Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"

Curso Superior de Tecnologia em Segurança da Informação

Caique Martins Braz

IA E IOT APLICADO EM MANUTENÇÃO PREDITIVA E SEGURANÇA DE DADOS NA INDÚSTRIA 4.0

Americana, SP

2025

Caique Martins Braz

IA E IOT APLICADO EM MANUTENÇÃO PREDITIVA E SEGURANÇA DE DADOS NA INDÚSTRIA 4.0

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação na área de concentração em Segurança da Informação.

Orientador: Prof. Me. CLERIVALDO JOSE ROCCIA

Este trabalho corresponde à versão final do Trabalho de Conclusão de Curso apresentado por Caique Martins Braz e orientado pelo Prof. Me. CLERIVALDO JOSE ROCCIA

Americana, SP

2025

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana Ministro Ralph Biasi- CEETEPS Dados Internacionais de Catalogação-na-fonte

BRAZ, Caique Martins

Ia e iot aplicado em manutenção preditiva e segurança de dados na indústria 4.0. / Caique Martins Braz – Americana, 2025.

78f.

Monografia (Curso Superior de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana Ministro Ralph Biasi – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Prof. Ms. Clerivaldo Jose Roccia

1. Analise de Dados 2. Inteligência artificial 3. Internet das coisas. I. BRAZ, Caique Martins II. ROCCIA, Clerivaldo Jose III. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana Ministro Ralph Biasi

CDU: 681519
007.52
681518

Elaborada pelo autor por meio de sistema automático gerador de ficha catalográfica da Fatec de Americana Ministro Ralph Biasi.

Caique Martins Braz

IA e IoT aplicado em manutenção preditiva e segurança de dados na indústria 4.0

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Curso Superior de Tecnologia em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana Ministro Ralph Biasi.
Área de concentração: Segurança da Informação

Americana, 27 de junho de 2025.

Banca Examinadora:

Clerivaldo José Roccia
Mestre
Fatec Americana "Ministro Ralph Biasi"

Renato Cividini Matthiesen
Mestre
Fatec Americana "Ministro Ralph Biasi"

Ana Karina Giusti Mantovani
Especialista
Fatec Americana "Ministro Ralph Biasi"

AGRADECIMENTOS

Registro minha profunda gratidão à minha família, especialmente aos meus pais Marcos e Elaine, incentivo e apoio incondicional durante todas as etapas da minha formação. Sem o suporte de vocês, este momento não teria sido possível.

Agradeço ao meu orientador, Professor Clerivaldo, pela paciência, dedicação e pelas valiosas orientações que foram essenciais para o desenvolvimento e conclusão deste trabalho.

Expresso também meus sinceros agradecimentos à Professora Maria Cristina, pelas orientações e dicas fundamentais para a elaboração do trabalho escrito, que contribuíram significativamente para a qualidade desta pesquisa.

Agradeço aos professores e colegas da Fatec Americana, cujas contribuições acadêmicas e troca de conhecimentos enriqueceram significativamente minha trajetória.

Sou grato à instituição Fatec, pela infraestrutura e ambiente propício ao aprendizado e crescimento profissional.

Por fim, agradeço a todos que, de forma direta ou indireta, colaboraram para a realização deste trabalho, manifestando meu sincero reconhecimento.

RESUMO

Este trabalho apresenta o desenvolvimento e análise de um sistema para manutenção preditiva que integra Inteligência Artificial (IA) e Internet das Coisas (IoT) em um cenário industrial. A proposta busca compreender de que forma essas tecnologias podem contribuir para o monitoramento de ativos, identificação antecipada de falhas e automação de processos de manutenção. A metodologia adotada contempla a revisão conceitual das tecnologias envolvidas e a construção de um protótipo funcional utilizando a plataforma ERPNext. Os dados coletados por sensores são processados por um sistema especialista, que avalia o funcionamento dos equipamentos e sugere ações corretivas quando necessário. Foram simulados três cenários distintos para validar o desempenho da solução, evidenciando sua eficácia na detecção de anomalias operacionais e na geração automatizada de ordens de serviço. Os resultados reforçam o potencial do sistema como ferramenta de apoio à gestão da manutenção e ao planejamento estratégico. O estudo também ressalta a importância da padronização de dados e da adoção de práticas de segurança da informação. A conclusão aponta que a combinação entre IA e IoT oferece resultados promissores para a modernização da indústria, otimizando recursos e prevenindo falhas. Pesquisas futuras podem aprimorar o modelo com algoritmos de aprendizado contínuo, ampliando sua precisão e capacidade de adaptação.

Palavras Chave: Inteligência Artificial; IoT; Manutenção Preditiva.

ABSTRACT

This research presents the development and evaluation of a predictive maintenance system that integrates Artificial Intelligence (AI) and the Internet of Things (IoT) within an industrial context. The goal is to investigate how these technologies can contribute to asset monitoring, early detection of failures, and automation of maintenance procedures. The approach includes a theoretical review of AI, IoT, and predictive maintenance, along with the creation of a prototype based on the ERPNext platform. Sensor readings are analyzed in real-time by an expert system that diagnoses equipment conditions and triggers necessary interventions. Three different simulation scenarios were applied to validate the solution's performance, confirming its ability to detect anomalies and generate automated service orders. The findings emphasize the importance of standardized data and information security to ensure operational reliability. Results indicate that combining AI and IoT can significantly enhance maintenance efficiency and support decision-making and strategic planning. With well-established rules and infrastructure, the prototype proved capable of minimizing risks and optimizing resource use. Future studies may explore the inclusion of continuous learning models to further increase system adaptability and predictive accuracy.

Keywords: *Artificial Intelligence; IoT; Predictive Maintenance.*

SUMÁRIO

1 INTRODUÇÃO

A revolução digital tem modificado profundamente a forma como as indústrias operam, com destaque para a Indústria 4.0 — um conceito que envolve a integração de tecnologias inteligentes, automação avançada e análise de grandes volumes de dados em tempo real. Dentro desse novo paradigma, estratégias como a manutenção preditiva vêm ganhando relevância, pois oferecem meios de identificar falhas potenciais antes que estas comprometam o funcionamento de máquinas e sistemas, minimizando paradas não planejadas e ampliando a eficiência dos processos.

Ao contrário da manutenção corretiva, que atua após falhas, ou da preventiva, que segue cronogramas predefinidos, a manutenção preditiva é guiada por dados coletados por sensores e dispositivos interligados. Esses dados são analisados para antecipar desgastes e anomalias, o que permite intervenções pontuais e mais eficazes. Essa abordagem tem o potencial de melhorar significativamente a produtividade ao mesmo tempo em que otimiza o uso de recursos — conforme apontado por Baldissarelli e Fabro (2019).

Com os avanços recentes em Inteligência Artificial (IA) e Internet das Coisas (IoT), tornou-se viável o desenvolvimento de soluções mais dinâmicas e precisas para esse tipo de manutenção. A IA contribui com algoritmos que aprendem continuamente com o comportamento das máquinas, enquanto a IoT promove a conectividade e o monitoramento em tempo real de diversos equipamentos. Essa integração viabiliza diagnósticos mais confiáveis e decisões operacionais mais assertivas.

O presente trabalho busca explorar como essas tecnologias podem ser aplicadas de forma conjunta e eficiente no contexto da manutenção preditiva. Além dos ganhos técnicos, o estudo considera também os desafios de segurança da informação em ambientes conectados, reconhecendo a importância de proteger os dados sensíveis envolvidos nesse processo.

Com base na implementação prática de um protótipo e na análise de diferentes cenários simulados, a pesquisa visa fornecer subsídios para empresas que pretendem adotar modelos de manutenção mais inteligentes e adaptáveis às exigências da Indústria 4.0. O objetivo é apresentar caminhos para reduzir riscos, ampliar a confiabilidade operacional e construir estratégias mais sustentáveis no ambiente industrial atual.

Problema da pesquisa: A digitalização crescente dos processos industriais tem impulsionado a necessidade por estratégias de manutenção mais inteligentes e eficientes. Embora a manutenção preditiva já seja reconhecida como uma abordagem promissora para reduzir falhas e otimizar o uso de recursos, sua implementação prática ainda enfrenta obstáculos consideráveis. Entre os principais desafios estão a integração eficaz de dados provenientes de dispositivos conectados, a confiabilidade das análises geradas e a adaptação dos sistemas às realidades específicas de cada ambiente produtivo. Além disso, muitas organizações encontram dificuldades para aplicar essas tecnologias devido a limitações em infraestrutura tecnológica, custos e capacitação técnica. Nesse cenário, torna-se essencial investigar o papel das tecnologias emergentes, como Inteligência Artificial (IA) e Internet das Coisas (IoT), na superação desses entraves e na construção de soluções mais eficazes.

Objetivo Geral: Este trabalho tem como finalidade principal analisar de que maneira a combinação entre Inteligência Artificial (IA) e Internet das Coisas (IoT) pode contribuir para o aprimoramento de sistemas de manutenção preditiva no setor industrial. A intenção é avaliar a aplicação integrada dessas tecnologias com foco na antecipação de falhas, na otimização do monitoramento dos ativos e na proteção dos dados envolvidos nos processos operacionais.

Objetivo específico: Para atingir o objetivo geral, este estudo buscará compreender os fundamentos teóricos da Inteligência Artificial (IA) e da Internet das Coisas (IoT), com ênfase em suas funcionalidades voltadas à conectividade, à coleta e à análise de dados em ambientes industriais. Será realizada uma avaliação dos principais algoritmos de IA aplicáveis à manutenção preditiva, como redes neurais e técnicas de aprendizado de máquina, considerando seus benefícios, limitações e aspectos relacionados à segurança. A pesquisa também examinará a utilização prática de sensores e dispositivos conectados, bem como os protocolos de comunicação que asseguram a integridade e a eficiência na transmissão dos dados. Além disso, serão analisados estudos de caso em diferentes segmentos da indústria, com o intuito de identificar os resultados alcançados, os desafios enfrentados e as estratégias utilizadas na implementação dessas tecnologias. Por fim, serão elaboradas recomendações técnicas direcionadas a empresas interessadas em adotar ou aprimorar soluções de manutenção preditiva baseadas em IA e IoT, levando em conta a importância da proteção da informação, da resiliência dos sistemas e da qualidade na tomada de decisões.

2 REFERENCIAL TEÓRICO

Este capítulo reúne os fundamentos teóricos necessários para o desenvolvimento do trabalho. São apresentados conceitos essenciais sobre Indústria 4.0, Internet, Internet das Coisas (IoT), Inteligência Artificial (IA) e segurança da informação, além de explorar suas interrelações com a manutenção preditiva. O objetivo é fornecer o embasamento conceitual que sustentará a análise dos capítulos seguintes.

2.1 Indústria 4.0

O conceito de Indústria 4.0 representa uma nova etapa da transformação industrial, marcada pela integração de tecnologias emergentes aos processos produtivos. Essa fase, por vezes chamada de Quarta Revolução Industrial, caracteriza-se pela adoção de sistemas interconectados e inteligentes, nos quais dispositivos físicos e digitais interagem em tempo real. Tecnologias como IoT, a robótica colaborativa, a análise massiva de dados (Big Data) e a manufatura aditiva, como a impressão 3D, desempenham papel central nesse novo cenário (Cardoso, 2016).

O objetivo central da Indústria 4.0 é elevar a flexibilidade e a eficiência das operações industriais, permitindo que linhas de produção respondam rapidamente a demandas de mercado e operem com níveis elevados de autonomia e precisão. A ideia é construir ambientes produtivos conectados e adaptáveis, com menor desperdício de recursos e maior capacidade de personalização. De acordo com Lima e Gomes (2020), a interligação entre os diversos elos da cadeia produtiva, desde o projeto inicial até o suporte ao consumidor, permite ganhos expressivos em produtividade e competitividade.

Além de impulsionar a eficiência operacional, esse modelo também promove inovações em modelos de negócio, exige novas competências profissionais e contribui para a sustentabilidade, ao otimizar o uso de insumos naturais e acelerar o desenvolvimento de soluções tecnológicas. A Indústria 4.0, portanto, não apenas transforma o modo de produzir, mas também redefine o papel da tecnologia nas estratégias organizacionais contemporâneas.

2.2 Internet

A Internet tornou-se uma infraestrutura essencial para a vida moderna, permitindo a comunicação entre dispositivos e pessoas em escala global. Sua criação remonta aos anos 1960, em um contexto de iniciativas militares dos Estados Unidos que buscavam desenvolver

uma rede de comunicação descentralizada e resiliente, sendo a ARPANET o marco inicial desse projeto (Corrêa, 2013). Embora tenha sido inicialmente restrita a aplicações acadêmicas e governamentais, a Internet passou por um processo de expansão gradual, alcançando o uso comercial e doméstico a partir da década de 1990.

No Brasil, as primeiras conexões com redes internacionais foram viabilizadas por instituições de pesquisa, mas a popularização da Internet se intensificou na segunda metade dos anos 1990. Esse crescimento foi impulsionado pela disseminação dos microcomputadores, pelo acesso discado e, posteriormente, pela chegada da banda larga. O avanço da mobilidade digital e a adoção em massa de dispositivos conectados aceleraram a transformação digital, promovendo a convergência de mídias e o surgimento de novas formas de interação, como redes sociais, plataformas de conteúdo e ambientes educacionais online (Rocha e Lins, 2013).

Além de seu papel fundamental na transformação da comunicação e do trabalho, a Internet serviu como alicerce para o desenvolvimento de tecnologias inovadoras, como a Internet das Coisas (IoT), que estende a conectividade para o mundo físico. Apesar de seus inúmeros benefícios, o uso intensivo da Internet também traz desafios críticos, como a necessidade de proteger dados pessoais, garantir a segurança das informações transmitidas e promover a inclusão digital de forma equitativa. Tais questões exigem políticas públicas e regulamentações eficazes para assegurar um ambiente digital ético e seguro (Corrêa, 2013; Rocha e Lins, 2013).

2.3 Internet das coisas (Internet of Things)

A Internet das Coisas (IoT) representa uma das principais evoluções tecnológicas da era digital, ao permitir que objetos físicos sejam conectados à internet, viabilizando a coleta e a troca de informações de forma autônoma. Essa abordagem amplia o conceito tradicional de conectividade, que antes se restringia a computadores e smartphones, e passa a incluir uma ampla gama de dispositivos — como sensores, eletrodomésticos, veículos e máquinas industriais — transformando-os em elementos ativos de redes inteligentes (Mancini, 2017).

No ambiente industrial, essa vertente é conhecida como Internet das Coisas Industrial (IIoT) e tem desempenhado papel central na modernização das fábricas. Por meio da integração de sensores e sistemas de automação, torna-se possível acompanhar em tempo real o desempenho de equipamentos, aplicar técnicas de manutenção preditiva e ajustar os

processos produtivos de forma mais precisa. Essa conectividade estendida contribui para reduzir desperdícios, antecipar falhas operacionais e melhorar a tomada de decisões estratégicas com base em dados concretos.

Apesar dos avanços, a adoção da IoT industrial também impõe desafios consideráveis. O grande volume de dados gerados exige estruturas tecnológicas robustas para armazenamento e processamento. Além disso, a segurança da informação torna-se uma prioridade, dada a sensibilidade dos dados envolvidos e os riscos de exposição indevida. Como apontado por Batista da Silva *et al.* (2024), implementar soluções eficazes de IoT requer um planejamento cuidadoso, investimentos em infraestrutura tecnológica e políticas de segurança cibernética adequadas ao contexto altamente conectado e heterogêneo das operações industriais.

2.4 Inteligência Artificial (IA)

A Inteligência Artificial (IA) é considerada uma das tecnologias mais transformadoras da era digital, por sua capacidade de dotar sistemas computacionais com habilidades tradicionalmente atribuídas à cognição humana, como identificar padrões, tomar decisões e aprender com a experiência acumulada em dados. A aspiração de construir máquinas inteligentes é antiga, mas só se tornou concreta com os avanços da computação no pós-Segunda Guerra Mundial, quando surgiram os primeiros modelos que simulam processos mentais básicos (Teixeira, 2019).

Esse campo abrange diversas subáreas, como o aprendizado de máquina (machine learning), redes neurais artificiais, processamento de linguagem natural (PLN) e visão computacional. Cada uma delas busca criar algoritmos e modelos capazes de realizar previsões ou ações com base em grandes volumes de dados históricos. Um marco conceitual importante foi a formulação da “máquina de Turing”, proposta por Alan Turing, que demonstrou a viabilidade de automatizar qualquer tarefa computacional por meio de instruções bem definidas.

Na indústria, a IA tem sido amplamente incorporada a processos que exigem respostas rápidas e precisas. Técnicas como redes neurais e algoritmos supervisionados têm se mostrado eficazes na detecção precoce de falhas, na previsão de eventos operacionais e na otimização contínua de processos produtivos. No entanto, como aponta Sichman (2021), a aplicação de IA nesse contexto também levanta questões relevantes sobre confiabilidade, ética

e transparência das decisões automatizadas.

Mais do que uma ferramenta técnica, a IA representa um campo interdisciplinar que abrange implicações sociais, filosóficas e éticas. Barbosa e Portes (2023, p. 17) destacam que os sistemas inteligentes não apenas processam dados, mas também os interpretam e os utilizam de maneira autônoma para alcançar objetivos específicos, o que exige reflexão crítica sobre os limites e responsabilidades associados a essas tecnologias.

2.5 Manutenção Preditiva

A manutenção preditiva consiste em uma abordagem voltada à identificação precoce de falhas em equipamentos industriais, com base no acompanhamento contínuo de variáveis operacionais como vibração, ruído, temperatura e pressão. Seu principal diferencial reside na capacidade de fornecer um diagnóstico em tempo real sobre o estado dos ativos, o que permite antecipar intervenções antes que ocorram falhas inesperadas ou danos mais severos. Essa estratégia tem ganhado destaque por possibilitar a redução de custos com manutenções corretivas e por promover maior confiabilidade nos processos produtivos (Baldissarelli e Fabro, 2019).

