SMALI

Sistema de Monitoramento de Ambientes Laborais e Industriais

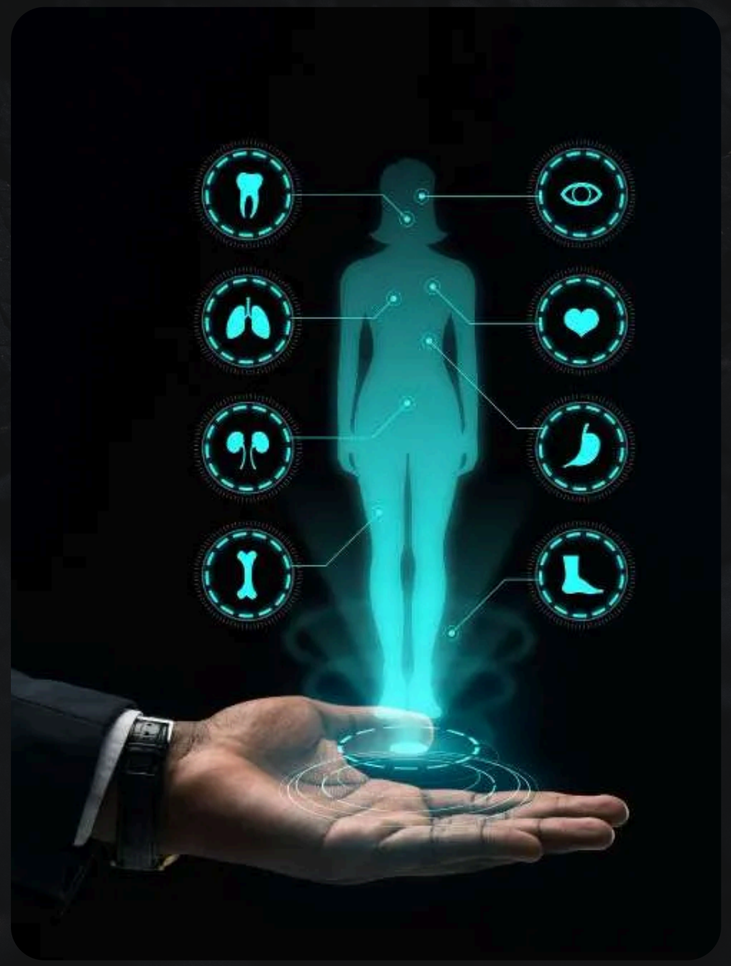
1. APRESENTAÇÃO DO PROJETO

1.1 Identificação

Nome da Empresa: CEPIL TECHNOLOGIES
Lema: Cura et protectio in labore
Nome da Solução/Produto: SMALI – Sistema de Monitoramento de Ambientes Laborais e Industriais
Data da Documentação: Novembro de 2025

1.2 COMPOSIÇÃO DA EQUIPE

- Ruan Nunes Gaspar RM 559567 Turma 2TDSPA
- Rodrigo Paes Morales RM 560209 Turma 2TDSPA
- Fernando Nachtigall Tessmann RM 559617 Turma 2TDSPR



1.3 Problema/Desafio Identificado

Desafio: A falta de sistemas integrados de monitoramento em tempo real dos níveis de insalubridade em ambientes laborais e industriais brasileiros representa um risco crítico à saúde dos trabalhadores e gera não conformidade com legislação de segurança do trabalho.

Problemas Específicos:

Ausência de Monitoramento Contínuo
A maioria das indústrias brasileiras realiza avaliações pontuais de agentes nocivos, sem monitoramento contínuo.

Conformidade Regulatória
Desafio em manter conformidade com NR-9 (PPRA), NR-15 (Atividades e Operações Insalubres) e normas de higiene ocupacional.

Reatividade vs. Proatividade
Acidentes ocorrem porque não há alertas antecipados quando níveis perigosos são atingidos.

Custo de Implementação
Soluções proprietárias existentes são caras e inacessíveis para PMEs do setor industrial.

Falta de Integração
Dados de diferentes sensores não são integrados em uma plataforma unificada.

Decisões Baseadas em Dados
Ausência de dashboards e visualizações que permitam análise de tendências e histórico.

