Relatório de Auditoria

Organização: Hospital YSL - Pouso Alegre

Documentos Analisados: Políticas de Segurança da Informação, Política de Privacidade, Plano de Backup e Recuperação e Relatório de Incidentes de Segurança.

Objetivo e Escopo

Objetivo: Desta auditoria é avaliar a conformidade das práticas de segurança e privacidade do Hospital YSL contra suas próprias políticas internas, planos operacionais e obrigações legais (como LGPD). A análise visa identificar não conformidades, avaliar os riscos associados e propor recomendações de melhoria para garantir a confidencialidade, integridade e disponibilidade das informações corporativas tudo isso alinhado com normas internacionais (ISO/IEC 27001, ISO/IEC 27701, ISO/IEC 20000, ISO/IEC 38500) e legislações vigentes, como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD).

Escopo: Esta auditoria aplica-se a todos os colaboradores, fornecedores e terceiros que utilizam os sistemas do Hospital YSL. A análise focou nos seguintes artefatos fornecidos:

- Política de Segurança da Informação
- Política de Privacidade
- Plano de Backup e Recuperação
- Relatório de Incidentes de Segurança

Sumário Executivo

A auditoria identificou não conformidades críticas na postura de segurança do Hospital YSL. Embora existam políticas de segurança e privacidade, há falhas graves na sua implementação técnica e validação operacional.

As principais falhas incluem controles de acesso tecnicamente inexistentes ou fracos (como a falta de MFA e de controle de permissão), uma política de senhas insuficiente (6 caracteres com troca anual) e um plano de recuperação de desastres que não é validado (testes de restauração não realizados desde 2024).

Essas falhas são validadas por incidentes recentes, incluindo um ataque de phishing bem-sucedido , vazamento de credenciais de um residente e uma queda de sistema de 3 horas. Coletivamente, esses problemas expõem o hospital a riscos críticos de violação de dados sensíveis de pacientes, não conformidade com a LGPD e interrupção operacional severa.

Metodologia

A auditoria foi conduzida através da análise cruzada dos documentos fornecidos:

- Políticas de Segurança e Logs de Acesso: Verificação da aplicabilidade e eficácia dos controles declarados na política em contraste com os acessos monitorados e a ausência de controles-chave.
- Política de Privacidade e Incidentes: Análise da política de privacidade à luz dos incidentes de segurança ocorridos, avaliando a proteção dos dados dos titulares.
- Plano de Backup e Organograma: Avaliação do plano de continuidade do negócio em relação à sua execução e responsabilidades, considerando a estrutura da equipe de TI.

Análise de Não Conformidades, Riscos e Normas Relacionadas

A seguir, são apresentadas as principais não conformidades identificadas, os incidentes correlacionados, os riscos associados e sua relação com normas e legislações aplicáveis.

1. Controles de Acesso Insuficientes e Conflito de Políticas

   Não conformidade: A Política de Segurança proíbe acesso a setores fora da atuação do colaborador, porém não há controle efetivo de permissões. Além disso, a política de senhas prevê apenas 6 caracteres com troca anual, sem exigir autenticação multifator (MFA), mesmo em acessos remotos via VPN.

   Incidente Correlacionado: Vazamento de login e senha de residente em fórum online (Abril/2025).

Risco Associado (Crítico): A fragilidade das senhas e ausência de MFA tornam trivial o uso indevido das credenciais vazadas. Como não há restrição de permissões, dados de pacientes podem ser acessados por colaboradores sem vínculo direto, violando a confidencialidade.

Norma/Lei Relacionada: LGPD (Art. 46 – medidas técnicas de segurança para dados sensíveis) e ISO 27001 (Anexo A.9 – Controle de Acesso).

2. Plano de Continuidade de Negócios Não Validado

   Não conformidade: Embora exista rotina de backup (semanal completo e diferencial diário), não há testes de restauração desde 2024. A retenção é de apenas 3 meses e não há definição clara de RTO e RPO.

   Incidente Correlacionado: Queda de 3 horas no sistema de prontuário eletrônico (Junho/2025).

   Risco Associado (Crítico): Sem testes, não há garantia de recuperação em incidentes graves, como ransomware ou falha de hardware. A queda já demonstrou impacto operacional crítico, comprometendo a disponibilidade.

   Norma/Lei Relacionada: ISO 27001 (Anexo A.17 – Gestão da Continuidade do Negócio).

3. Gestão de Privacidade Desatualizada e Insegura

   Não conformidade: A Política de Privacidade está desatualizada (última revisão em 2022). Pacientes podem solicitar cópia de dados sensíveis por e-mail, sem critérios de segurança definidos. Não há classificação formal das informações (confidencial, restrita, pública).

   Risco Associado (Crítico): O uso de e-mail fragiliza a verificação de identidade e expõe dados médicos a risco de interceptação ou fraude. A ausência de classificação impede que dados sensíveis recebam proteção diferenciada.

   Norma/Lei Relacionada: LGPD (direitos dos titulares e princípio da segurança) e ISO 27701 (Gestão de Informação de Privacidade).

4. Falha na Conscientização de Colaboradores

Não conformidade: A política proíbe o compartilhamento de credenciais, porém incidentes recentes revelam a inobservância dessa regra. Não há programa contínuo de treinamento em segurança.