Essa prática depende da instalação de sensores nos equipamentos, responsáveis por coletar dados de funcionamento de forma automatizada. As informações obtidas são analisadas de maneira contínua, permitindo a identificação de comportamentos anômalos mesmo sem a interrupção das operações. Segundo Souza (2013), essa antecipação favorece um planejamento mais eficiente das intervenções, prolonga a vida útil dos componentes monitorados e reduz os riscos de paradas imprevistas.

Com o avanço das tecnologias habilitadoras da Indústria 4.0, como IoT e IA, a manutenção preditiva foi significativamente ampliada. A possibilidade de analisar grandes volumes de dados em tempo real, com base em históricos operacionais e padrões de desempenho específicos, elevou o nível de precisão dos diagnósticos. A integração entre essas tecnologias permite uma resposta rápida diante de alterações no comportamento dos sistemas, aumentando a eficiência operacional e fortalecendo a tomada de decisão (Baldissarelli e Fabro, 2019).

Dessa maneira, a manutenção preditiva consolida-se como um recurso estratégico para empresas que desejam aumentar a disponibilidade de seus ativos, reduzir desperdícios e

otimizar recursos. Além de melhorar a performance dos equipamentos, essa prática também contribui para a evolução digital das organizações, tornando-as mais preparadas para lidar com os desafios de um ambiente industrial dinâmico e altamente automatizado.

2.6 Sistemas Especialistas na Manutenção Preditiva

Os sistemas especialistas representam uma aplicação relevante da inteligência artificial no ambiente industrial, especialmente em estratégias de manutenção preditiva. Seu objetivo é simular o raciocínio de profissionais experientes por meio de um conjunto de regras organizadas em uma base de conhecimento específica. Com o apoio de mecanismos de inferência, essas regras são utilizadas para interpretar dados operacionais, identificar anomalias e indicar possíveis ações corretivas (Jackson, 1999).

No contexto da Indústria 4.0, essa tecnologia tem ganhado espaço por sua capacidade de antecipar falhas e reduzir paradas inesperadas. Como apontado por Lee, Kao e Yang (2014), ao processar continuamente informações como variações de temperatura, pressão ou vibração, os sistemas especialistas auxiliam na manutenção da disponibilidade e do desempenho dos ativos.

As decisões tomadas por esses sistemas geralmente se baseiam em estruturas condicionais do tipo “se-então”. Por exemplo: “se o nível de vibração ultrapassar determinado limite, acionar alerta de manutenção”. Conforme destacado por Moura e Oliveira (2017), essas regras podem variar em complexidade, indo desde instruções diretas até abordagens mais flexíveis, como a lógica fuzzy, que é útil para tratar incertezas presentes em ambientes industriais reais.

A integração dos sistemas especialistas com a Internet das Coisas ampliou consideravelmente suas possibilidades. Com sensores conectados em tempo real, os dados são enviados de forma contínua para análise, permitindo diagnósticos ágeis e decisões automatizadas. Porter e Heppelmann (2014) ressaltam que essa conectividade viabiliza intervenções imediatas diante de condições críticas, aumentando a eficácia do sistema.

Atualmente, observa-se também o crescimento de modelos híbridos, que combinam regras fixas com algoritmos de aprendizado de máquina. Essa fusão permite que os sistemas se ajustem ao longo do tempo com base em novos dados, aumentando sua precisão e adaptabilidade em ambientes de alta variabilidade.

Assim, os sistemas especialistas consolidam-se como uma ferramenta prática para incorporar o conhecimento técnico em processos automatizados, oferecendo suporte ágil à tomada de decisão, com rastreabilidade e padronização — características essenciais na gestão moderna da manutenção industrial.

2.7 Modelos de Aprendizado de Máquina (*Machine Learning*) e Redes Neurais na Manutenção Preditiva

Os avanços no campo do aprendizado de máquina têm permitido o desenvolvimento de modelos computacionais cada vez mais sofisticados para prever falhas e melhorar a eficiência dos processos industriais. Essa abordagem baseia-se na capacidade de algoritmos em identificar padrões complexos em grandes volumes de dados operacionais, viabilizando a realização automática de previsões e auxiliando na tomada de decisões fundamentadas. Ferreira *et al.* (2018) destacam que essa tecnologia se sobressai em ambientes industriais devido à sua habilidade de processar informações em tempo real e oferecer diagnósticos precisos.

Entre as técnicas mais utilizadas nesse contexto estão as redes neurais artificiais, inspiradas na estrutura dos neurônios humanos. Compostas por múltiplas camadas interconectadas, essas redes são capazes de aprender a partir de dados históricos e prever situações futuras com base em novas informações. Borges *et al.* (2020) observam que esse tipo de modelo é particularmente eficaz na detecção de pequenas variações nos dados que podem indicar o início de falhas operacionais.

Além das redes neurais, outros algoritmos como árvores de decisão, máquinas de vetor de suporte (*SVM*) e florestas aleatórias também são amplamente aplicados para aprimorar a confiabilidade dos diagnósticos. Moura Filho *et al.* (2020) sugerem que a combinação dessas técnicas em arquiteturas híbridas pode tornar os modelos mais robustos, reduzindo a incidência de falsos alarmes.

Entretanto, o desempenho dessas ferramentas está diretamente ligado à qualidade dos dados utilizados durante o treinamento. Dados incompletos, ruidosos ou mal classificados podem comprometer a eficácia dos modelos. Por isso, é essencial aplicar estratégias de pré-processamento, normalização e seleção adequada de variáveis para assegurar resultados consistentes.

O aprendizado de máquina é uma peça-chave no conceito de manutenção inteligente, permitindo que os sistemas não apenas identifiquem potenciais falhas, mas também proponham soluções corretivas e adaptem suas estratégias com base na experiência acumulada. Essa capacidade de evolução contínua torna os modelos preditivos mais alinhados com as demandas de ambientes industriais modernos, caracterizados por elevada automação e constante variabilidade operacional.

2.8 Segurança em Sistemas IoT e IA na Manutenção Preditiva

A introdução de tecnologias como a Internet das Coisas e a Inteligência Artificial no ambiente industrial exige um cuidado redobrado com a segurança da informação. Em sistemas de manutenção preditiva, a troca constante de dados entre sensores, dispositivos conectados e plataformas analíticas eleva significativamente os riscos de acessos indevidos, interceptações maliciosas e manipulações que podem comprometer a integridade do sistema como um todo. Por isso, garantir a proteção das informações torna-se um aspecto estratégico, e não apenas técnico.

Segundo Almeida e Soares (2022), em ambientes digitais altamente integrados, a segurança deve ser pensada desde o início dos projetos, com a adoção de práticas como o uso de protocolos seguros de comunicação, criptografia de ponta, autenticação multifatorial e controles rigorosos de acesso. A ausência dessas camadas de proteção pode acarretar impactos que vão além do operacional, atingindo também as esferas financeira e jurídica das organizações.

A aderência às legislações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD), é outro ponto fundamental nesse cenário. Mesmo dados provenientes de sensores industriais podem conter informações sensíveis, cuja exposição pode representar riscos tanto à empresa quanto a seus parceiros. Conforme apontado por Nascimento e Silva (2023), incorporar medidas de segurança já na fase de concepção dos sistemas não apenas fortalece a proteção técnica, mas também reforça a confiança entre os agentes envolvidos nos processos produtivos e tecnológicos.

Entretanto, a tecnologia por si só não é suficiente. A criação de uma cultura organizacional voltada à segurança digital é igualmente necessária. Iniciativas como programas de capacitação contínua, atualizações regulares de software e auditorias sistemáticas contribuem para identificar e mitigar vulnerabilidades de forma proativa. Nesse

contexto, proteger a informação é mais do que uma medida de prevenção: é uma condição essencial para a resiliência e sustentabilidade das operações industriais que dependem de IA e IoT.

2.9 Controle de Acesso e Gerenciamento de Identidade no Sistema de Manutenção Preditiva

O controle de acesso baseado em perfis de usuários é um dos pilares da segurança da informação em sistemas que utilizam tecnologias como IoT e IA, especialmente em soluções de manutenção preditiva. Esse tipo de gerenciamento assegura que apenas pessoas devidamente autorizadas possam visualizar, editar ou manipular dados sensíveis, como leituras captadas por sensores ou resultados de análises preditivas.

No sistema ERPNext, utilizado neste estudo, as permissões foram configuradas de acordo com as funções operacionais dos usuários. Cada perfil tem um conjunto específico de acessos, projetado para limitar suas ações conforme o nível de responsabilidade e a necessidade de atuação:

- **Operador**: possui acesso para leitura, edição, criação e exclusão de registros, além de submissão, mas não tem permissão para exportar dados. Essa configuração permite o ajuste de informações registradas, sem comprometer a integridade externa dos dados.

- **Técnico de Manutenção**: limitado à leitura, esse perfil permite a consulta às informações relevantes para o diagnóstico e atuação na manutenção, sem a possibilidade de modificar registros, evitando alterações indevidas.

- **Analista de IA**: tem acesso de leitura e exportação. Isso possibilita a extração dos dados necessários para o desenvolvimento e execução de modelos analíticos, sem a capacidade de alterar ou adicionar dados ao sistema.

- **Supervisor**: possui todas as permissões habilitadas, incluindo leitura, edição, criação, exclusão e exportação. Este papel gerencial garante total controle sobre o sistema, permitindo ajustes globais e validação de informações.

O impacto desse modelo de controle sobre a segurança da informação é significativo. Ao atribuir permissões de maneira segmentada, evita-se que usuários executem ações além de suas atribuições, o que reduz o risco de falhas humanas ou acessos indevidos. A possibilidade de exportar dados, por exemplo, é restrita a perfis específicos, assegurando que análises externas possam ocorrer sem comprometer a base de dados original.

De forma geral, definir e aplicar um modelo eficaz de controle de acesso é essencial para garantir a confiabilidade do sistema, apoiar diagnósticos precisos e proteger dados estratégicos. Esse cuidado permite que as empresas mantenham um ambiente digital controlado e seguro, favorecendo a continuidade operacional e a prevenção de riscos.

2.10 Proteção contra Dados Inválidos e Manipulação de Dados

Com o avanço da Internet das Coisas na indústria, surgem não apenas ganhos em eficiência operacional, mas também preocupações crescentes quanto à qualidade e integridade dos dados coletados. Muitos dispositivos conectados, especialmente os de baixo custo, operam com limitações significativas em termos de segurança e capacidade de processamento. Isso os torna vulneráveis a falhas de autenticação, ausência de criptografia e à falta de mecanismos eficazes de validação. Como observam Silva, Santos e Pereira (2022), essas deficiências são visíveis até em aplicações domésticas e se tornam ainda mais críticas em ambientes industriais, onde decisões automatizadas dependem diretamente da confiabilidade dos dados.

Em sistemas preditivos baseados em inteligência artificial, a qualidade dos dados desempenha um papel central. Algoritmos treinados com informações distorcidas, incompletas ou manipuladas podem gerar interpretações equivocadas, afetando a precisão das previsões. Cruz (2024) alerta para os riscos do viés algorítmico e para os erros sistemáticos que podem surgir quando não há um controle rigoroso ao longo de todo o ciclo de vida dos dados — da captura à análise. A ausência de boas práticas nesse processo pode levar a decisões incorretas, manutenções desnecessárias ou até mesmo à falha em identificar problemas reais.

Para mitigar esses riscos, autores como Estrada *et al.* (2024) sugerem a adoção de tecnologias emergentes, como o *blockchain* e a própria IA aplicada à segurança. O uso do *blockchain*, por exemplo, oferece uma trilha de auditoria confiável e imutável, garantindo a rastreabilidade de leituras sensoriais e impedindo alterações indevidas. Por sua vez, sistemas

inteligentes, quando aliados a boas práticas de engenharia de dados, são capazes de detectar padrões anômalos automaticamente, sinalizando informações que fujam do comportamento esperado.

Proteger os dados contra distorções, adulterações ou inconsistências é, portanto, um requisito básico para a confiabilidade dos sistemas de manutenção preditiva. Entre as práticas recomendadas estão a validação em tempo real, a padronização das entradas, a autenticação das fontes e a incorporação de tecnologias que garantam transparência e integridade. Essas medidas fortalecem a robustez dos modelos analíticos e asseguram que as decisões baseadas em IA estejam fundamentadas em informações precisas e confiáveis.

2.11 Auditoria de Execuções da IA

A evolução da Indústria 4.0, impulsionada pela convergência entre Internet das Coisas e Inteligência Artificial, ampliou significativamente o papel dos sistemas automatizados na tomada de decisão. Nesse contexto, a auditoria das execuções algorítmicas torna-se uma necessidade estratégica, sobretudo em cenários industriais, onde decisões baseadas em IA podem impactar diretamente a operação de máquinas e a segurança dos dados.

Conforme discute Kaufman (2021), modelos baseados em redes neurais profundas (*DLNNs*), embora eficazes, apresentam desafios de transparência e aplicabilidade, frequentemente classificados como o "problema da caixa-preta". Essa característica dificulta a compreensão do processo decisório interno desses modelos, o que pode acarretar riscos éticos, como vieses não detectados e falta de clareza sobre quem é responsável por determinadas ações. Diante disso, a autora defende a realização de auditorias externas e imparciais, voltadas não apenas para os resultados, mas também para a conformidade com padrões regulatórios e princípios éticos.

Lerner e Flach (2024) propõem uma abordagem prática para esse desafio, utilizando Modelos de Linguagem de Grande Escala (*LLMs*) como o *LLama 3* em ambientes isolados, o que garante maior proteção a dados sensíveis e aderência à Lei Geral de Proteção de Dados. Essa estratégia permite ajustes contínuos por meio de técnicas de personalização (*prompts e fine-tuning*), facilitando o rastreamento das respostas e o controle sobre as variáveis envolvidas na tomada de decisão automatizada.

Já Reyes (2023) ressalta que as auditorias de IA não devem se limitar a processos estáticos. Ele argumenta que o monitoramento contínuo e proativo das execuções é fundamental para identificar anomalias e inconsistências em tempo real. Ferramentas de análise de grandes volumes de dados, aprendizado de máquina e processamento de linguagem natural (*NLP*) tornam possível esse tipo de avaliação dinâmica, mas a supervisão humana continua indispensável para validar e contextualizar os achados.

Almeida e Souza (2025) ampliam essa visão ao descrever o conceito de auditoria contínua — uma evolução do modelo tradicional, adaptada à realidade de sistemas digitais em constante operação. Nessa abordagem, a IA também atua como agente de auditoria, analisando logs, registros e eventos operacionais à medida que ocorrem. Tecnologias como *blockchain* e *machine learning* podem reforçar esse processo, desde que acompanhadas por políticas claras de governança e critérios bem definidos de supervisão.

Por fim, a presença da IA em processos decisórios exige mais do que automação técnica: requer mecanismos de responsabilidade. Como destaca Kaufman (2021), é fundamental que exista uma instância humana capaz de responder pelas decisões geradas, explicá-las e, quando necessário, corrigi-las. Nesse cenário, a auditoria das execuções se consolida como uma prática essencial para garantir a legitimidade, a segurança e a confiabilidade dos sistemas de inteligência artificial aplicados à indústria.

2.12 Restrição de Execução Externa

Limitar o acesso externo a sistemas industriais é uma medida essencial para proteger dados e garantir a integridade das operações em ambientes que utilizam Internet das Coisas e Inteligência Artificial. A principal finalidade dessa restrição é evitar interferências de agentes não autorizados, prevenindo ações maliciosas que possam comprometer o funcionamento do sistema ou expor informações sensíveis.

Dentre as principais práticas utilizadas nesse contexto estão os *firewalls* de próxima geração (*NGFWs*), capazes de filtrar o tráfego de rede com base em análise profunda de pacotes, protocolos e padrões comportamentais Fernández *et al.* (2020). Já as redes privadas virtuais (*VPNs*) oferecem uma camada adicional de proteção ao criar túneis criptografados entre os dispositivos e a rede interna, restringindo o acesso a equipamentos previamente autenticados.

Outra prática importante é o uso de listas de controle de acesso (*ACLs*), que determinam quais usuários ou endereços IP podem interagir com os sistemas. Segundo Nascimento e Silva (2020), essas listas são simples de configurar e bastante eficazes para impedir acessos indesejados. A segmentação da rede, por sua vez, limita a exposição de dispositivos críticos, isolando-os de zonas mais vulneráveis.

Além dessas barreiras, é fundamental controlar a execução de scripts externos. O ambiente interconectado da IoT amplia a superfície de ataque, especialmente quando códigos não verificados podem ser executados remotamente. Lima *et al.* (2021) alertam para os riscos associados a esse tipo de brecha, que pode resultar em ataques de negação de serviço (*DoS*) ou exploração de vulnerabilidades. Para mitigar esses riscos, é recomendável implementar autenticação rígida, auditoria de execuções e validação prévia de scripts.

Silva *et al.* (2021) enfatizam que em sistemas críticos, como os voltados à manutenção preditiva, a execução automatizada deve ocorrer somente sob condições controladas, com registros detalhados de cada ação. Essa rastreabilidade é vital para garantir a segurança operacional e facilitar a investigação de incidentes, caso ocorram.

Portanto, a combinação de tecnologias de proteção — como f*irewalls, VPNs, ACLs* e auditoria de *scripts* — é essencial para preservar a confiabilidade dos sistemas industriais baseados em IA e IoT. A proteção contra acessos externos não autorizados é um requisito básico para qualquer ambiente conectado que lide com dados sensíveis e operações estratégicas.

2.13 Conformidade com a Indústria 4.0

A Indústria 4.0 representa uma nova era da manufatura, caracterizada pela fusão entre os mundos físico e digital por meio de tecnologias como Internet das Coisas, Inteligência Artificial, *Big Data*, computação em nuvem e impressão 3D. Essa integração transforma profundamente os processos produtivos, desde o desenvolvimento até a manutenção dos produtos Kipper *et al.* (2024).