Trabalhando no presente, impactando o futuro

Solução Proposta

SMALI oferece uma plataforma IoT integrada que monitora continuamente gases prejudiciais (CO, CO_2, CH_4, H_2S), temperatura e umidade em ambientes industriais, fornecendo alertas em tempo real via aplicativo mobile e dashboard web, com conformidade comprovada às normas brasileiras de segurança do trabalho.

2.1 Segmentação do Público-Alvo

Público-Alvo Primário

Indústrias de Transformação

Fabricação de química, siderurgia, refinaria, petroquímica

~3.500 empresas

Indústrias Extrativistas

Mineração, garimpo, extração de minérios

~2.100 empresas

Indústrias de Utilidades

Tratamento de água, saneamento, energia

~1.800 empresas

Empresas de Logística e Armazenagem

Portos, aeroportos, centros de distribuição

~5.200 empresas

Empresas de Logística e Armazenagem

Órgãos de defesa civil, corpo de bombeiros

~2.500 instituições

Público-Alvo Secundário

Empresas de Logística e Armazenagem

- Consultores de segurança ocupacional
- Escritórios de engenharia de segurança
- Órgãos reguladores (CEREST, vigilância sanitária)

2.2 Dados de Mercado e Estatísticas

Mercado Brasileiro de Segurança Ocupacional

Tamanho do Mercado

- Mercado global de IoT para segurança ocupacional: US$ 12,4 bilhões em 2023
- Projeção para 2030: US$ 48,7 bilhões (CAGR de 18,5%)
- Mercado brasileiro de segurança do trabalho: R$ 4,8 bilhões em 2023

Incidência de Acidentes

- Brasil registra 550 mil acidentes de trabalho por ano
- Taxa de incidência: 10,84 por 1.000 trabalhadores
- Custos anuais com acidentes: R$ 87 bilhões (estimado)

Conformidade Regulatória

- 72% das indústrias brasileiras não possuem sistema de monitoramento contínuo
- Multas por não conformidade: R$ 50 mil a R$ 500 mil por violação de NR-9
- Responsabilidade civil: indenizações médias de R$ 2 a R$ 15 milhões por morte ocupacional

Penetração de Tecnologia

- 58% das indústrias brasileiras pretendem investir em IoT nos próximos 3 anos
- Preço médio de soluções equivalentes: R$ 50 mil a R$ 200 mil por instalação
- Demanda por soluções cloud: crescimento de 42% ao ano no Brasil

2.2 Dados de Mercado e Estatísticas

Pressupostos

- Indústria média com 150 trabalhadores
- 5 setores de produção a monitorar
- Custo evitado por acidente de trabalho: R$ 180 mil (média histórica)
- Prevenção de 1-2 acidentes/ano com SMALI: 70% de probabilidade

Investimento Inicial (instalação + licença 1º ano)	**R$ 85.000**
Economia com Prevenção (1º ano)	**R$ 126.000**
ROI (1º ano)	**148%**
Payback	**8 meses**
Economia acumulada (5 anos)	**R$ 890.000**

Análise de ROI para Cliente Tipo (Indústria Média)

2.4 Impacto Estimado para o Público-Alvo

Benefícios Quantificáveis

1. Redução de Acidentes:
Meta: Redução de 40-50% em acidentes por exposição a agentes nocivos
Impacto: 220-275 vidas protegidas por ano (considerando mercado-alvo)
2. Conformidade Regulatória:
Redução de multas: -R$ 18 milhões/ano (setor alvo)
Manutenção de certificações: ISO 45001 otimizada
3. Produtividade:
Redução de ausências por doença ocupacional: 20-30%
Aumento de produtividade: 5-8% estimado
Economia com licenças INSS: R$ 120-180 mil/empresa/ano
4. Responsabilidade Social:
Demonstração de compromisso com segurança do trabalho
Melhoria da imagem corporativa (44% dos clientes B2B priorizam segurança)[12]
5. Competitividade:
Acesso a novos contratos que exigem rastreabilidade de segurança
Diferencial competitivo em processos de licitação pública

