e terceiros que utilizam sistemas do Hospital YSL

Análise baseada em ISO/IEC 27001, 27701, 20000, 38500 e Lei Geral de Proteção de Dados

Documentos Analisados

Política de Segurança da Informação

Diretrizes e controles de acesso corporativo

Política de Privacidade

Proteção de dados pessoais e direitos dos titulares

Plano de Backup e Recuperação

Continuidade operacional e recuperação de desastres

Relatório de Incidentes

Análise de eventos de segurança recentes

Sumário Executivo

A auditoria identificou **não conformidades críticas** na postura de segurança do Hospital YSL

Embora existam políticas estabelecidas, há falhas graves na implementação técnica e validação operacional

Não Conformidades Críticas Identificadas

Controles de Acesso Insuficientes

Política vs. Realidade

Proíbe acesso fora da atuação, mas **não há controle efetivo de permissões**

Senhas Fracas

Apenas **6 caracteres** com troca anual

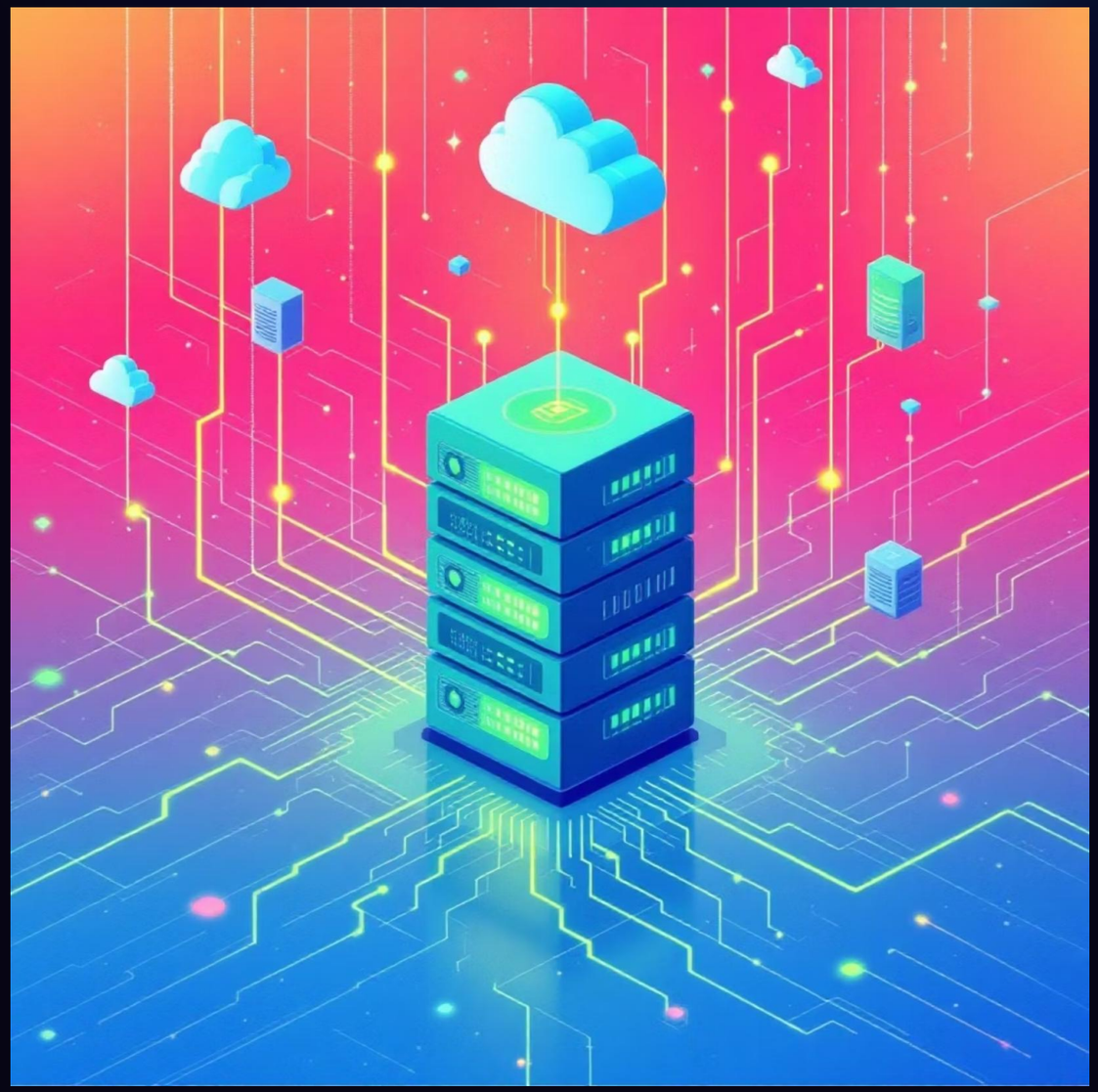
Ausência total de MFA

Incidente Relacionado

Vazamento de credenciais de residente em fórum online (Abril/2025)