Conforme discutido por Tortorelli *et al.* (2024), estar em conformidade com esse novo paradigma não significa apenas adotar ferramentas tecnológicas, mas também reformular a forma como decisões são tomadas e operações são gerenciadas. Tecnologias como *MRP* (*Manufacturing Resource Planning*) e *CAPP (Computer-Aided Process Planning)*

exemplificam essa mudança, permitindo fluxos de trabalho baseados em dados em tempo real e decisões autônomas, cada vez mais dependentes de sistemas inteligentes.

A manufatura avançada, segundo Pinto, Lima e Maduro (2024), demanda não apenas sensores e conectividade, mas também o uso intensivo da IA para previsão de falhas, análise de desempenho e resposta adaptativa a mudanças nas condições operacionais. Isso exige não apenas infraestrutura tecnológica moderna, mas também profissionais capacitados para operar em ambientes digitais e políticas robustas de cibersegurança.

No Brasil, a adaptação à Indústria 4.0 ainda enfrenta obstáculos como altos custos de implementação, falta de infraestrutura adequada e escassez de mão de obra qualificada Takayama e Panhan (2022). Mesmo assim, iniciativas como a Política Nacional de Inovação e a atuação da Câmara Brasileira da Indústria 4.0 têm buscado criar um ambiente mais propício à transformação digital.

Neste trabalho, o projeto que propõe a integração entre IA e IoT para manutenção preditiva se alinha diretamente aos princípios da Indústria 4.0. Ele incorpora automação inteligente, coleta e análise de dados em tempo real e redução da intervenção humana em processos críticos, contribuindo para maior eficiência e segurança operacional. A conformidade com esse modelo exige, além de recursos técnicos, uma mudança de mentalidade nas organizações, com foco em inovação, gestão baseada em dados e cibersegurança como requisito estratégico.

3 METODOLOGIA

Este trabalho utiliza uma abordagem metodológica exploratória e aplicada. A pesquisa é considerada exploratória por investigar, de forma aprofundada, como as tecnologias de Inteligência Artificial (IA) e Internet das Coisas (IoT) podem ser integradas para promover melhorias nos processos de manutenção preditiva — um campo ainda em evolução no contexto da Indústria 4.0. Trata-se também de uma pesquisa aplicada, pois tem como finalidade a solução de um problema concreto por meio do desenvolvimento e validação de um protótipo funcional, voltado ao monitoramento e diagnóstico inteligente de equipamentos industriais. Os procedimentos envolveram revisão bibliográfica, escolha de ferramentas tecnológicas adequadas, implementação de funcionalidades específicas na plataforma ERPNext e simulação de cenários para validação dos resultados. Assim, a metodologia adotada alia fundamentação teórica e aplicação prática com o objetivo de gerar conhecimento técnico-científico útil para o setor industrial.

3.1 Descrição do Sistema

O sistema desenvolvido neste projeto tem como finalidade antecipar falhas em equipamentos industriais por meio da integração entre Inteligência Artificial e Internet das Coisas. A proposta foi implementada sobre a plataforma *ERPNext*, um sistema de gestão empresarial de código aberto, que serviu como base para registrar e gerenciar os dados operacionais. Através de sensores conectados, as informações foram captadas em tempo real e armazenadas no *ERP*. A partir desses dados, um conjunto de regras inteligentes foi utilizado para identificar padrões de desgaste e, sempre que necessário, gerar automaticamente registros relacionados à manutenção preditiva.

3.2 Procedimentos de Implementação

A implementação do sistema foi dividida em várias etapas. A seguir, detalhamos os *scripts* utilizados em cada uma das fases:

3.2.1 Instalação do *ERPNext*

A instalação do ERPNext foi realizada utilizando um script automatizado desenvolvido para configurar o ambiente, instalar as dependências, preparar o banco de dados e iniciar a aplicação.

Esse script realiza todo o processo de instalação, incluindo a configuração do MariaDB, a instalação do Node.js e do Yarn via NVM, e a criação do site ERPNext com o banco de dados associado.

O conteúdo completo do script pode ser consultado no Apêndice A.

3.2.2 Criação do *Doctype* "SensorLeitura"

O *DocType* "SensorLeitura" foi criado por meio da interface gráfica do *ERPNext*. O objetivo desse *DocType* é gerenciar as leituras dos sensores, armazenando as informações essenciais para o funcionamento do sistema de manutenção preditiva. A seguir (Tabela 1) estão os campos configurados para esse *DocType*:

Tabela 1 – Estrutura dos campos do DocType "SensorLeitura" no ERPNext

Campo	**Tipo**	**Nome**	**Descrição**
ID do Sensor	Data	id_do_sensor	Este campo é utilizado para armazenar o identificador único de cada sensor.
Tipo do Sensor	*Select*	tipo_do_sensor	Define o tipo de sensor utilizado para coletar os dados (opções: Temperatura, Vibração, Pressão, Umidade, Outros).
Valor da Leitura	*Float*	valor_da_leitura	Armazena o valor numérico da leitura realizada pelo sensor.
Unidade	Data	unidade	Define a unidade de medida da leitura, como °C para

			temperatura, Pa para pressão e mm/s para vibração.
Data/Hora da Leitura	*Datetime*	data_hora	Armazena a data e hora em que a leitura foi realizada pelo sensor.
Status	*Select*	*status*	Define o *status* da leitura, que pode ser Normal, Alerta ou Crítico para indicar a gravidade da leitura coletada.

Fonte: Próprio Autor

Essa estrutura de campos no *DocType* "SensorLeitura" permite um controle detalhado das informações de cada leitura realizada pelos sensores, facilitando a análise e as ações da manutenção preditiva. Cada campo foi cuidadosamente configurado para suportar a coleta e o gerenciamento eficaz dos dados dos sensores no sistema *ERPNext*.

3.2.3 Criação do *DocType* Manutenção Preditiva

O *DocType* Manutenção Preditiva foi desenvolvido no *ERPNext* com o objetivo de registrar as informações relacionadas à análise preditiva de manutenção dos sensores conectados ao sistema. A criação do *DocType* foi realizada por meio da interface gráfica do *ERPNext*, onde foram definidos os campos necessários para capturar e armazenar as leituras dos sensores, os resultados das análises preditivas, e o *status* das manutenções.

Campos do *DocType* Manutenção Preditiva

A seguir, a tabela 2 com a descrição dos campos utilizados no *DocType* Manutenção Preditiva:

Tabela 2 – Descrição dos campos do DocType "Manutenção Preditiva" no ERPNext

No.	**Label**	**Type**	**Name**	**Options**
1	ID do Sensor	*Link*	id_do_sensor	SensorLeitura
2	Data/Hora da Análise	*Datetime*	datahora_da_analise	
3	Valor Avaliado	*Float*	valor_avaliado	
4	*Status* Previsto	*Select*	status_previsto	Ok, Alerta, Manutenção
5	Comentário	*Small Text*	comentario	

Fonte: Próprio Autor

Descrição dos Campos:

ID do Sensor: Este campo está vinculado ao *DocType* SensorLeitura e armazena o identificador do sensor cujos dados foram analisados. Ele é do tipo *Link*, o que permite que o sistema se conecte diretamente ao registro do sensor, proporcionando uma navegação fácil entre os dados.

1. Data/Hora da Análise: Armazena o *timestamp* da análise preditiva feita sobre os dados do sensor. O tipo de campo é *Datetime*, essencial para o registro da data e hora da execução da manutenção preditiva.
2. Valor Avaliado: Este campo registra o valor numérico resultante da análise preditiva. O tipo de campo é *Float*, permitindo o armazenamento de valores decimais.
3. *Status* Previsto: O *status* da manutenção previsto com base nos dados analisados. O campo é do tipo *Select*, com opções Ok, Alerta, e Manutenção, permitindo a classificação do estado do sensor de acordo com as regras de IA definidas no sistema.

4. Comentário: Este campo foi criado para permitir que os analistas ou responsáveis pela manutenção deixe um comentário adicional sobre a análise. Ele é do tipo *Small Text*, permitindo a inserção de um texto breve.

Importância do *DocType* Manutenção Preditiva

A criação deste *DocType* foi fundamental para a integração dos dados de manutenção com a parte preditiva do sistema, permitindo uma gestão eficiente e uma visão clara das manutenções previstas, sem a necessidade de intervenção manual constante. O uso dos campos adequados, como o campo de ID do Sensor vinculado ao SensorLeitura, e o uso do campo *Status* Previsto para definir ações de manutenção, proporcionam uma gestão inteligente e automática, alinhada aos conceitos de Manutenção Preditiva com o uso de IA e IoT.

3.2.4 Simulação de Manutenção Preditiva

A manutenção preditiva foi simulada utilizando regras de Inteligência Artificial. As leituras dos sensores foram avaliadas com base em limites de segurança predefinidos e, sempre que algum valor ultrapassa esses limites, um registro de manutenção preditiva era gerado automaticamente no sistema.

A lógica de simulação considera parâmetros como temperatura, pressão e vibração, associando cada leitura a um status (“Ok” ou “Alerta”) com base nos valores observados. O processo é executado em lote, e os resultados são inseridos em registros específicos no ERP para análise posterior.

O script completo responsável por esta simulação encontra-se no Apêndice B.

3.2.5 Implementação de Auditoria de Execução (*Logs*)

Este tópico agora abordará, de forma geral, como os processos de segurança foram implementados no sistema. Incluindo:

- **Controle de Acesso**: Descrição de como o acesso ao sistema é restringido com base em diferentes perfis de usuário.

- **Proteção contra Dados Inválidos**: Como o sistema valida os dados recebidos para garantir a integridade e segurança da informação.

- **Restrição de Execução Externa**: As medidas tomadas para impedir a execução de *scripts* não autorizados e proteger o sistema contra acessos externos indesejados.

3.3 Testes e Validação

A validação do sistema foi realizada utilizando cenários de teste, que simulam diferentes condições de leitura de sensores para verificar se as regras de manutenção preditiva estão funcionando corretamente e se o sistema de auditoria de execução está registrando os *logs* adequadamente.

3.4 Escolha do *ERPNext* e Comparativo com Outros Softwares

A escolha do sistema de gestão para o projeto foi uma decisão estratégica que levou em consideração diversos fatores, como a flexibilidade, o custo-benefício, a capacidade de integração com outras tecnologias, e a facilidade de personalização. A plataforma *ERPNext* foi escolhida por ser uma solução *open-source*, altamente configurável e que oferece um módulo de manutenção adequado para o gerenciamento de ativos e ordens de serviço. Este módulo é essencial para o desenvolvimento da funcionalidade de manutenção preditiva integrada com IoT e IA.

O *ERPNext* se destaca pela sua facilidade de integração com tecnologias de sensores IoT e a possibilidade de expandir suas funcionalidades para incluir algoritmos de inteligência artificial (IA). A plataforma permite o desenvolvimento e personalização de *Doctypes* para o gerenciamento de dados de sensores e a execução de tarefas automatizadas, como a manutenção preditiva. Porém, uma desvantagem do *ERPNext* é sua complexidade na configuração e a curva de aprendizado para implementar integrações mais avançadas.

Além do *ERPNext*, foi realizada uma comparação com outros sistemas de gestão, como o *OpenMAINT*, *CMMS* (*Maintenance Assistant*), *Snipe-IT, FMIS, Mainsys, AssetTiger* e outros softwares do mercado. A seguir, apresentamos a descrição de cada software, suas

funcionalidades e um comparativo geral para avaliar a adequação a um sistema de manutenção preditiva com IoT e IA.

Descrição dos Softwares

OpenMAINT

- Descrição: Software *open-source* de gerenciamento de ativos e manutenção de instalações, utilizado principalmente para o controle de bens físicos, como equipamentos e infraestrutura.
- Funcionalidade: Inclui módulos de manutenção preventiva e corretiva, gestão de inventário e controle financeiro.

CMMS (Maintenance Assistant)

- Descrição: Sistema de gerenciamento de manutenção de equipamentos industriais.
- Funcionalidade: Permite planejar, monitorar e registrar ordens de serviço, além de acompanhar ativos e gerenciar peças de reposição.

Snipe-IT

- Descrição: Software de gerenciamento de ativos de TI, focado no rastreamento de hardware, licenças e dispositivos.
- Funcionalidade: Facilita o acompanhamento da vida útil dos ativos e o controle de alocações de equipamentos.

FMIS (Facilities Management Information System)

- Descrição: Sistema para o gerenciamento de instalações físicas, com foco em infraestrutura e recursos prediais.
- Funcionalidade: Inclui módulos de manutenção, rastreamento de ativos e planejamento de espaço.

Mainsys

- Descrição: Sistema especializado em manutenção industrial, que permite o controle de ativos e monitoramento de equipamentos.
- Funcionalidade: Suporta ordens de serviço, gestão de desempenho e manutenção preditiva baseada em dados de sensores.

AssetTiger

- Descrição: Sistema de rastreamento de ativos, focado em empresas de TI.
- Funcionalidade: Fornece controle de inventário, alertas de manutenção e rastreamento de histórico.

ERPNext

- Descrição: Sistema de ERP *open-source* com módulo de manutenção para o gerenciamento de ativos e ordens de serviço.
- Funcionalidade: Permite agendar manutenções, controlar ordens de serviço, gerenciar estoques e gerar relatórios analíticos.

Tabela 3 – Comparativo dos softwares de gestão de manutenção e integração com IoT e IA

Software	**Foco Principal**	**Manutenção Preventiva/Corretiva**	**Gestão de Ativos**	**Relatórios e Análises**	**Integração com IoT**	**Facilidade de Implementação**	**Melhor para IoT e IA?**
OpenMAINT	Gestão de ativos e manutenção predial	Sim	Sim	Sim	Parcial	Média	Parcial
CMMS	Manutenção de equipamentos industriais	Sim	Sim	Sim	Parcial	Média	Sim
Snipe-IT	Gestão de ativos de TI	Não	Sim	Sim	Não	Alta	Não
FMIS	Gestão de instalações	Sim	Sim	Sim	Parcial	Média	Parcial
Mainsys	Manutenção industrial	Sim	Sim	Sim	Sim	Média	Sim
AssetTiger	Rastreio de ativos de TI	Sim	Sim	Sim	Não	Alta	Não

ERPNext	ERP com módulo de manutençã o	Sim	Sim	Sim	Sim	Baixa	Sim

Fonte: Próprio Autor

Melhor Escolha para o TCC

A escolha do software de gestão depende das necessidades do sistema de manutenção preditiva integrado com IoT e IA. Considerando a análise feita, as melhores opções para esse projeto seriam:

1. Mainsys – Oferece suporte à manutenção preditiva baseada em dados, alinhando-se bem com IA e IoT, o que é crucial para a previsão de falhas.

2. CMMS (Maintenance Assistant) – É focado em manutenção industrial e pode ser facilmente integrado a sistemas IoT.

3. *ERPNext* – Embora a implementação de IoT e IA seja mais complexa no *ERPNext*, sua flexibilidade e a possibilidade de personalização fazem dele uma boa escolha para integrar IA e IoT em um sistema de manutenção preditiva.

Caso o foco seja em manutenção preditiva avançada, o Mainsys é a melhor opção. Para um sistema mais flexível e com facilidade de integração, o *ERPNext* é recomendado. Se for necessário um sistema simples e eficiente, o CMMS pode ser a escolha ideal.

3.5 Especificações e Configurações da Máquina de Desenvolvimento

A parte prática do desenvolvimento foi realizada utilizando uma máquina virtual configurada no *Oracle VM VirtualBox*. A escolha por uma máquina virtual foi feita devido à sua flexibilidade e ao isolamento que oferece, permitindo um ambiente de testes controlado e seguro, além de garantir a replicabilidade do ambiente de desenvolvimento.

Configurações da Máquina Virtual:

A máquina virtual foi configurada com o sistema operacional *Ubuntu* 64-bit para garantir compatibilidade com as tecnologias utilizadas no desenvolvimento, como o *ERPNext*, *Python*, IoT e IA. A seguir, estão as especificações detalhadas da máquina virtual utilizada:

- Sistema Operacional: *Ubuntu* 64-bit
- Memória RAM: 2 GB
- Armazenamento: 25 GB (disco virtual com formato *VDI*)
- Placa de Rede: Adaptador Intel PRO/1000 MT Desktop (*NAT*)
- Controladora Gráfica: *VMSVGA*
- Áudio: Padrão, com controlador *ICH AC97*

A máquina virtual foi configurada para utilizar rede NAT, permitindo que a VM tenha acesso à internet, essencial para a instalação de dependências e comunicação com o sistema *ERPNext* hospedado.

Motivação para o Uso da Máquina Virtual:

O uso de uma máquina virtual permite um ambiente isolado e dedicado para o desenvolvimento e testes do sistema, sem interferir nas configurações principais da máquina física. Além disso, a máquina virtual oferece a capacidade de testar diferentes versões do sistema operacional e das ferramentas utilizadas, sem a necessidade de realizar mudanças permanentes no sistema físico.

4 DESENVOLVIMENTO

Este capítulo aborda a aplicação prática dos conceitos discutidos anteriormente, analisando como a IA e a IoT estão sendo utilizadas na manutenção preditiva e na segurança da informação no contexto da Indústria 4.0. São discutidos casos reais, tecnologias empregadas, benefícios, desafios e estratégias de implementação. Busca-se demonstrar os impactos e as contribuições dessas tecnologias para o setor industrial.

4.1 Simulação e Implementação da IA

4.1.1 Objetivo da Implementação da IA

A implementação da Inteligência Artificial (IA) no projeto tem como objetivo prever falhas em equipamentos industriais antes que estas ocorram, utilizando dados coletados por sensores IoT. A intenção é evitar manutenções corretivas, reduzindo custos e melhorando a eficiência operacional. A IA, nesse contexto, atua como um sistema inteligente de apoio à decisão, identificando padrões em leituras de sensores e classificando automaticamente o *status* do equipamento.

4.1.2 Algoritmos de IA Utilizados

Escolha da Abordagem de IA

Nesta fase do projeto, optou-se pela utilização de um sistema especialista baseado em regras, ao invés de modelos tradicionais de aprendizado de máquina. Essa abordagem foi escolhida devido à necessidade de rápida validação da funcionalidade da manutenção preditiva e à ausência de uma base de dados histórica extensa para treinamento supervisionado. O sistema especialista simula o conhecimento de um especialista humano ao aplicar regras de decisão fixas para analisar os dados dos sensores e prever a necessidade de manutenção.