2.5 Estratégia de Penetração de Mercado

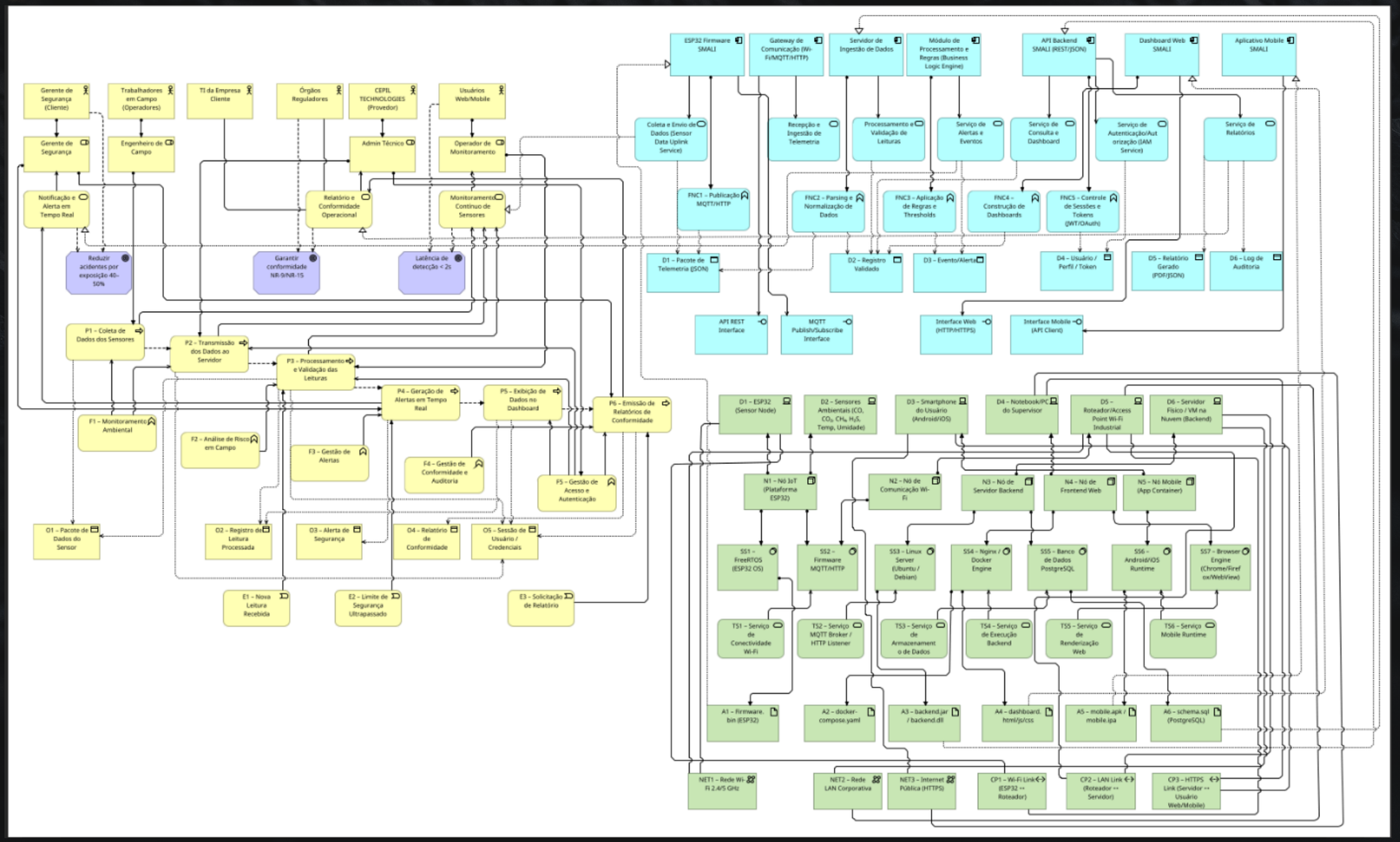
Fase 1 (Meses 1-6): Pilotos em 3-5 empresas-âncora com case studies

Fase 3 (Ano 2): Expansão para setor público e consultoria

Fase 2 (Meses 7-12): Parcerias com integradores de segurança

Fase 4 (Anos 2-3): Internacionalização (MERCOSUL)