Incidentes Correlacionados: Phishing bem-sucedido contra equipe administrativa (Fevereiro/2025) e vazamento de credenciais de residente (Abril/2025).

Risco Associado (Alto): Colaboradores se tornam o principal vetor de ataque. A falta de treinamento reduz a eficácia das políticas e dos controles técnicos existentes.

Norma/Lei Relacionada: ISO 27001 (Anexo A.7 – Segurança em Recursos Humanos, com foco em Conscientização e Treinamento).

Riscos Consolidados e Classificação

Área	**Risco Identificado**	**Classificação**
Autenticação	Senhas fracas, ausência de MFA	Alto
Gestão de Acesso	Falta de classificação da informação e de permissões granulares	Alto
Backup	Falta de testes de restauração, retenção insuficiente, sem RTO/RPO	Crítico
Privacidade	Política desatualizada e falhas no atendimento aos direitos dos titulares	Crítico
Incidentes	Phishing, credenciais expostas e indisponibilidade de sistemas	Crítico

Conscientização	Falta de treinamentos periódicos e cultura de segurança	Alto

Recomendações de Melhoria

Com base nas não conformidades identificadas, são propostas as seguintes ações corretivas e de melhoria, organizadas por prioridade e área de atuação.

Prioridade Alta (0–30 dias)

5. Autenticação Multifator (MFA): Implementar MFA em todos os acessos administrativos, clínicos e remotos (incluindo prontuários eletrônicos).

    - Justificativa: A ausência de MFA foi explorada no incidente de Abril/2025. Mesmo que credenciais sejam vazadas, o segundo fator bloqueia o uso indevido.
    - Norma/Referência: LGPD (Art. 46) e ISO 27001 (A.9 – Controle de Acesso).

6. Revisão de Política de Senhas: Aumentar a complexidade mínima (mínimo 12 caracteres, preferencialmente passphrases), remover trocas periódicas sem justificativa e recomendar uso de gestores de senha.

    - Justificativa: Senhas curtas e fracas são facilmente quebradas por força bruta. Normas modernas (NIST/ISO) priorizam MFA e complexidade adequada.

7. Testes de Backup (Restore Drill): Realizar testes completos de restauração em até 30 dias, documentando RTO (tempo máximo de recuperação) e RPO (tempo máximo de perda de dados). Ampliar retenção por pelo menos 1 ano.

    - Justificativa: A queda de 3h em Junho/2025 já demonstrou risco crítico de indisponibilidade
    - Norma/Referência: ISO 27001 (A.17 – Continuidade do Negócio).

8. Resposta a Incidente de Credenciais Vazadas: Rotacionar e isolar credenciais comprometidas, conduzindo análise mínima do vetor de vazamento.
    - Justificativa: Reduz risco de exploração contínua e fornece insumos para reforço de controles.
9. Atualização da Política de Privacidade: Nomear encarregado (DPO), atualizar a política (última revisão em 2022), definir bases legais, finalidades e meios formais de exercício de direitos dos titulares.
    - Justificativa: Alinhamento à LGPD e ISO 27701, evitando multas e fortalecendo a confiança de pacientes.

Prioridade Média (30–90 dias)
Ações estruturantes para reduzir riscos de médio prazo e amadurecer a governança.

1. Controle de Acesso Baseado em Função (RBAC): Implantar RBAC e revisar permissões segundo o princípio do menor privilégio.

    - Justificativa: Corrige a lacuna atual de “nenhum controle de permissão”, evitando acesso irrestrito a dados.

2. Classificação da Informação: Definir níveis (pública, restrita, confidencial, sensível) e aplicar controles técnicos diferenciados para cada classe.

    - Justificativa: Sem classificação, dados sensíveis podem receber proteção insuficiente.

3. Monitoramento e Resposta a Incidentes (SIEM): Implantar ferramenta e processos de monitoramento contínuo de logs, com alertas e playbooks de resposta.

    - Justificativa: Previne falhas não detectadas e acelera a contenção de incidentes.

4. Treinamento de Conscientização em Segurança: Implementar programa contínuo de capacitação, com simulações de phishing e foco em higiene de credenciais.

    - Justificativa: Incidentes de fevereiro e abril/2025 confirmam a vulnerabilidade humana como vetor de ataque.
    - Norma/Referência: ISO 27001 (A.7 – Conscientização e Treinamento).

Prioridade Baixa / Contínua (90 dias+)
Ações de maturidade e evolução contínua da segurança.

5. Adequação a ISO 27701 (PIMS): Iniciar processo de implementação/certificação para fortalecer a governança em privacidade e demonstrar conformidade à LGPD.
6. Planejamento Contínuo de Capacidade e Recuperação: Realizar exercícios regulares de recuperação (BCP), com redundância em nuvem ou datacenter secundário.

    - Justificativa: Em caso de desastre físico (incêndio, enchente), garante continuidade do atendimento.

7. Auditoria Periódica de Logs e SLA de Disponibilidade: Estabelecer auditorias trimestrais de logs e definir SLA de disponibilidade mínima para sistemas críticos.

    - Justificativa: A queda de 3h demonstrou impacto direto no atendimento. Um SLA formal assegura priorização de recursos.