Estrutura do Sistema Especialista

O sistema desenvolvido segue a estrutura clássica de um sistema especialista, composto por três elementos principais:

Base de Conhecimento: Conjunto de regras do tipo “se-condição-então-ação”, como por exemplo:

- Se a Temperatura ≥ 70, então o *status* é Alerta;
- Se a Pressão ≥ 120, então o *status* é Alerta;
- Se a Vibração ≥ 15, então o *status* é Alerta;

Mecanismo de Inferência: Implementado em *Python*, esse mecanismo percorre os registros de sensores, verifica cada valor com base nas regras, e decide o *status* da máquina (Ok ou Alerta).

Interface com o Sistema: Os resultados do diagnóstico são registrados automaticamente no *ERPNext* por meio do *DocType* ManutencaoPreditiva, e as execuções são auditadas no *DocType* LogExecucaoIA.

Justificativa Técnica

A escolha por um sistema especialista apresenta as seguintes vantagens neste contexto:

Transparência e auditabilidade: As regras são claras e compreensíveis, facilitando a validação do comportamento do sistema;

Simplicidade de implementação: Ideal para projetos iniciais, protótipos e sistemas com conjuntos de regras bem definidos;

Escalabilidade futura: A lógica atual pode futuramente ser substituída ou complementada por algoritmos de aprendizado supervisionado à medida que mais dados forem coletados.

4.1.3 Preparo dos Dados

Coleta e Pré-processamento dos Dados

Para a simulação do sistema de manutenção preditiva, foram utilizadas três bases de dados sintéticos geradas com auxílio de ferramentas de Inteligência Artificial. Os cenários simulados contemplaram diferentes situações operacionais, com o objetivo de testar a eficácia das regras do sistema especialista:

Cenário 1 – Funcionamento Normal: Leituras próximas dos valores de operação padrão, com temperatura abaixo de 75 °C, pressão por volta de 90 Pa e vibração inferior a 12 mm/s.

Cenário 2 – Mistura de Estados: Situações intermediárias com variações que simulam equipamentos alternando entre estado normal e alerta, como temperaturas entre 78 °C e 88 °C e vibrações acima de 15 mm/s.

Cenário 3 – Falha Múltipla: Condições críticas simuladas, com todas as variáveis excedendo os limites, como temperatura superior a 90 °C, pressão acima de 100 Pa e vibração em torno de 18 mm/s.

Esses dados foram carregados no *ERPNext* por meio do módulo de importação de dados no *DocType* SensorLeitura, garantindo estruturação compatível com o sistema especialista desenvolvido.

Organização dos Dados

As variáveis utilizadas em cada cenário foram padronizadas conforme a tabela abaixo, garantindo compatibilidade com o *ERPNext* e clareza no processamento pelos algoritmos de IA, apresentadas na tabela 4:

Tabela 4 – Padronização das Variáveis Utilizadas nos Cenários de Teste

Campo	**Descrição**
ID do Sensor	Identificador único do sensor, combinando tipo e posição (ex: TEMP-04A)
Tipo do Sensor	Categoria do sensor: Temperatura, Pressão ou Vibração
Valor da Leitura	Valor numérico medido pelo sensor
Unidade	Unidade de medida correspondente (°C, Pa, mm/s)
Data/Hora da Leitura	Registro temporal do momento da leitura, no formato `YYYY-MM-DD HH:MM:SS`
Status	Indicador do estado do sensor ou da máquina (ex: Ativo)

Fonte: Próprio autor

Simulação sem Treinamento Clássico

Por se tratar de um sistema especialista baseado em regras, não foi necessário realizar divisão entre dados de treino e teste. No entanto, os três conjuntos de dados foram utilizados para validar a lógica das regras sob diferentes contextos de falha, garantindo diversidade de casos simulados.

4.1.4 Integração com o *ERPNext*

Como os Dados são Enviados ao *ERPNext*

A integração da *IA* com o sistema *ERPNext* foi realizada por meio do uso de *Doctypes* personalizados. Após o *upload* dos dados simulados nos *Doctypes* de leitura (SensorLeitura), o *script* de IA — implementado em *Python* — acessa essas leituras diretamente na base de dados e aplica as regras do sistema especialista.

A inferência do sistema classifica cada leitura como “Ok” ou “Alerta” com base em faixas pré-estabelecidas para os sensores de temperatura, pressão e vibração. Para cada decisão gerada, um novo registro é criado automaticamente no *DocType* ManutencaoPreditiva, contendo:

1. Sensor relacionado;
2. Valor avaliado;
3. Data/hora da análise;
4. *Status* previsto;
5. Comentários explicativos.

Geração de Manutenções Preditivas

O modelo também gera registros no *DocType* LogExecucaoIA, permitindo a rastreabilidade completa de cada execução da IA. Esse log inclui informações como a data/hora da execução e a quantidade de análises realizadas. Isso garante auditoria, controle e possibilidade de revisão futura do comportamento da IA.

Além disso, a previsão de falha é utilizada para acionar processos de manutenção, como abertura de ordens de serviço ou alertas automáticos para os responsáveis.

4.1.5 Resultados da Simulação da IA

Avaliação da Lógica do Sistema

Como a IA implementada é baseada em regras fixas (sistema especialista), não foram aplicadas métricas estatísticas como accuracy, precision ou F1-score. No entanto, a validação foi feita por meio da aplicação das regras sobre bases de dados sintéticas representando diferentes cenários operacionais.

A lógica do sistema demonstrou coerência e capacidade de identificar corretamente os estados “Ok” e “Alerta” de forma automatizada. A simulação confirmou o correto funcionamento do ciclo completo: da leitura à geração da previsão.

Impacto no Sistema

A principal contribuição do sistema está na automação do diagnóstico preventivo, reduzindo a dependência de análises manuais. Mesmo em fase inicial, os benefícios incluem:

1. Previsibilidade de falhas com base em leituras em tempo real;
2. Geração automática de registros e ordens de manutenção;
3. Melhoria na confiabilidade do sistema industrial simulado;

4. Base sólida para futura evolução com IA baseada em dados reais.

4.1.6 Desafios Encontrados na Implementação da IA

Desafios Técnicos

1. Estruturação dos Dados: Foi necessário padronizar os dados simulados para garantir compatibilidade com os campos definidos no *ERPNext*.
2. Validação das Regras: A lógica de inferência precisou ser ajustada para evitar falsos positivos ou negativos em leituras intermediárias.
3. Execução Cíclica: Como o *script* é executado manualmente ou por agendamento, foi necessário controlar a repetição de análises sobre os mesmos dados.

Desafios de Integração

4. Customização do *ERPNext*: Foi preciso criar *Doctypes* personalizados e configurar permissões específicas para garantir segurança e rastreabilidade.
5. Log de Execução: A implementação de um mecanismo de log foi essencial para garantir a auditoria e controle das decisões tomadas pela IA.
6. Ajustes de desempenho: Otimizações foram feitas para que o *script* processe grandes volumes de leituras sem impactar o sistema.

Conclusão do Tópico

Sumarização

A aplicação da Inteligência Artificial na manutenção preditiva mostrou-se uma estratégia eficaz para antecipar falhas e otimizar a gestão de ativos industriais. Mesmo utilizando um sistema especialista simples baseado em regras, foi possível simular um ambiente funcional no qual decisões automatizadas foram tomadas com base em dados de sensores. Essa abordagem permite não apenas a detecção precoce de anomalias, mas também a automação de processos de manutenção, o que contribui diretamente para a redução de custos operacionais, minimização do tempo de inatividade e aumento da confiabilidade das máquinas.

A integração com o *ERPNext* fortalece ainda mais esse processo, centralizando informações, notificações e *logs* em um único ambiente gerencial, promovendo rastreabilidade e maior controle das ações de manutenção.

Possíveis Melhorias Futuras

- Apesar dos resultados positivos alcançados com a abordagem atual, há diversas possibilidades de evolução para tornar o sistema mais robusto e inteligente:
- Substituição das regras fixas por modelos de aprendizado de máquina supervisionado, como árvores de decisão, redes neurais ou regressão logística, utilizando dados reais e históricos para melhorar a acurácia das previsões;
- Adoção de técnicas de aprendizado não supervisionado, como clustering, para detecção automática de padrões anômalos sem a necessidade de rótulos prévios;
    - Melhoria na coleta de dados, com sensores mais precisos, maior frequência de leitura e integração em tempo real;
- Implementação de *dashboards* interativos e relatórios gerenciais com visualização gráfica dos riscos, histórico de falhas e projeções de manutenção;
- Automação da execução da IA por agendamento (*cron jobs*), eliminando a necessidade de execução manual.

Esses aprimoramentos permitiriam transformar o sistema atual em uma solução completa de manutenção preditiva inteligente, com potencial para aplicação real em ambientes industriais.

4.2 Processos de Segurança

4.2.1 Introdução aos Processos de Segurança

No contexto de sistemas que envolvem dados sensíveis e aplicações críticas, como o sistema de manutenção preditiva baseado em IA e IoT, a implementação de processos de segurança robustos é fundamental para proteger os dados e garantir a integridade do sistema. No projeto, foram adotadas várias práticas e medidas de segurança para proteger o acesso ao sistema, garantir a qualidade dos dados, prevenir acessos não autorizados, e controlar a execução de *scripts* externos.

4.2.2 Controle de Acesso por Perfis de Usuários

O controle de acesso é um componente essencial para garantir que apenas usuários autorizados possam acessar funcionalidades específicas do sistema. No *ERPNext*, o controle de acesso foi configurado com base em perfis de usuários, e as permissões foram definidas para cada tipo de usuário, de acordo com suas responsabilidades.

Perfis de Usuários Criados:

1. Operador: Acesso restrito à leitura e edição das leituras de sensores, sem permissão para criar ou excluir dados.
2. Técnico de Manutenção: Acesso restrito à leitura das leituras de sensores.
3. Analista de IA: Acesso somente para leitura e exportação dos dados para processamento fora do ERP.
4. Supervisor: Acesso completo, com permissão para criar, editar, excluir e visualizar todas as leituras dos sensores.

Esses perfis foram definidos para garantir que cada usuário tenha apenas os privilégios necessários para realizar seu trabalho, minimizando os riscos de acessos indevidos ou alterações não autorizadas.

4.2.3 Proteção contra Dados Inválidos e Manipulação de Dados

A proteção contra dados inválidos é crucial para a integridade do sistema, especialmente em aplicações que utilizam IA para análise e tomada de decisões. Dados corrompidos ou inconsistentes podem levar a falhas nos modelos preditivos e comprometer a qualidade das previsões.

Validação de Dados:

Validação de Entrada: Antes de qualquer dado ser inserido ou modificado no sistema, ele passa por um processo de validação rigorosa. Isso inclui a verificação de formatos corretos (como datas, números e unidades), valores dentro dos limites esperados (por exemplo, temperaturas ou pressões dentro de uma faixa segura), e a ausência de dados duplicados.

Monitoramento de Dados: Implementação de monitoramento contínuo para detectar e corrigir dados inválidos ou anômalos em tempo real, minimizando os impactos de falhas nos sensores ou erros de leitura.

4.2.4 Auditoria e Registro de Execuções

Neste tópico, detalharemos a implementação de auditoria no sistema para rastrear todas as execuções da IA, garantindo que as operações sejam registradas e possam ser auditadas. A auditoria é crucial para a segurança, pois permite verificar o histórico das ações realizadas e monitorar qualquer operação de risco.

O processo de auditoria foi implementado utilizando o módulo de logs do ERPNext, que registra informações detalhadas sobre a execução do algoritmo de IA e ações realizadas pelo sistema.

O script utilizado para esse controle está descrito no Apêndice B.

O código executa automaticamente após cada análise da IA, criando um documento do tipo *LogExecucaoIA* com os seguintes campos:

1. **data_hora_execucao**: Registra a data e hora exatas da execução.
2. **usuario**: Armazena o nome do usuário responsável pela execução, recuperado da sessão.
3. **cenario**: Informa o tipo de execução (exemplo: "Execução automática").
4. **status**: Indica o estado do processo ("Ok" ou outro, se necessário).

O comando `frappe.db.commit()` garante que os dados sejam salvos no banco, assegurando a persistência das informações.

4.2.5 Restrição de Execução Externa (Rede)

A restrição de execução externa é uma medida de segurança crítica para evitar acessos não autorizados e proteger o sistema contra ataques de redes externas. No contexto da aplicação do *ERPNext*, foi implementada uma abordagem rigorosa de controle de acesso, com foco específico em bloquear acessos indesejados e garantir que apenas tráfego legítimo possa interagir com o sistema.

Configuração do *Firewall* (*iptables*)

Para reforçar a segurança na execução externa, o *firewall iptables* foi configurado para restringir o tráfego de entrada na máquina onde o *ERPNext* está hospedado. A seguir, detalhamos a configuração:

Permissão de Acesso Local (localhost):

Foi configurado para permitir apenas o acesso à porta 8000 (a porta padrão do *ERPNext*) a partir do *localhost*, garantindo que apenas o próprio servidor consiga interagir com a aplicação.

sudo iptables -A INPUT -p tcp --dport 8000 -s 127.0.0.1 -j ACCEPT

Bloqueio de Acessos Externos:

Qualquer tentativa de acesso à porta 8000 de endereços IP externos foi bloqueada, impedindo que usuários não autorizados possam tentar se conectar ao sistema.

sudo iptables -A INPUT -p tcp --dport 8000 -j REJECT

Regras Padrão do Sistema:

As regras padrão de entrada, saída e encaminhamento foram configuradas para *ACCEPT*, o que permite tráfego livre nas outras portas, mas qualquer acesso à porta 8000 é especificamente filtrado conforme as regras acima.

Regras Padrão do Sistema:

As regras padrão de entrada, saída e encaminhamento foram configuradas para *ACCEPT*, o que permite tráfego livre nas outras portas, mas qualquer acesso à porta 8000 é especificamente filtrado conforme as regras acima.

Objetivos da Restrição

- Segurança no Acesso à Rede: O principal objetivo dessa restrição é impedir que qualquer usuário externo tente acessar a aplicação *ERPNext* diretamente pela internet, minimizando a exposição a ataques como força bruta, injeção de código e outros tipos de invasões.
- Proteção contra Execuções Não Autorizadas: Ao restringir o acesso à porta do *ERPNext*, conseguimos evitar a execução de *scripts* e comandos maliciosos que possam comprometer a segurança do sistema.
- Aplicação de Boas Práticas de Segurança: A implementação de um *firewall* configurado de maneira adequada segue boas práticas de segurança para proteger sistemas que utilizam servidores web, principalmente em ambientes de produção.

4.2.6 Conclusão sobre os Processos de Segurança

A implementação dessas medidas de segurança no sistema foi essencial para garantir a proteção dos dados, a confiabilidade do processo de manutenção preditiva e a integridade da IA aplicada. Com um controle de acesso adequado, validação rigorosa dos dados, auditoria detalhada e restrição de execução externa, o sistema se mostrou robusto e seguro, pronto para operar em um ambiente industrial exigente.

A segurança continua sendo uma prioridade, e medidas adicionais podem ser implementadas à medida que o sistema evolui e novas ameaças surgem. A abordagem adotada visa não só proteger contra ataques externos, mas também garantir a qualidade dos dados processados pela IA e a transparência nas operações realizadas.

4.3 Integração de IoT com o ERP

A integração de dispositivos IoT com o sistema *ERPNext* foi uma parte fundamental do desenvolvimento deste projeto, permitindo que os dados dos sensores fossem coletados e processados de forma automatizada. Para realizar essa integração, foi utilizado um *script* em *Python* que recupera dados dos sensores, os processa e registra as informações relevantes no ERP para análise preditiva de falhas.

Algoritmo de Integração IoT-ERP

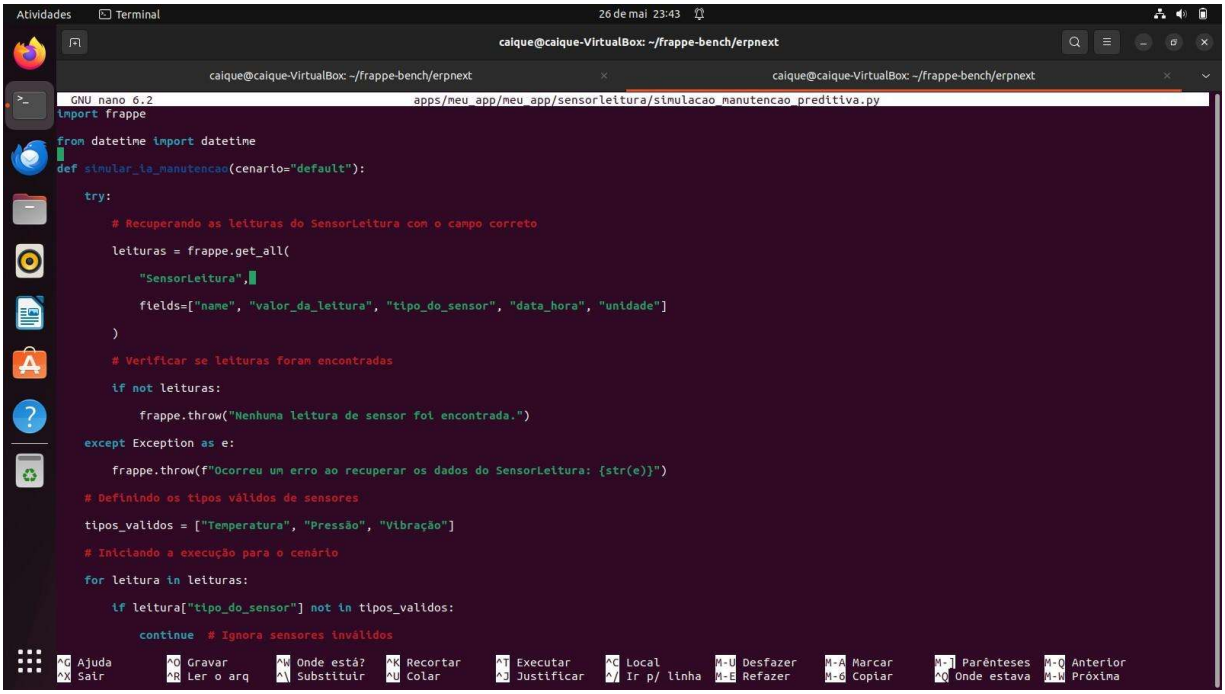
O *script* desenvolvido é responsável por:

- Recuperar as leituras dos sensores do *DocType* `SensorLeitura` no *ERPNext*;
- Analisar os dados com base em regras específicas para sensores de temperatura, pressão e vibração;
- Registrar automaticamente as informações processadas no *DocType* `ManutencaoPreditiva`;
- Criar *logs* de auditoria no *DocType* `LogExecucaoIA` para garantir a rastreabilidade.