3. ARQUITETURA DA SOLUÇÃO (MODELO TOGAF)



3. ARQUITETURA DA SOLUÇÃO (MODELO TOGAF)

3.1 Visão de Arquitetura

3.1.1 Stakeholders

Stakeholder	Interesse Crítico	Preocupações
Gerente de Segurança (Cliente)	Confmidade com NRs, redução de acidentes	Facilidade de uso, integração com sistemas
Trabalhadores em Campo	Segurança, notificações rápidas	Confiabilidade dos alertas
TI da Empresa Cliente	Integração, escalabilidade, suporte	Manutenção, custo de operação
Órgãos Reguladores	Conformidade, auditoria	Rastreabilidade de dados, validação
CEPIL TECHNOLOGIES	Viabilidade comercial, market share	Custo de suporte, diferenciação
Usuários via Web	Acesso a dashboards, relatórios	Performance, segurança de dados
Usuários via Mobile	Alertas em tempo real, mobilidade	Performance, segurança de dados

3.1.2 Objetivos Estratégicos

1. Objetivo O1: Reduzir em 40-50% os acidentes por exposição a agentes nocivos em ambientes industriais monitorados
2. Objetivo O2: Garantir 99,9% de conformidade com legislação brasileira de segurança do trabalho (NR-9, NR-15)
3. Objetivo O3: Fornecer detecção de anomalias com latência < 2 segundos
4. Objetivo O4: Oferecer solução com ROI em 8-12 meses
5. Objetivo O5: Escalar para 500+ instalações em 24 meses

3.1.3 Requisitos Arquiteturais

Requisitos Funcionais

- RF1: Sistema deve capturar dados de 6 tipos de sensores (CO, CO_2, CH_4, H_2S, Temperatura, Umidade)
- RF2: Transmissão de dados com latência < 5 segundos do sensor até o usuário
- RF3: Geração de alertas automáticos quando valores excedem limites seguros
- RF4: Persistência de histórico de dados por mínimo de 2 anos
- RF5: Acesso via aplicativo mobile (iOS/Android) e web responsiva
- RF6: Suporte para múltiplas empresas (SaaS) com isolamento de dados
- RF7: Integração com sistema de emissão de notas fiscais (ASAAS)

Requisitos Não-Funcionais

- RNF1: Disponibilidade: 99,9% uptime anual
- RNF2: Performance: API responde < 500ms em 95º percentil
- RNF3: Segurança: Criptografia TLS 1.3 em trânsito, AES-256 em repouso
- RNF4: Escalabilidade: Suportar 50.000+ eventos/segundo
- RNF5: Conformidade: LGPD, compliance com NRs brasileiras
- RNF6: Auditoria: Rastreamento completo de ações (audit trail)
- RNF7: Recovery: RTO < 4 horas, RPO < 1 hora

3.2 Arquitetura de Negócio

3.2.1 Processos de Negócio

Processo P1: Onboarding de Cliente

Cliente Solicita → CEPIL Avalia → Instalação Sensores → Configuração API → Ativação Conta → Treinamento → Go-Live
Atores: Gerente de Vendas, Engenheiro de Campo, Suporte

Processo P2: Monitoramento Contínuo

Sensor Lê Dados → ESP32 Processa → MQTT Pub → Adafruit → Node-RED Converte → APIs Registram → DB Persiste → Dashboard Visualiza → Usuário Notificado
Atores: Sistema Automatizado, Usuário Notificado

Processo P3: Tratamento de Anomalias

Leitura Acima do Limiar → Alerta Gerado → Push Mobile + Email + SMS → Usuário Aciona → Registro de Incidente → Análise Pós-Evento → Relatório Gerado
Atores: Sistema, Gerente de Segurança, Analista

Processo P4: Conformidade e Auditoria

Coleta Dados Período → Consolidação → Relatório NR → Validação Regulatória → Arquivo Audit Trail → Disponibilização para Órgãos
Atores: Analista CEPIL, Sistema, Órgão Regulador

