

# Relatório de Auditoria Interna de Segurança - HealU

## 1. Introdução

**Contexto:**

A HealU é uma startup brasileira especializada em aplicativos de saúde e wearables (como smartwatches) para monitoramento de pacientes crônicos. Com operações online no Brasil, América Latina e Europa, a empresa lida com dados sensíveis (históricos médicos, dados de sensores) e processamento de pagamentos internacionais (PIX, cartões, PayPal).

**Motivação da Auditoria:**

- Notificação da ANPD sobre possível violação da **LGPD** devido a vazamentos de dados.
  - Tentativas de **ransomware** no servidor de backup.
  - Necessidade de conformidade com **GDPR** (mercado europeu).
- 

## 2. Escopo e Objetivos

**Escopo:**

- Ativos críticos (bancos de dados, APIs, pagamentos, backups).
- Conformidade com **LGPD** e **GDPR**.
- Controles de segurança (NIST CSF).

**Objetivos:**

1. Identificar vulnerabilidades nos sistemas (apps, cloud, APIs).
  2. Avaliar conformidade com leis de proteção de dados.
  3. Priorizar ações para reduzir riscos (ex: ransomware, vazamentos).
  4. **Meta:** Reduzir pontuação de risco de **8** para **≤5** em 6 meses.
- 

## 3. Ativos Críticos e Priorização

| Ativo                        | Tipo           | Criticidade | Responsável |
|------------------------------|----------------|-------------|-------------|
| Banco de dados (SQL/MongoDB) | Dados de saúde | Alta        | TI/DPO      |

|                       |                |            |            |
|-----------------------|----------------|------------|------------|
| APIs de hospitais     | Integração     | Média-Alta | DevSecOps  |
| Serviço de pagamentos | Terceirizado   | Alta       | Financeiro |
| Backup AWS S3         | Infraestrutura | Crítica    | TI         |

#### 4. Avaliação de Riscos

##### Risco 1: Não Conformidade com LGPD/GDPR

- **Impacto:** Multas de até 2% do faturamento (LGPD) ou €20 milhões (GDPR).
- **Causa:** Falta de criptografia, treinamento e plano de resposta a incidentes.




##### Risco 2: Ransomware em Backups

- **Impacto:** Perda de dados por 72h+ e paralisação operacional.
- **Causa:** Backup não isolado e sem monitoramento proativo.

Pontuação de Risco: 8/10 (Alta)




#### 5. Checklist de Controles de Segurança

| Controle              | Status             | Justificativa                                    | Ação Recomendada                                             |
|-----------------------|--------------------|--------------------------------------------------|--------------------------------------------------------------|
| Least Privilege       | ✗ Não implementado | 80% dos funcionários têm acesso total aos dados. | Implementar <b>RBAC</b> em 30 dias.                          |
| Criptografia de Dados | ✗ Não implementado | Dados de saúde trafegam em texto plano.          | Adotar <b>AES-256</b> para bancos de dados e APIs (15 dias). |

|                            |                                                                                                    |                                                   |                                                                         |
|----------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------------------------------------------------------------|
| <b>Plano de Backup</b>     |  Parcial          | Backups existem, mas não há teste de recuperação. | Testar restauração mensal e isolar backups (1 mês).                     |
| <b>IDS/IPS</b>             |  Não implementado | Ataques de ransomware detectados manualmente.     | Implementar <b>Splunk</b> ou <b>Wazuh</b> para monitoramento (2 meses). |
| <b>Treinamento de LGPD</b> |  Não realizado    | Funcionários desconhecem procedimentos.           | Capacitação trimestral com certificação (iniciar em 14 dias).           |

## 6. Conformidade com LGPD e GDPR

### LGPD

| Requisito                       | Status                                                                                    | Ação Urgente                                                     |
|---------------------------------|-------------------------------------------------------------------------------------------|------------------------------------------------------------------|
| Notificação de vazamentos (72h) |  Falta | Criar plano de resposta com fluxo para ANPD/titulares (30 dias). |
| Nomeação de DPO                 |  Falta | Designar encarregado em 15 dias (Art. 41).                       |
| Anonimização de dados           |  Falta | Implementar <b>tokenização</b> para dados sensíveis (3 meses).   |

### GDPR

| Requisito | Status | Ação Urgente |
|-----------|--------|--------------|
|-----------|--------|--------------|

Representante na UE ✗ Falta Contratar representante legal (Art. 27).

Inventário de dados ✗ Falta Mapear fluxos de dados europeus (1 mês).

---

## 7. Recomendações Prioritárias

1. **Crítico (0-30 dias):**
    - Isolar servidor de backup e auditar logs.
    - Criptografar bancos de dados (SQL/MongoDB).
  2. **Alto (1-3 meses):**
    - Treinamento em LGPD/GDPR para toda a equipe.
    - Implementar IDS/IPS para detecção de ameaças.
  3. **Médio (3-6 meses):**
    - Testes de recuperação de desastres (DRP).
    - Revisão de contratos com terceiros (cláusulas de segurança).
- 

## 8. Conclusão

A HealU enfrenta riscos significativos em segurança e conformidade, mas com um plano estruturado (prazos, responsáveis e métricas), é possível mitigá-los. **Próximos passos:**

- Apresentar este relatório à diretoria para alocação de recursos.
- Criar um **comitê de segurança** com TI, jurídico e DPO.