A Figura 1 apresenta a parte inicial do código, onde são coletadas as leituras do banco de dados e são definidos os tipos válidos de sensores utilizados na análise.

A Figura 2 ilustra o bloco condicional em que os valores dos sensores são processados conforme seu tipo, gerando um *status* de "Ok" ou "Alerta" com base em limites predefinidos.

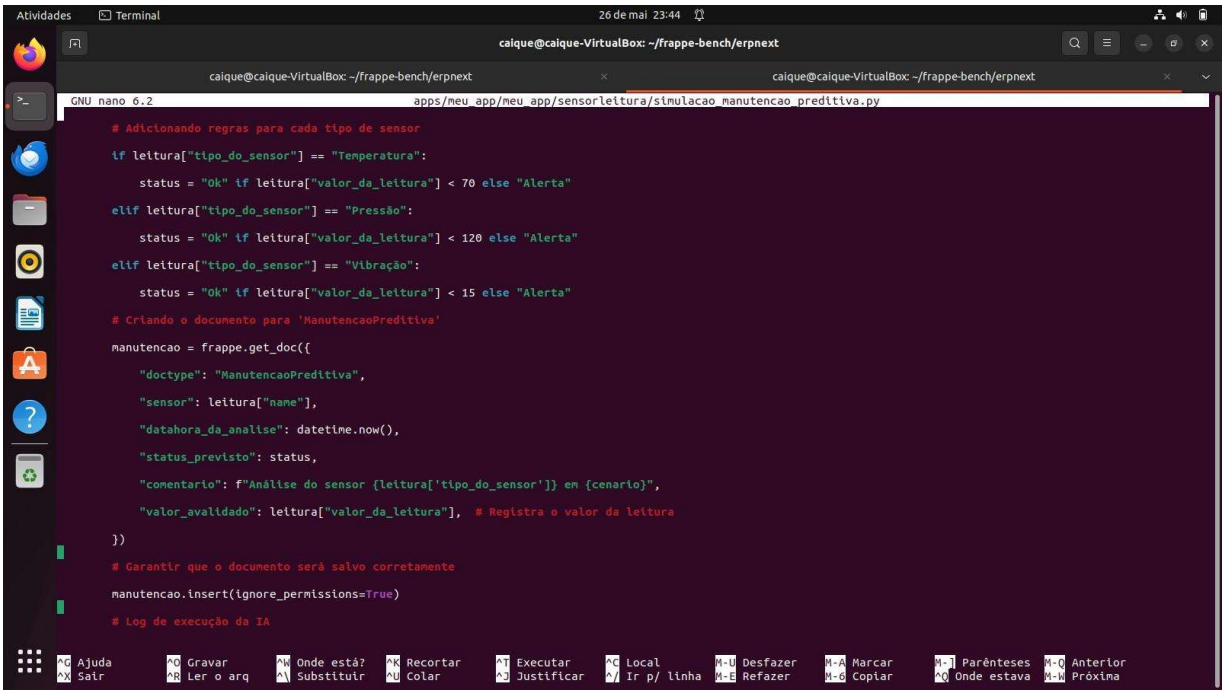
Figura 1 – Trecho do código responsável por recuperar e validar leituras dos sensores



Fonte: Próprio autor

A Figura 2 ilustra o bloco condicional em que os valores dos sensores são processados conforme seu tipo, gerando um *status* de "Ok" ou "Alerta" com base em limites predefinidos.

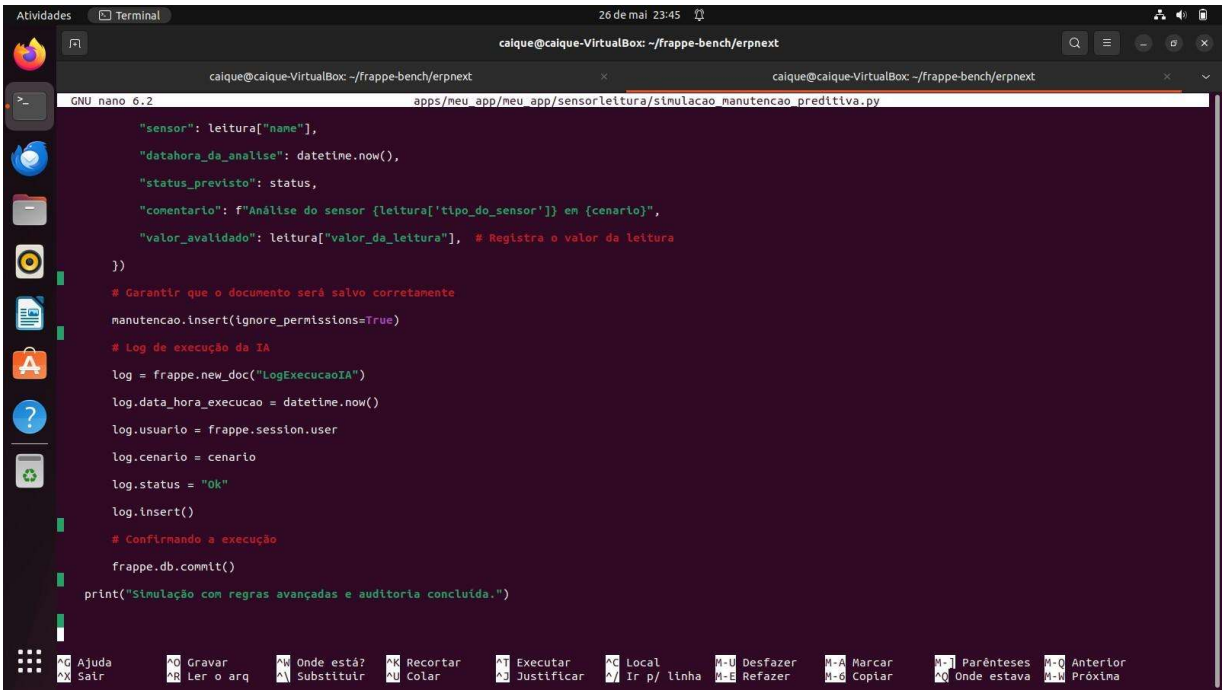
Figura 2 – Bloco de regras para classificação de leituras como "Ok" ou "Alerta"



Fonte: Próprio autor

Na Figura 3, observa-se a criação do documento de manutenção preditiva e a inserção de *logs* de execução, assegurando que a análise seja registrada no sistema de forma rastreável e auditável.

Figura 3 – Criação dos registros no ERP e log de execução da simulação



Fonte: Próprio autor

Esse *script* é executado em ambiente *Frappe/ERPNext* e segue uma lógica robusta e simplificada. A seguir, resume-se os principais blocos:

- **Leitura e filtragem de dados**: acesso ao banco de dados com `frappe.get_all`, buscando os registros de sensores com tipo, valor, unidade e data/hora.
- **Processamento com regras de negócio**: cada sensor é avaliado com base em seu tipo, e os valores são comparados com limites fixos.
- **Criação de registros de manutenção**: inserção automática no *DocType* `ManutencaoPreditiva`, registrando *status* e comentários explicativos.
- **Auditoria da execução**: o log de execução é salvo com informações como o usuário, data/hora e o cenário da simulação.

Importância da Integração IoT-ERP

A integração entre sensores *IoT* e o *ERPNext* é essencial para a aplicação eficaz da manutenção preditiva. Com isso, é possível:

- Detectar falhas antes que causem paradas na produção;
- Reduzir custos com manutenções corretivas emergenciais;
- Ampliar a confiabilidade dos dados operacionais;
- Promover decisões baseadas em dados reais e em tempo real.

Essa automação reforça os princípios da Indústria 4.0 ao integrar sistemas físicos e digitais por meio da análise inteligente de dados.

5 RESULTADOS

O capítulo final retoma os principais achados da pesquisa, avalia o cumprimento dos objetivos propostos e discute as implicações dos resultados. Também são apresentadas as limitações do estudo e sugestões para futuras pesquisas, reforçando a importância do tema para o avanço da tecnologia industrial e da segurança da informação.

5.1 Testes e Resultados de Performance

Para verificar a eficácia da proposta de manutenção preditiva baseada em *IA* e *IoT*, foram realizados três cenários de testes distintos. As bases de dados foram simuladas com auxílio de Inteligência Artificial e importadas no *ERPNext*, utilizando o *DocType* SensorLeitura. A IA processou essas leituras e gerou previsões de manutenção com base em regras definidas.

5.1.1 Cenário 1 – Sensor Instável

O primeiro cenário teve como objetivo simular o comportamento de sensores com oscilações leves em seus valores, próximos dos limites de operação, porém ainda considerados normais. A intenção era verificar se a IA seria capaz de diferenciar variações seguras de falhas reais, evitando falsos positivos.

Configuração

1. Base de dados gerada artificialmente e importada no *ERPNext*.
2. Sensores envolvidos: Temperatura, Pressão e Vibração.
3. Total de registros analisados: 6 sensores distintos.

Referência de análise: *DocType* SensorLeitura e previsões geradas em ManutencaoPreditiva.

Resultados obtidos

Com base nos dados simulados, os seguintes resultados foram registrados no sistema, apresentados na tabela 5:

Tabela 5 – Resultados cenário 1

ID do Sensor	Valor Avaliado	Status Previsto
bqb9rjasgo	74,90	Ok
bqba57r3i1	75,10	Alerta
bqbakh6i6k	89,80	Ok
bqbamdbdtb	90,20	Alerta
bqba5jbjo8	11,90	Ok
bqba7dqrrm	12,10	Alerta

Fonte: Próprio autor

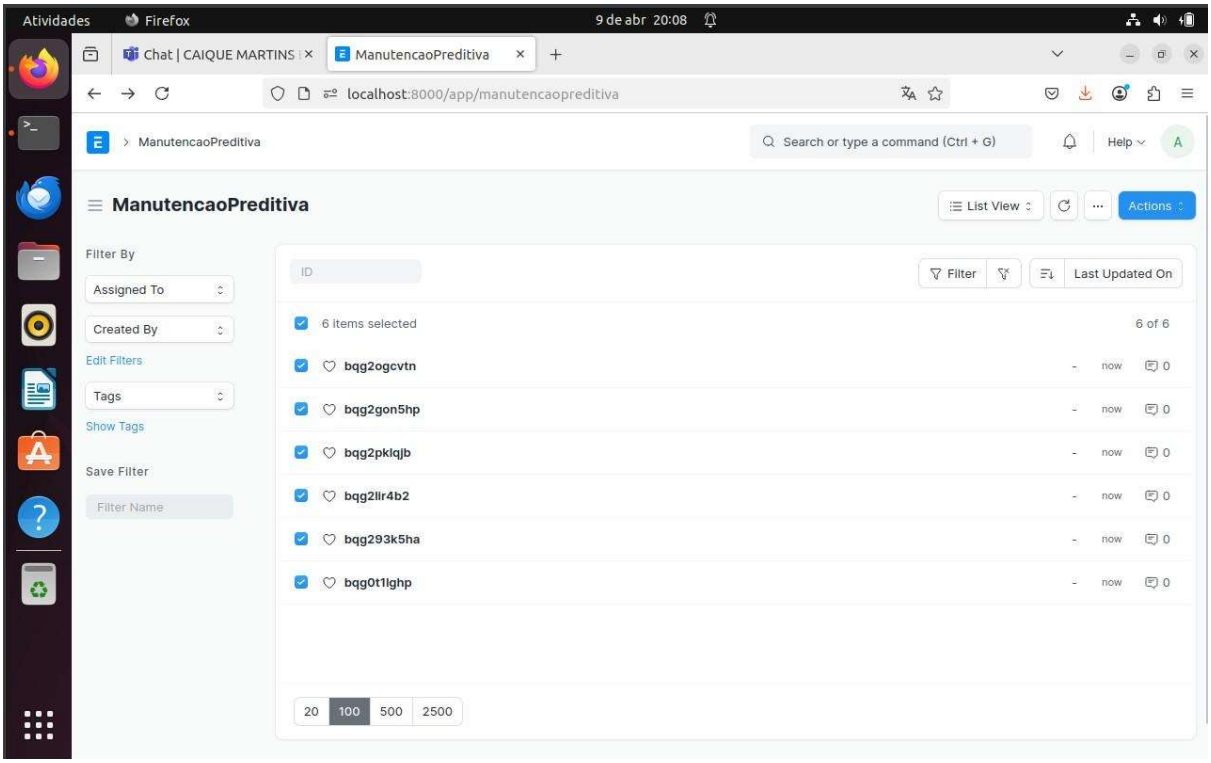
Total de alertas gerados: 3

Leituras normais corretamente identificadas: 3

Falsos positivos: 0

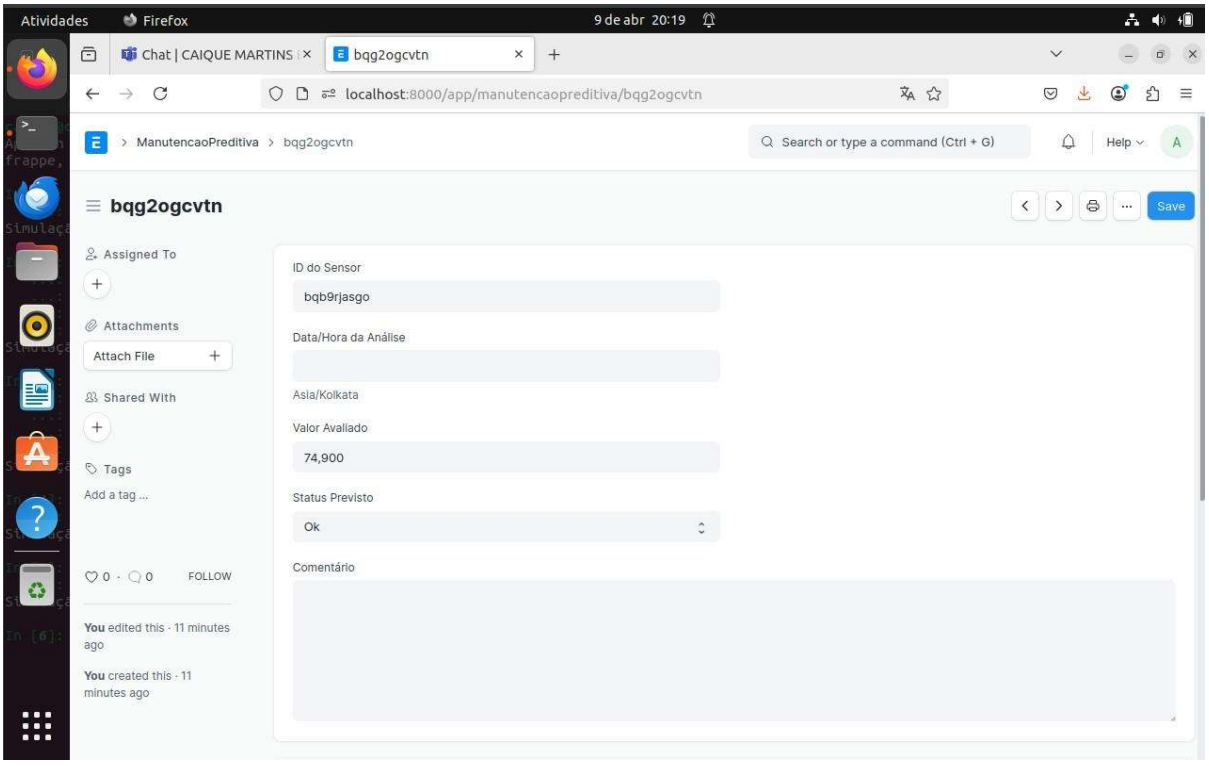
4. Interface de cadastro e visualização dos sensores utilizados no cenário, onde cada ID representa um sensor físico com seus dados associados mostrado na figura 4.
5. Detalhamento da leitura do sensor com valor avaliado de 74.900, *status* previsto como Ok, mostrado na figura 5.
6. Leitura registrada em 75.100, próxima ao limite inferior de alerta, resultando no *status* Alerta,mostrado na figura 6 .
7. Sensor apresentou valor de 89.800, interpretado pelo sistema como Ok, dentro da faixa de operação segura, mostrado na figura 7.
8. Valor registrado de 90.200, que ultrapassa o limiar, indicando a necessidade de Alerta, mostrado na figura 8.