3.2.2 Funções Organizacionais

Função	Responsabilidade
Vendas e Consultoria	Prospecção, diagnóstico de necessidades, propostas
Engenharia de Campo	Instalação de sensores, configuração, testes
Suporte Técnico	Troubleshooting, manutenção preventiva
Operações	Monitoramento de plataforma, escalabilidade
Produto	Evolução de features, roadmap
Conformidade	Garantia de legislação, auditorias

3.2.3 Atores e Papéis

Ator	Papel	Responsabilidades
Gerente de Segurança	Usuário Executor	Configura limites, analisa alertas, genera relatórios
Operador em Campo	Usuário Consultor	Visualiza status em tempo real, recebe notificações
Engenheiro CEPIL	Provedor de Serviço	Instala, configura, mantém sensores
Admin Técnico	Gestor de Plataforma	Gerencia contas, permissões, integrações
Sistema Automatizado	Processador	Coleta dados, gera alertas, persiste em DB

3.3 Arquitetura de Sistemas (Camadas de Serviços)

3.3.1 Componentes de Aplicação

Camada de Apresentação

Componente	Tecnologia	Função	Hosting
App Mobile SMALI	React Native	Interface móvel multiplataforma	Google Play + App Store
Dashboard Web ASP.NET	ASP.NET Core MVC	Portal web gerencial	Azure VM
Interface Responsiva	HTML5/CSS3/React	Acesso web responsivo	Azure VM

Camada de Serviços (APIs)

Componente	Tecnologia	Função	Hosting
API Dados Sensores	Spring Boot + REST	Crud usuario/setor/sensor	Oracle Cloud VM
API Dashboard Web	ASP.NET Core MVC	Consultas para web dashboard	Azure VM
Serviço Node-RED	Node-RED	Conversão MQTT → HTTP	Oracle Cloud + Azure
Serviço Integração Fiscal	REST Client	Integração ASAAS	Oracle Cloud

Camada de Integração IoT

Componente	Tecnologia	Função	Hosting
Firmware Sensor	C++ em ESP32	Leitura e transmissão de dados	Embarcado no ESP32
Broker MQTT	Adafruit MQTT	Pub/Sub de mensagens	Nuvem Adafruit
Message Queue	MQTT Topics	Fila de eventos de sensores	Adafruit

3.3.2 Componentes de Dados

Banco de Dados Primário (API Java)

Entidade	Função	Tecnologia
Usuário (Empresa)	Conta master com acesso administrativo	Oracle DB
Setor	Agrupamento de sensores por localização	Oracle DB
Sensor	Registro de dispositivo e suas leituras	Oracle DB
Leitura	Histórico de valores (CO, CO2, etc)	Oracle DB (Particionado)
Alerta	Eventos de violação de limites	Oracle DB
Auditoria	Log de todas as ações do sistema	Oracle DB

3.3.3 Serviços e Padrões de Comunicação

Camada 1 - IoT/Sensores

- Sensores IoT (ESP32) enviam dados via MQTT ao Broker Adafruit
- Protocolo: MQTT v3.1.1 com QoS 1
- Frequência: 1 leitura a cada 30 segundos por sensor

Camada 2 - Integração/Middleware

- Node-RED recebe mensagens MQTT e converte para HTTP/JSON
- Distribui para ambas as APIs (Java e .NET)
- Implementa retry logic e tratamento de falhas

Camada 3 - APIs de Negócio

- API Java Spring Boot: CRUD completo, orquestração de lógica
- API .NET Core MVC: Views web + API REST para dashboard
- Comunicação entre APIs: assíncrona via eventos

Camada 4 - Dados

- Replicação Oracle ↔ SQLite conforme necessário
- Sincronização de estado via serviço de integração

Camada 5 - Apresentação

- App Mobile conecta diretamente à API Java (REST)
- Web Dashboard conecta à API .NET (MVC)

3.4 Arquitetura de Tecnologia

3.4.1 Topologia de Rede

Rede de Campo (On-Premises Cliente)

```
[Sensores ESP32]
↓ WiFi/4G
[Roteador Industrial] → [Firewall]
```