Risco Crítico: Dados de pacientes acessíveis por colaboradores sem vínculo direto

Plano de Continuidade Falho



Sem Testes de Restauração

Nenhum teste realizado desde 2024

Retenção Insuficiente

Apenas 3 meses de backup

RTO/RPO Indefinidos

Sem métricas de recuperação

⚠ **Impacto Comprovado:** Queda de 3 horas no sistema de prontuário (Junho/2025)

Incidentes Críticos Recentes

1

Fevereiro/2025

Ataque de phishing bem-sucedido contra equipe administrativa

2

Abril/2025

Vazamento de credenciais de residente em fórum online

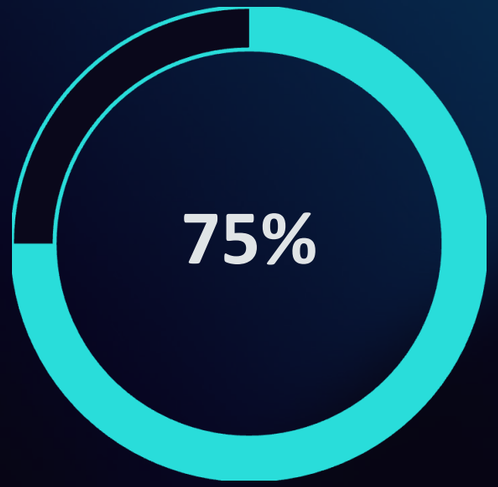
3

Junho/2025

Queda de sistema de 3 horas no prontuário eletrônico

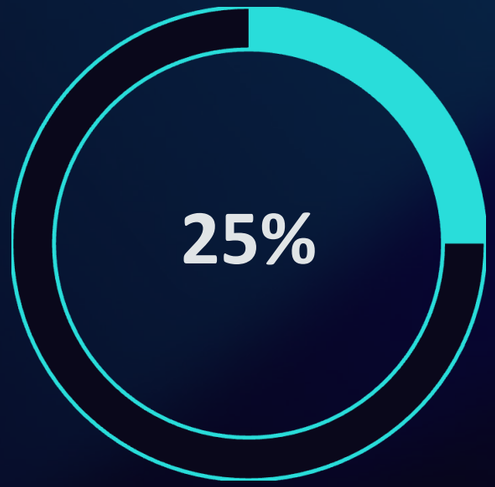
Estes incidentes validam as vulnerabilidades identificadas na auditoria

Classificação de Riscos



Riscos Críticos

Backup, privacidade e incidentes



Riscos Altos

Autenticação e conscientização

Área	Risco Identificado	Nível
Backup	Falta de testes, retenção insuficiente	Crítico
Privacidade	Política desatualizada (2022)	Crítico
Autenticação	Senhas fracas, ausência de MFA	Alto
Conscientização	Falta de treinamentos periódicos	Alto

Ações Prioritárias - 0 a 30 dias

01

Implementar MFA

Autenticação multifator em todos acessos administrativos, clínicos e remotos

02

Revisar Política de Senhas

Aumentar para mínimo 12 caracteres, eliminar trocas periódicas desnecessárias

03

Testar Backups

Realizar testes completos de restauração, documentar RTO e RPO

04

Atualizar Política de Privacidade

Nomear DPO, atualizar documento (última revisão: 2022)

Plano de Implementação Estruturado

0-30 dias

Prioridade Alta

- MFA obrigatório
- Política de senhas
- Testes de backup
- DPO e privacidade

30-90 dias

Prioridade Média

- Controle RBAC
- Classificação da informação
- Monitoramento SIEM
- Treinamento contínuo

90+ dias

Melhoria Contínua

- Certificação ISO 27701
- BCP avançado
- Auditoria periódica