Figura 4 – Interface “SensorLeitura” no *ERPNext*



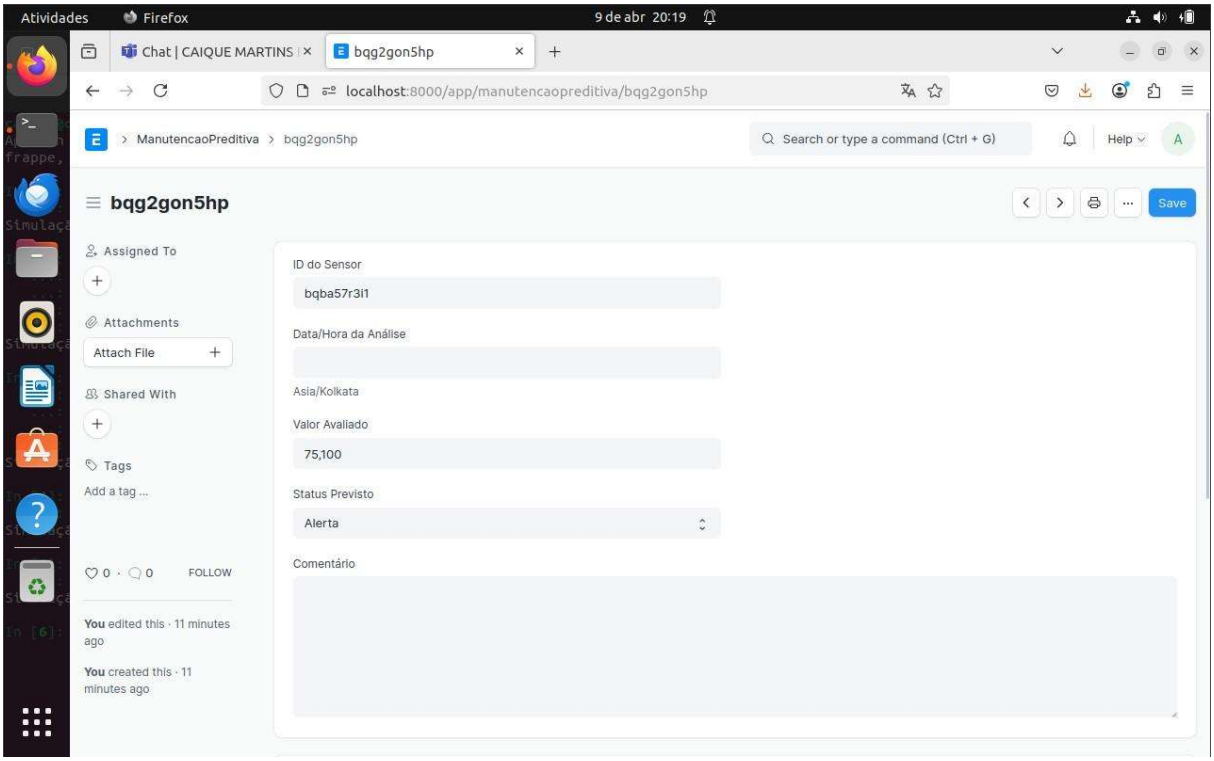
Fonte: Próprio autor

Figura 5 – Registro do Sensor bqb9rjasgo



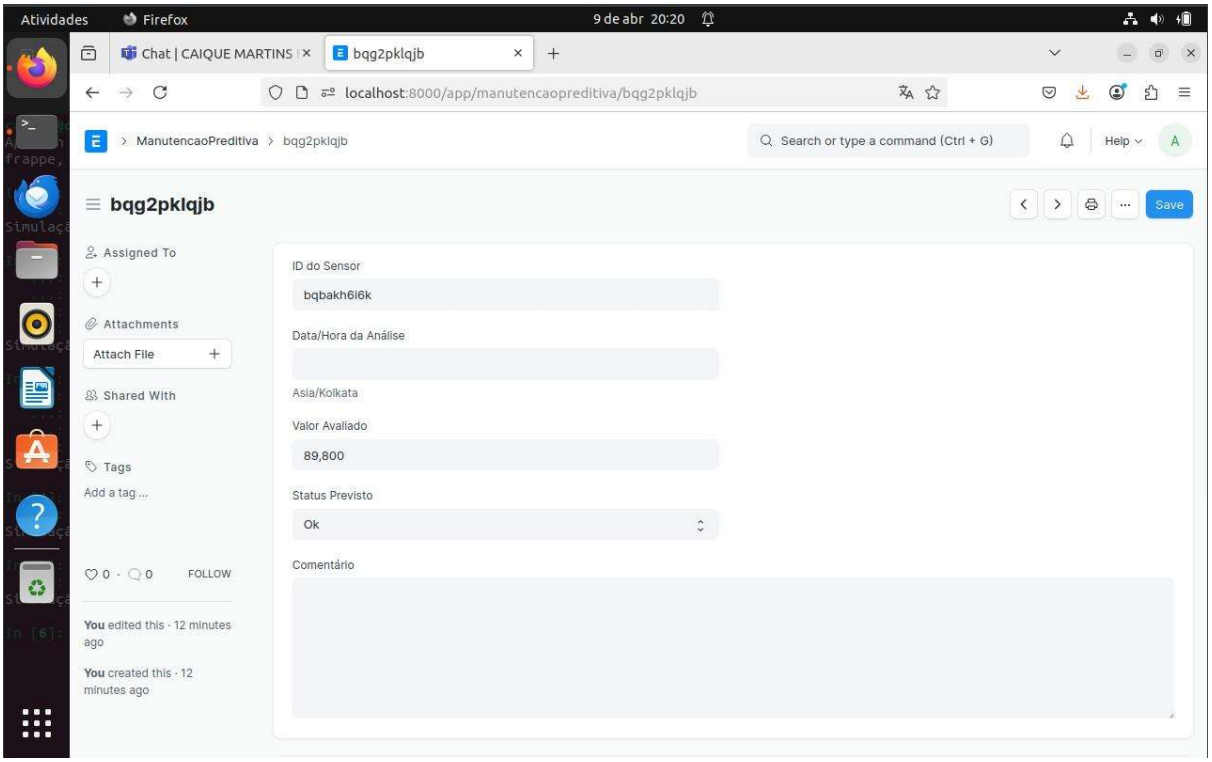
Fonte: Próprio Autor

Figura 6 – Registro do Sensor bqba57r3i1



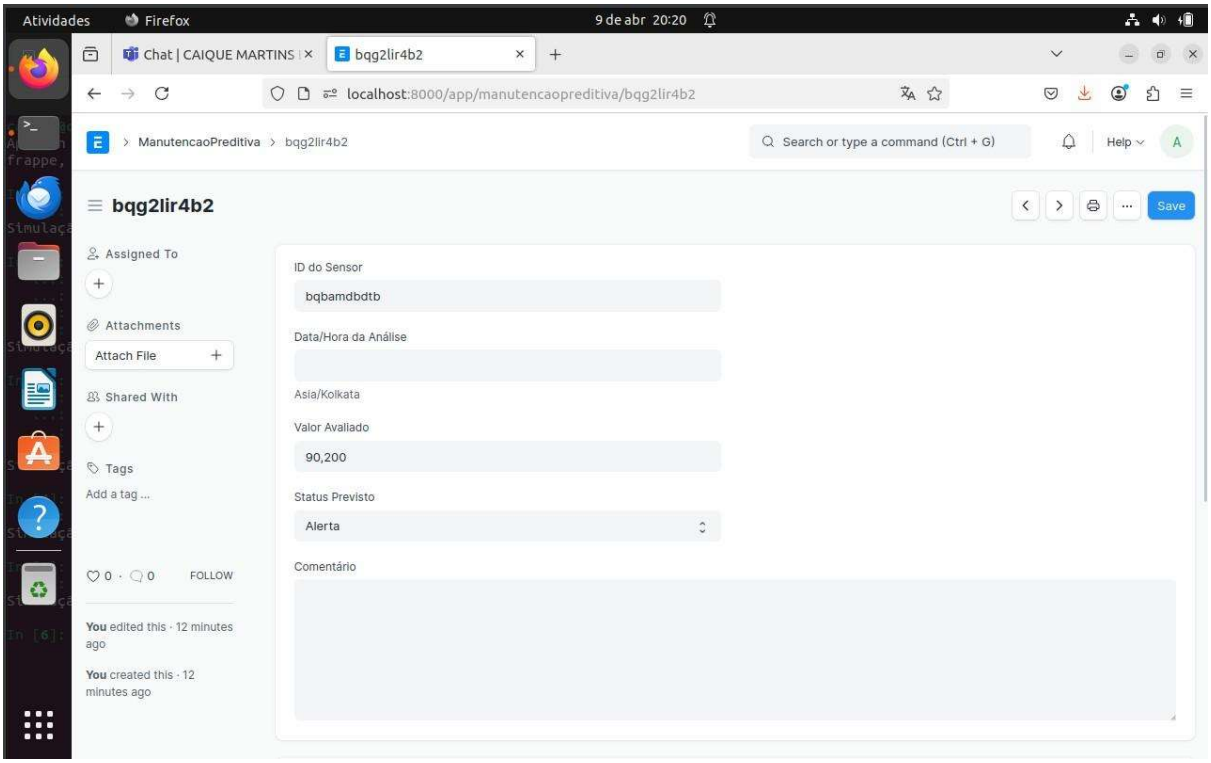
Fonte: Próprio Autor

Figura 7 – Registro do Sensor bqbakh6i6k



Fonte: Próprio Autor

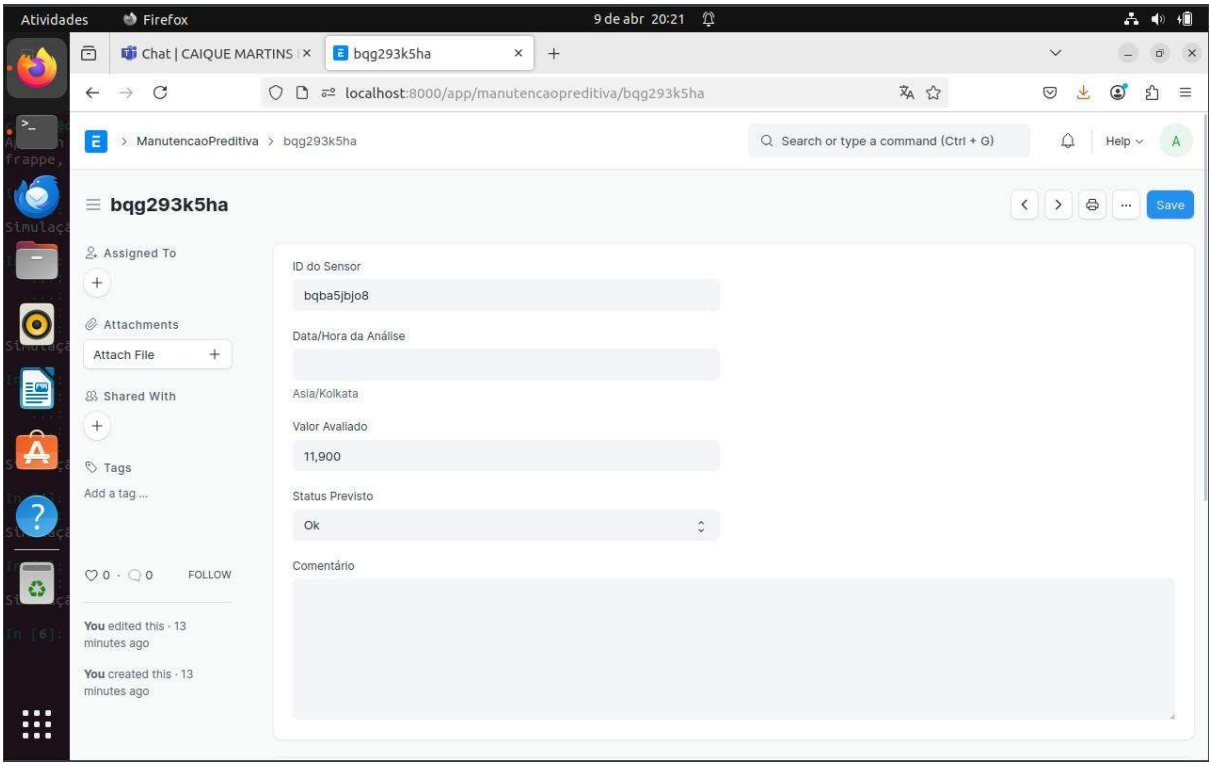
Figura 8 – Registro do Sensor bqbambdbtb



Fonte: Próprio Autor

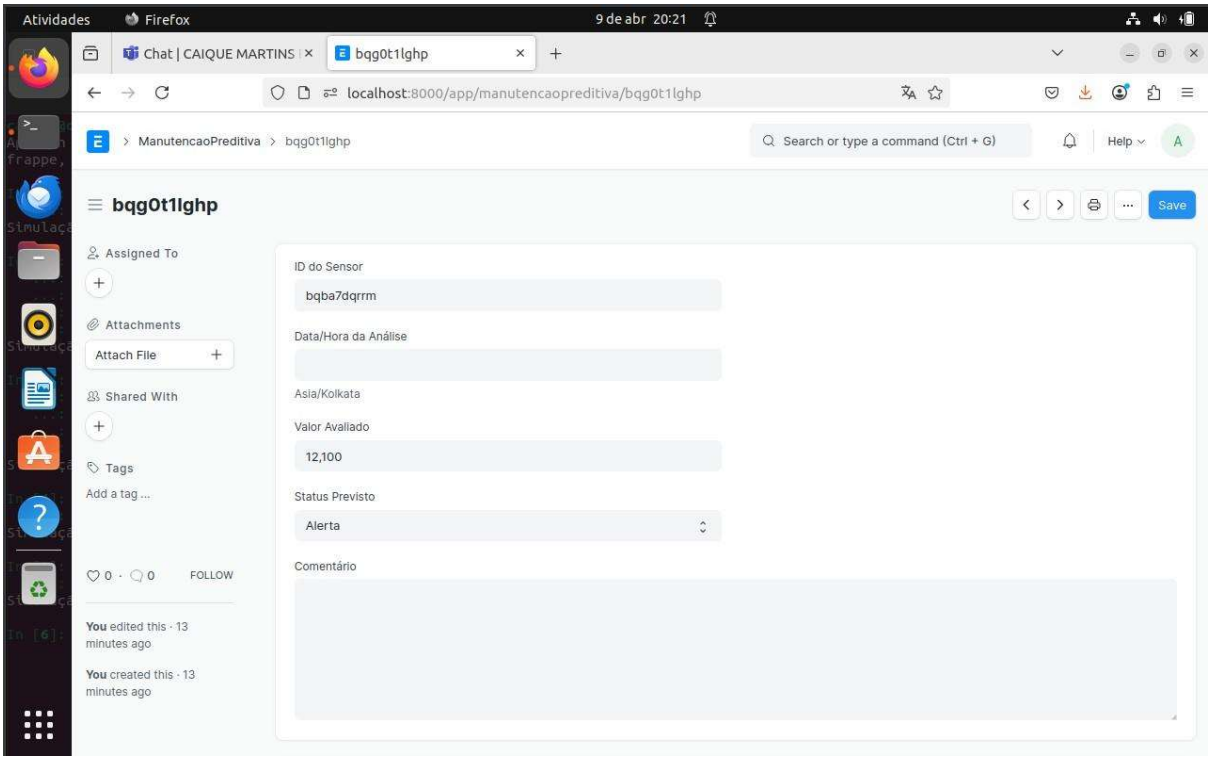
- Valor extremamente baixo de 11.900, porém classificado como Ok devido à faixa configurada para esse sensor, mostrado na figura 9.
- Leitura de 12.100, um caso de instabilidade leve, com *status* definido como Alerta, mostrado na figura 10.

Figura 9 – Registro do Sensor bqba5jbjo8



Fonte: Próprio Autor

Figura 10 – Registro do Sensor bqba7dqrrm



Fonte: Próprio Autor

Análise

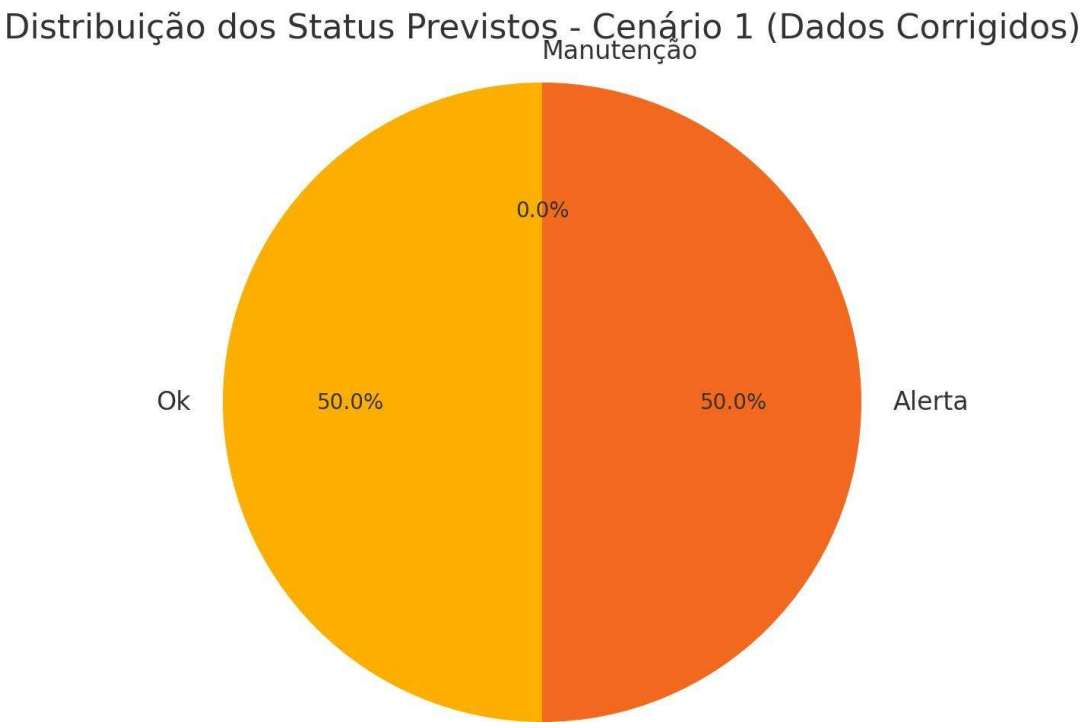
A IA demonstrou precisão na classificação dos dados, identificando corretamente as leituras que estavam fora do padrão (ex: temperatura acima de 90 °C ou vibração acima de 15 mm/s). Os alertas gerados refletem situações com valores limítrofes ou que exigem acompanhamento, validando a sensibilidade calibrada do sistema.