Rede de Campo (On-Premises Cliente)

```
[Internet]
↓
[Adafruit Cloud - MQTT Broker]
↓
[Oracle Cloud Network]
 ├─── [VM Oracle Cloud - API Java + Node-RED]
 └─── [Azure Network]
 ├─── [VM Azure - API .NET + Node-RED]
 └─── [SQLite Local]
[Mobile Devices] → REST API Java (Oracle Cloud)
[Web Browsers] → MVC ASP.NET (Azure)
```

3.4.2 Equipamentos e Servidores

1. Equipamento de Sensoriamento (Cliente)

Equipamento	Especificação	Quantidade	Software
Placa Base	ESP32 Dev Board	1 por pátio	Firmware C++
Sensor CO	Alphasense OX-A431	1+	Driver integrado
Sensor CO2	SenseAir K30	1+	Driver integrado
Sensor CH4	Alphasense LEL-A231	1+	Driver integrado
Sensor H2S	Alphasense H2S-A4	1+	Driver integrado
Sensor Temp/Umidade	DHT22	1+	Driver integrado
Roteador Industrial	Cisco IR1800	1	IOS XE
Gabinete Proteção	IP65 Alumínio	1 por cluster	N/A
Fonte Redundante	24VDC/5A	2 (redundância)	N/A

Software no ESP32

- Sistema Operacional: FreeRTOS
- Linguagem: C++ (Arduino-compatible)
- Bibliotecas: PubSubClient (MQTT), Sensor drivers individuais
- Firmware updates: Over-the-air (OTA) via WiFi

2. Servidor Cloud - Oracle Cloud (API Java + Node-RED)

Componente	Especificação/Software
VM Instance	Ubuntu 22.04 LTS, 4 vCPU, 16 GB RAM
Java Runtime	OpenJDK 17 LTS
Framework API	Spring Boot 3.x
Build Tool	Maven 3.8+
Web Server	Tomcat 10.x (embedded)
Node-RED	Node.js 18.x + Node-RED 3.x
MQTT Client	Mosquitto Client Library
Database Driver	Oracle JDBC Driver

3. Servidor Web – Azure VM (API .NET + Dashboard Web)

Componente	Especificação/Software
VM Instance	Windows Server 2022, 4 vCPU, 16 GB RAM
Runtime	.NET 8.0 (ou .NET Core 7)
Framework Web	ASP.NET Core MVC
IDE/Dev Tools	Visual Studio Build Tools 2022
IIS	Internet Information Services 10.0
Database	SQLite 3.x (local)
ORM	Entity Framework Core 8.x
Web UI	HTML5, CSS3, Bootstrap 5, JavaScript

4. Database Servers:

Oracle Cloud (Primário)

Componente	Especificação
Database	Oracle Database 21c ou 23c
Armazenamento	500 GB (leituras de sensores)
Backup	RMAN com retenção 2 anos
Replicação	Data Guard (opcional, para DR)
Monitoring	Enterprise Manager Cloud Control

Azure (Local/Cliente):

Componente	Especificação
Database	SQLite 3.x
Armazenamento	50 GB (cache local)
Backup	Sincronização automática a cada 6h
Acesso	Local machine access

3.4.3 Conectividade e Protocolos

1. Sensores → Adafruit (Campo)

- Protocolo: MQTT 3.1.1
- Porta: 8883 (MQTT over TLS)
- Autenticação: Username/Password + TLS Certificate
- Intervalo: 30 segundos por sensor
- QoS: Level 1 (Atleast Once)

2. Adafruit → Node-RED (Cloud)

- Protocolo: MQTT
- Porta: 8883 (TLS)
- Autenticação: API Key + TLS
- Latência esperada: < 2 segundos

3. Node-RED → APIs

- Protocolo: HTTP/REST (POST)
- Porta: 443 (HTTPS TLS 1.3)
- Content-Type: application/json
- Autenticação: Bearer Token (OAuth2)

4. APIs ↔ Banco de Dados

- Protocolo: DB native (JDBC para Oracle, SQLite native)
- Porta: 1521 (Oracle)
- Autenticação: Usuario/Senha com conexão criptografada