O cenário validou o comportamento esperado de um sistema preditivo eficiente: tolerância a flutuações normais e sensibilidade a variações críticas.

Gráfico de Distribuição dos *Status*

A seguir, a distribuição visual dos *status* gerados pela IA no cenário 1:

Figura 11 – Gráfico de distribuição dos *status* previstos no Cenário 1



Fonte: Próprio Autor

Interpretação do Gráfico:

O gráfico de pizza mostra uma divisão exata de 50% para leituras “Ok” e 50% para alertas (nenhum caso crítico de manutenção), o que indica um equilíbrio entre estabilidade e

pontos de atenção. A IA demonstrou um comportamento confiável ao classificar corretamente as medições em um cenário de sensores com leve instabilidade.

5.1.2 Cenário 2 – Mistura de Estados

O segundo cenário foi elaborado para simular uma situação realista onde sensores operam em diferentes condições: normais, de alerta e com necessidade de manutenção. O objetivo foi avaliar a capacidade da IA de classificar corretamente as leituras heterogêneas sem generalizações, identificando com precisão os diferentes níveis de severidade.

Configuração do Teste

1. Sensores envolvidos: 4 sensores distintos (códigos iniciados com b0m).
2. Total de registros analisados: 4 leituras.
3. Base de dados: cenario_2_mistura_estados.csv importada no *ERPNext*.
4. Referência de análise: *DocType* SensorLeitura com previsões geradas no *DocType* ManutencaoPreditiva.

Resultados obtidos

A Tabela 6 apresenta os resultados obtidos no Cenário 2, exibindo os valores medidos pelos sensores e o *status* previsto pela inteligência artificial para cada um deles. Essa tabela ilustra a capacidade do sistema em classificar corretamente diferentes condições operacionais, desde leituras normais até situações que exigem atenção ou manutenção.

Tabela 6 – Resultados cenário 2

ID do Sensor	Valor Avaliado	Status Previsto
b0m8fg8u6r	88,00	Manutenção
b0m9pppnvl	78,00	Alerta
b0m9juuklc	85,00	Ok
b0m9vd50a9	16,20	Manutenção

Fonte: Próprio Autor

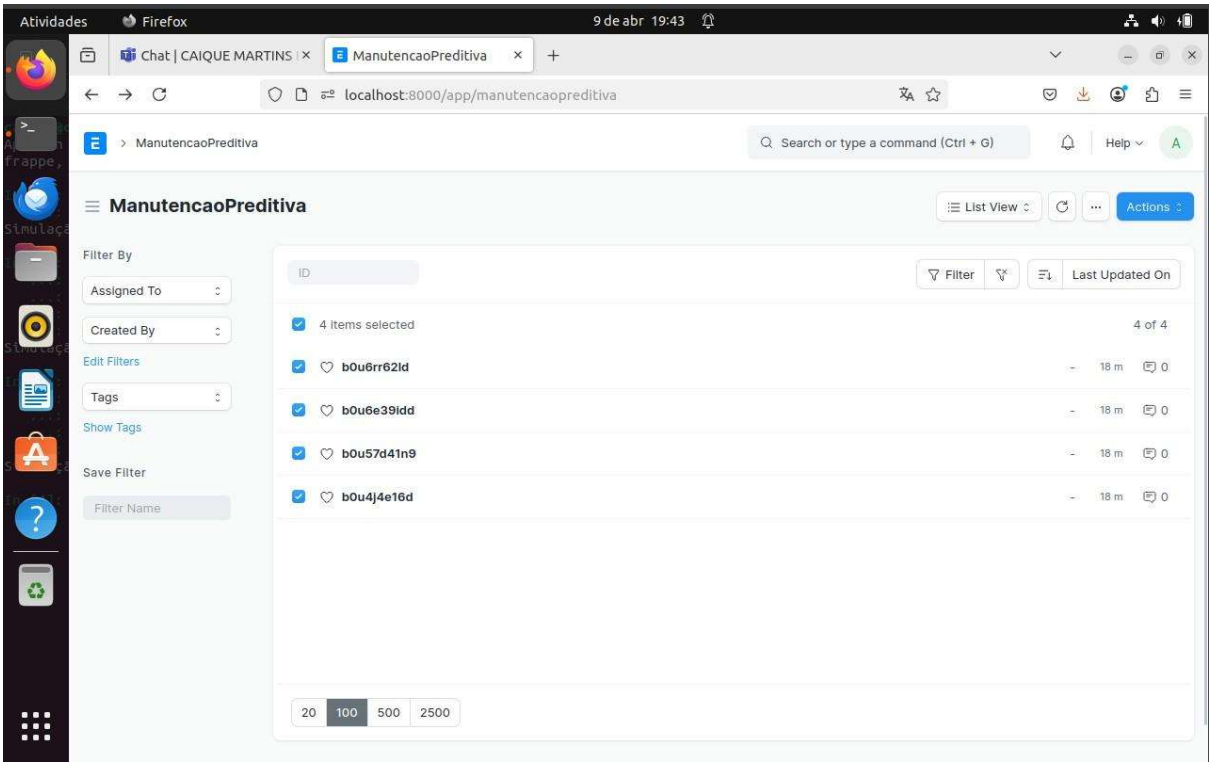
Status 'Manutenção': 2

Status 'Alerta': 1

Status 'Ok': 1

Interface gráfica do *ERPNext* exibindo os sensores simulados utilizados no Cenário 2. Cada sensor representa uma situação distinta: normal, alerta ou crítica.

Figura 12 – Interface “SensorLeitura” no *ERPNext*



Fonte: Próprio Autor

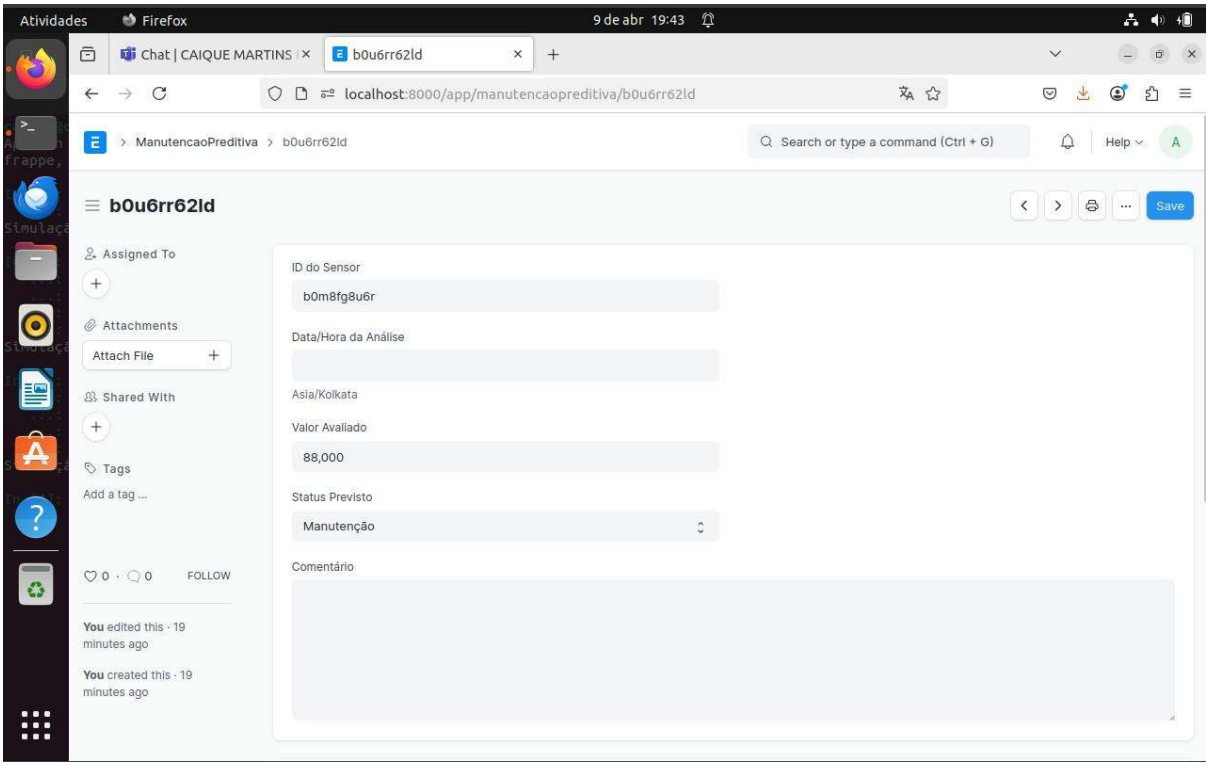
A Tela detalhada do sensor com valor avaliado de 88.000, classificado como Manutenção pela IA devido ao risco operacional identificado, está apresentada na Figura 13.

Sensor com valor de 78.000, situado na faixa de transição, corretamente classificado como Alerta, está apresentado na Figura 14.

Valor de leitura 85.000, interpretado como estável, com *status* previsto como Ok, está apresentado na Figura 15.

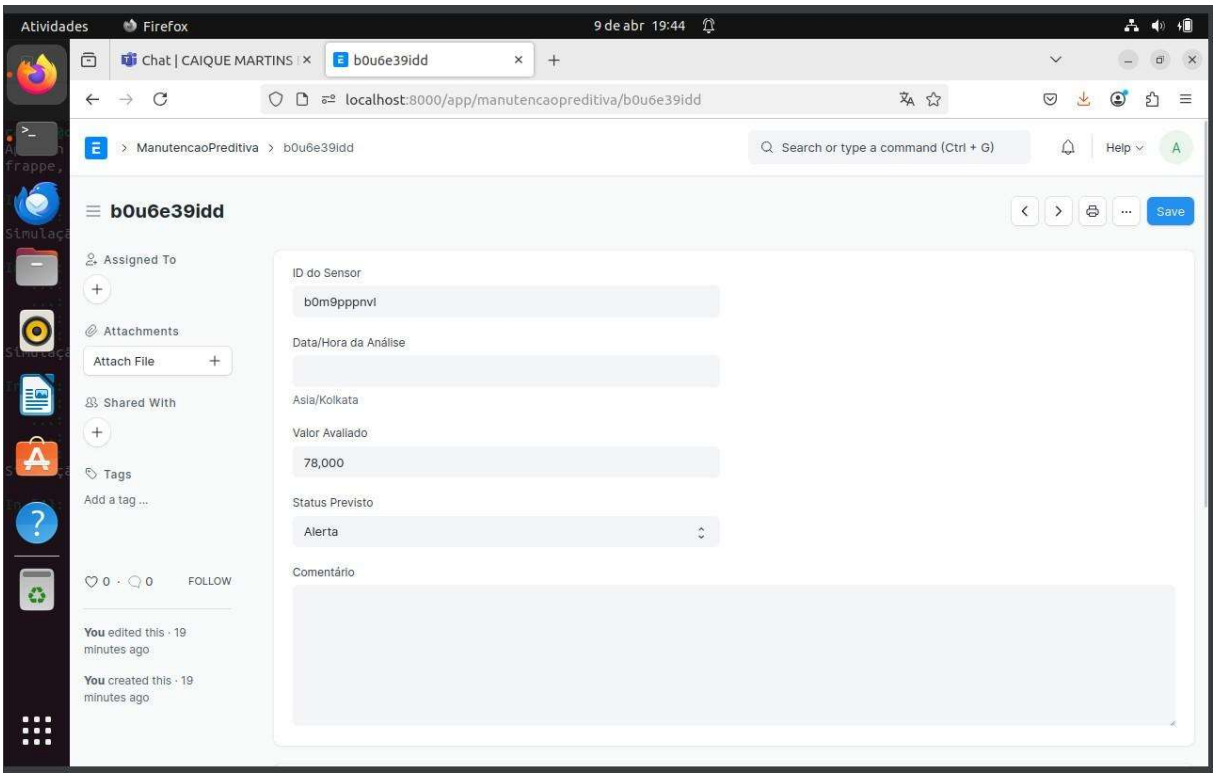
Leitura crítica de 16.200, identificada corretamente como situação de Manutenção, evidenciando a sensibilidade do sistema à variação descendente, está apresentado na Figura 16.