5. Mobile App → API Java

- Protocolo: HTTP/REST
- Porta: 443 (HTTPS)
- Autenticação: JWT Token
- Endpoints: /api/v1/sensors, /api/v1/users, /api/v1/alerts

6. Web Browser → API .NET

- Protocolo: HTTP/HTTPS
- Porta: 443 (HTTPS)
- Sessão: ASP.NET Session (cookies seguros)
- Endpoints: MVC Controllers + REST API

3.4.4 Especificações de Segurança

Segurança em Trânsito

- TLS 1.3 para todas as comunicações externas
- Certificados SSL/TLS de CA confiável (Let's Encrypt ou Azure Certificates)
- Pinning de certificado no App Mobile

Segurança em Repouso

- Criptografia AES-256 para dados sensíveis em BD
- Hashing SHA-256 com salt para senhas
- Tokens JWT com expiração de 24 horas

Autenticação

- OAuth2 para APIs
- MFA (Multi-Factor Authentication) para admin

Autorização

- Role-Based Access Control (RBAC): Admin, Gestor, Operador, Visualizador
- Isolamento de dados por tenant (multi-tenancy segura)

4. FLUXO DE DADOS DETALHADO

Fluxo 1: Coleta de Dados (Sensor → Visualização)

- 1. ESP32 lê sensores a cada 30s
- 2. Publica em topic MQTT: "sensores/{empresa}/{setor}/{sensorId}"
- 3. Broker Adafruit recebe e armazena
- 4. Node-RED subscreve ao topic
- 5. Converte MQTT → HTTP/JSON
- 6. POST para API Java: /api/v1/sensor-reading
- 7. API Java valida e persiste em Oracle
- 8. API Java envia para API .NET (async)
- 9. API .NET armazena em SQLite (cache)
- 10. App Mobile e Dashboard Web atualizam em tempo real
- 11. Se valor > limite: gera alerta (email + push mobile + SMS)

Fluxo 2: Tratamento de Alerta

- 1. Leitura de CO = 1000 ppm (limiar = 800 ppm)
- 2. API Java detecta anomalia
- 3. Cria registro em tabela "ALERTAS"
- 4. Dispara evento para sistema de notificação
- 5. Serviço envia:
- - Push notification para App Mobile
- - Email para gerente de segurança
- - SMS para coordenador de campo
- 6. Alerta fica visível no Dashboard (badge)
- 7. Usuário pode marcar como "Visualizado" ou "Resolvido"
- 8. Auditoria registra timestamp de ação

5. CONFORMIDADE E NORMAS

- NR-9 (PPRA): Programa de Prevenção de Riscos Ambientais
- NR-15 (Atividades Insalubres): Limites de tolerância para agentes químicos
- LGPD (Lei Geral de Proteção de Dados): Conformidade de privacidade
- NBR ISO/IEC 27001: Gestão de segurança da informação
- ISO 45001: Gestão de saúde e segurança ocupacional

REFERÊNCIAS

[1] Grand View Research. IoT in Safety and Security Market Report 2024.
[2] Associação Brasileira de Segurança do Trabalho (ABST). Market Report 2023.
[3] INSS - Instituto Nacional do Seguro Social. Anuário Estatístico 2023.
[4] CNI - Confederação Nacional da Indústria. Custos de Acidentes no Brasil.
[5] Sebrae. Adoção de IoT em PMEs Brasileiras 2023.
[6] MTE - Ministério do Trabalho e Emprego. Tabela de Penalidades 2024.
[7] ABJD - Associação Brasileira de Juristas pela Democracia. Jurisprudência em Responsabilidade Civil.
[8] IDC Brasil. Digital Transformation Report 2024.
[9] Gartner. Market Price for Industrial IoT Solutions 2023.
[10] Statista. Cloud Market Growth Brazil 2024.
[11] NIOSH - National Institute for Occupational Safety and Health. IoT Safety Efficacy Study 2023.
[12] McKinsey. State of Business Supply Chains 2024.

Our Team

Ruan Nunes Gaspar

RM 559567
Turma 2TDSPA

Rodrigo Paes Morales

RM 560209
Turma 2TDSPA

Fernando Nachtigall Tessmann

RM 559617
Turma 2TDSPR