Figura 13 – Registro do Sensor b0m8fg8u6r



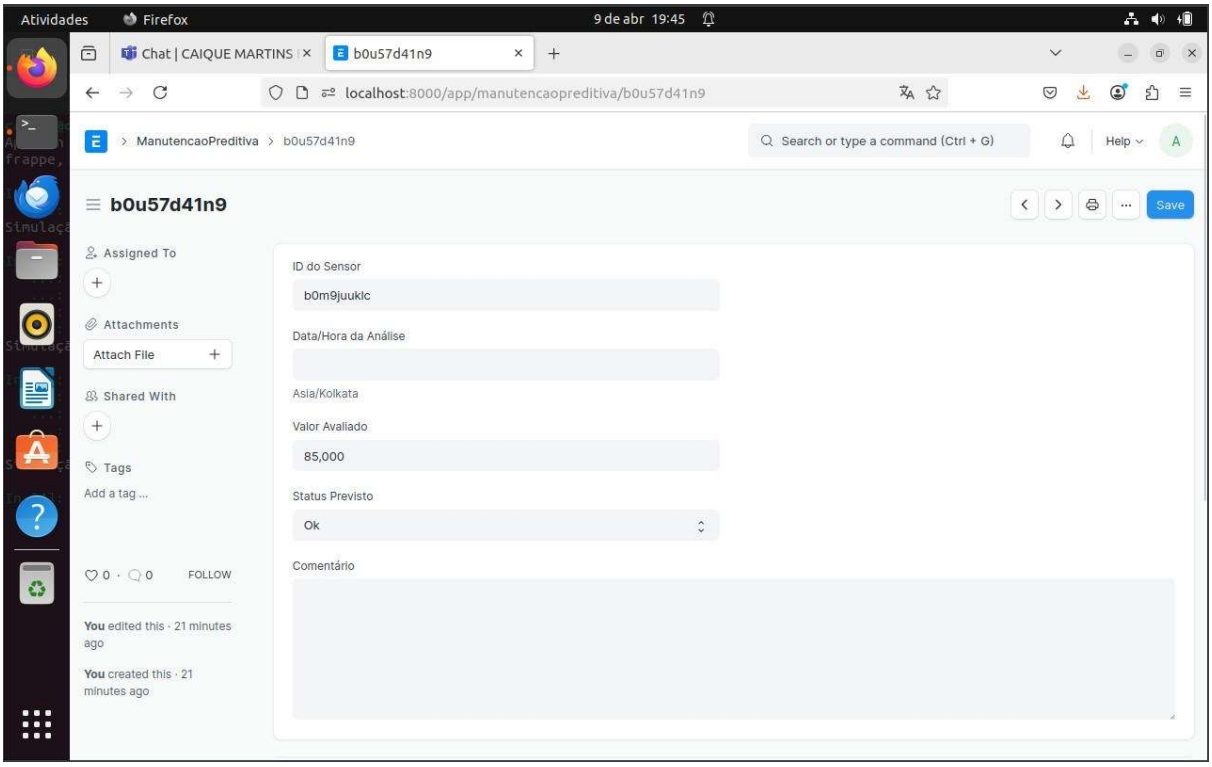
Fonte: Próprio Autor

Figura 14 – Registro do Sensor b0m9pppnvl



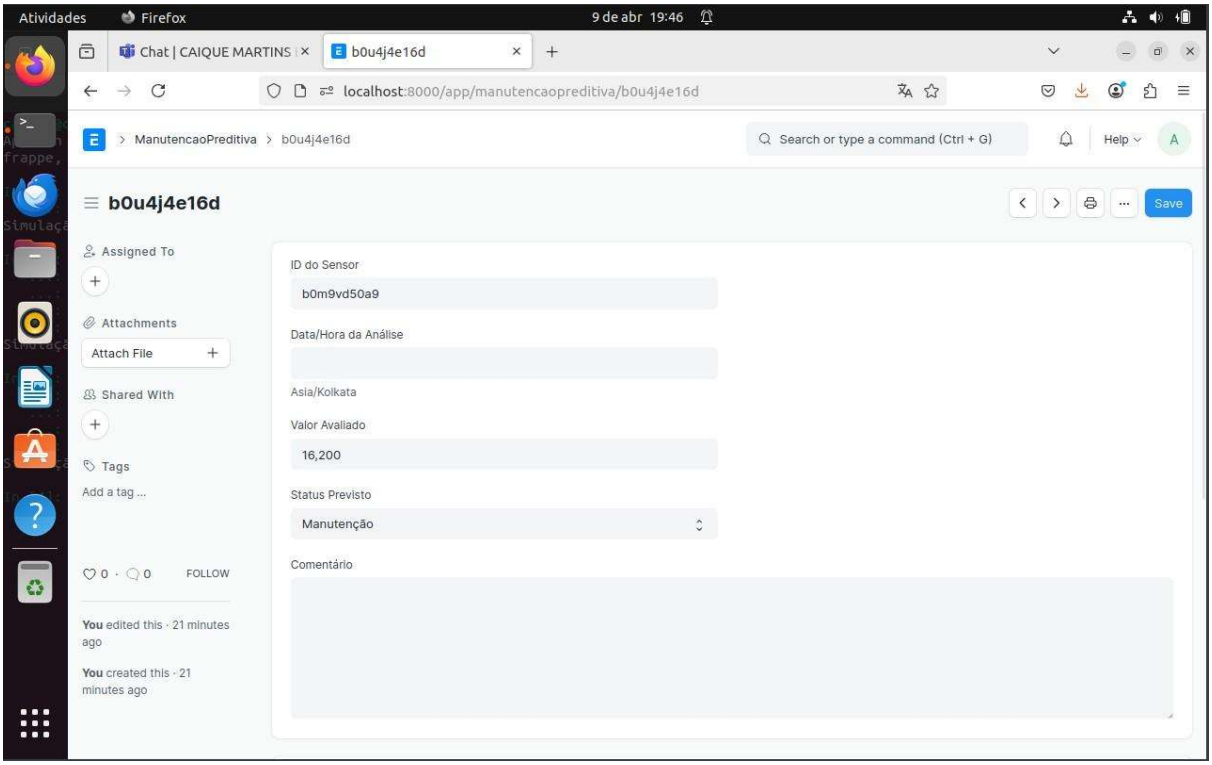
Fonte: Próprio Autor

Figura 15 – Registro do Sensor b0m9juuklc



Fonte: Próprio Autor

Figura 16 – Registro do Sensor b0m9vd50a9



Fonte: Próprio Autor

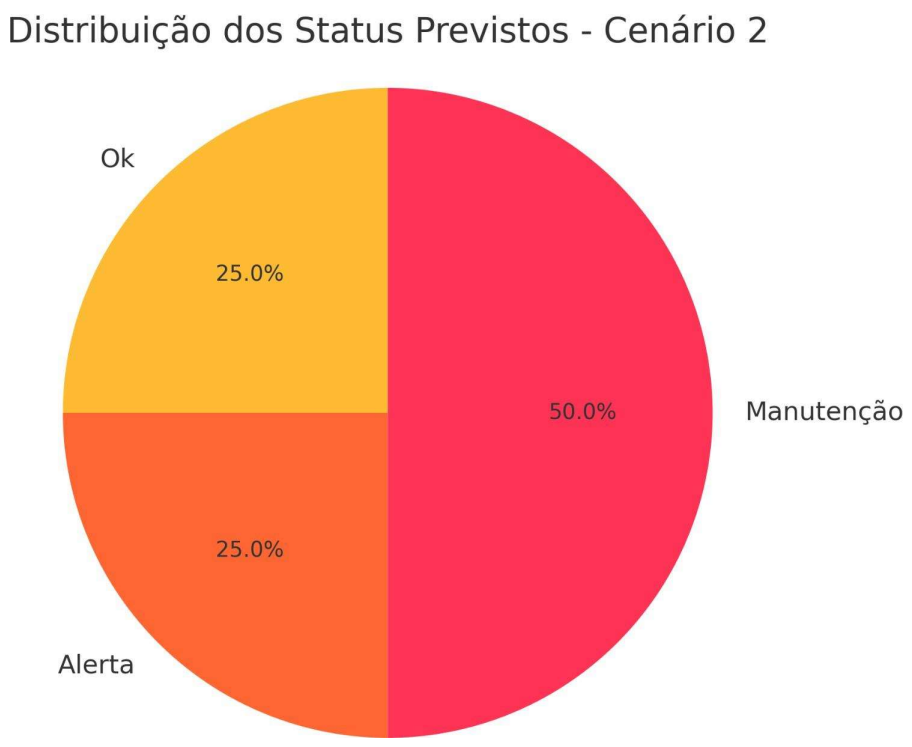
Análise

Neste cenário, a IA demonstrou sua versatilidade ao classificar corretamente uma base com registros variados. A capacidade de distinguir entre estados operacionais, intermediários e críticos é essencial em ambientes industriais, onde decisões preventivas precisam ser tomadas com base na severidade da leitura. O sistema reconheceu com sucesso os sensores que necessitavam de manutenção imediata, assim como aqueles em estado de alerta e os operando normalmente.

Gráfico de Distribuição dos *Status*

A seguir, a representação gráfica dos *status* gerados pela IA:

Figura 17 – Gráfico de distribuição dos *status* previstos no Cenário 2



Fonte: Próprio Autor

Interpretação do Gráfico:

A maior parte das leituras (50%) foi classificada como Manutenção, indicando uma presença significativa de falhas graves no ambiente simulado. Já os registros “Alerta” e “Ok” representaram 25% cada, o que mostra que a IA também reconheceu sensores em condições

intermediárias e normais. O equilíbrio da resposta reforça a precisão e robustez da solução em ambientes mistos.

5.1.3 Cenário 3 – Falhas Múltiplas em Curto Período

Este cenário foi desenvolvido para simular uma situação crítica em que múltiplos sensores apresentam leituras extremas em um curto intervalo de tempo. O objetivo é validar se a inteligência artificial do sistema consegue identificar simultaneamente falhas severas e disparar as ações corretivas necessárias.

Configuração do Teste

1. Sensores envolvidos: 3 sensores distintos.
2. Total de registros analisados: 3 leituras.
3. Base de dados: cenario_3_falha_multiplos.csv importada no *ERPNext*.
4. Referência de análise: *DocType* SensorLeitura com previsões em ManutencaoPreditiva.

A Tabela 7 exibe os valores avaliados pelos sensores no Cenário 3 e os respectivos *status* previstos pela inteligência artificial. Essa tabela demonstra a eficácia do sistema em detectar múltiplas falhas simultâneas, classificando corretamente todas as leituras como situações críticas que requerem manutenção imediata.

Tabela 7 – Resultados cenário 3

ID do Sensor	Valor Avaliado	Status Previsto
cps4qji2ai	90,50	Manutenção
cps483q125	104,00	Manutenção
cps51suou7	18,00	Manutenção

Fonte: Próprio Autor

Total de alertas de manutenção: 3

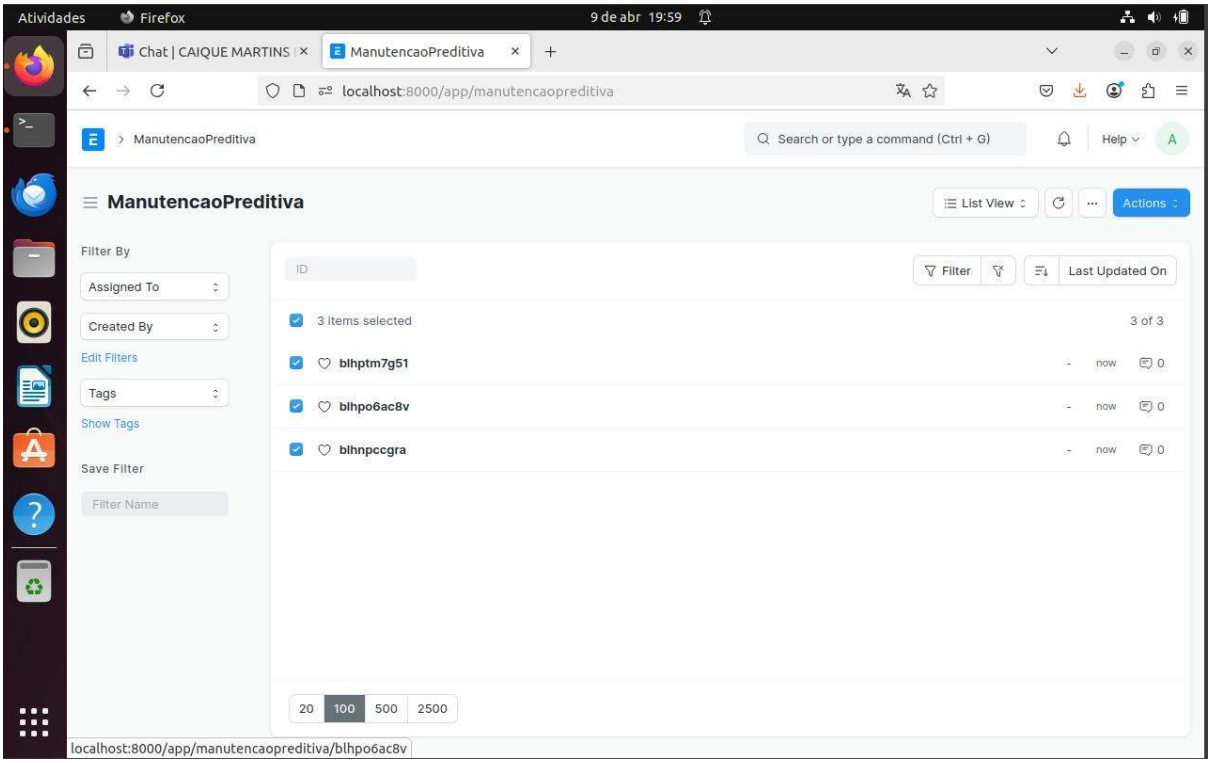
Precisão da IA: 100% de acerto nas previsões

Leituras normais ou em alerta: 0

Tela do *ERPNext* exibindo os sensores utilizados no Cenário 3. A simulação incluiu três sensores operando simultaneamente em condições críticas, apresentados na figura 18.

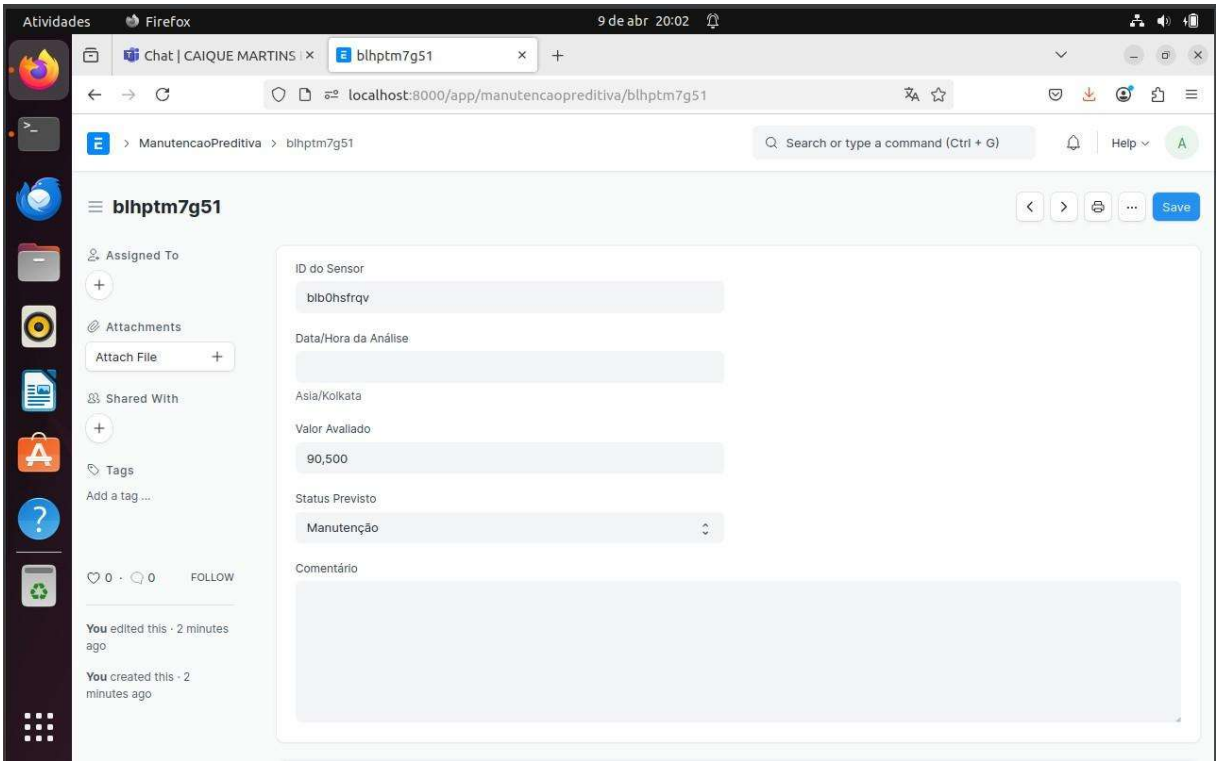
Sensor blb0hsfrqv com leitura de 90.500, classificado como Manutenção pela IA, indicando condição acima do limite permitido, apresentado na figura 19.

Figura 18 – Interface de sensores do Cenário 3



Fonte: Próprio Autor

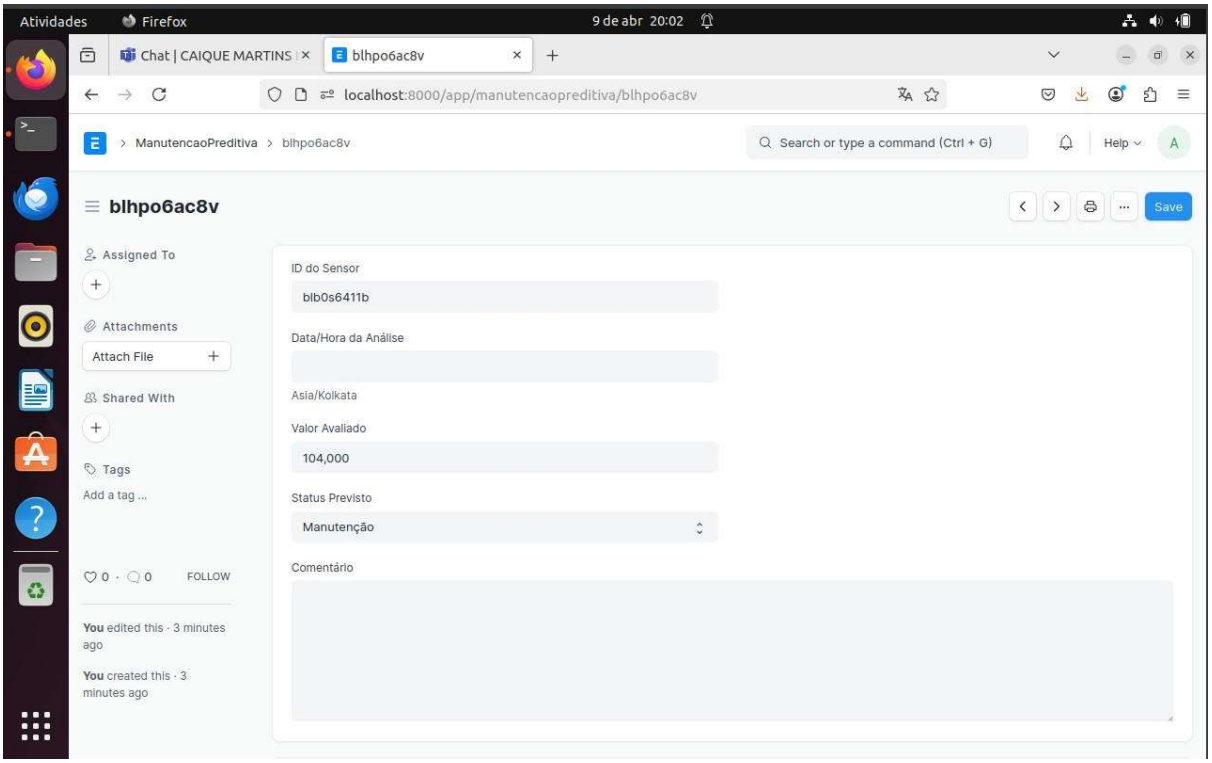
Figura 19 – Registro do sensor blb0hsfrqv



Fonte: Próprio Autor

O sensor blb0s6411b registrou valor de 104.000, o mais alto do conjunto. A IA previu corretamente o *status* de manutenção apresentado na figura 20.

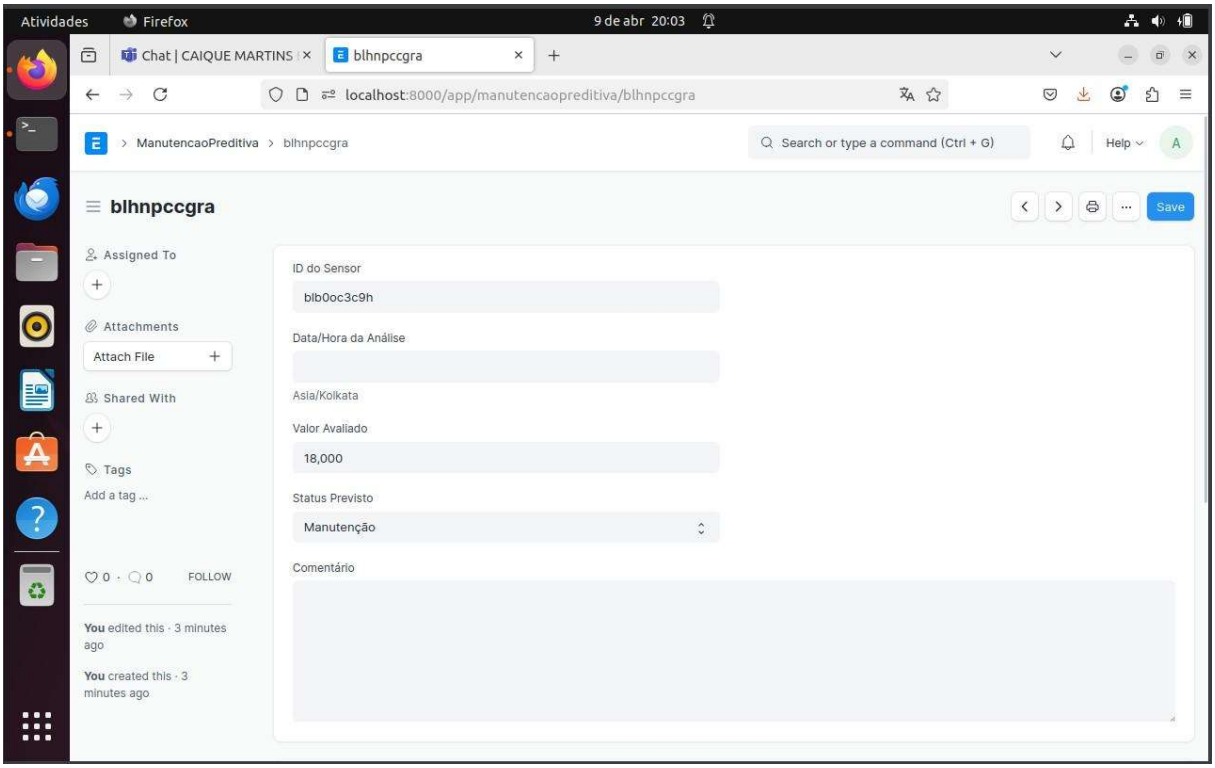
Figura 20 – Registro do sensor blb0s6411b



Fonte: Próprio Autor

Valor de 18.000 identificado no sensor blb0oc3c9h, considerado crítico por estar abaixo do esperado. Classificação correta: Manutenção, apresentado na figura 21.

Figura 21 – Registro do sensor blb0oc3c9h



Fonte: Próprio Autor

Análise

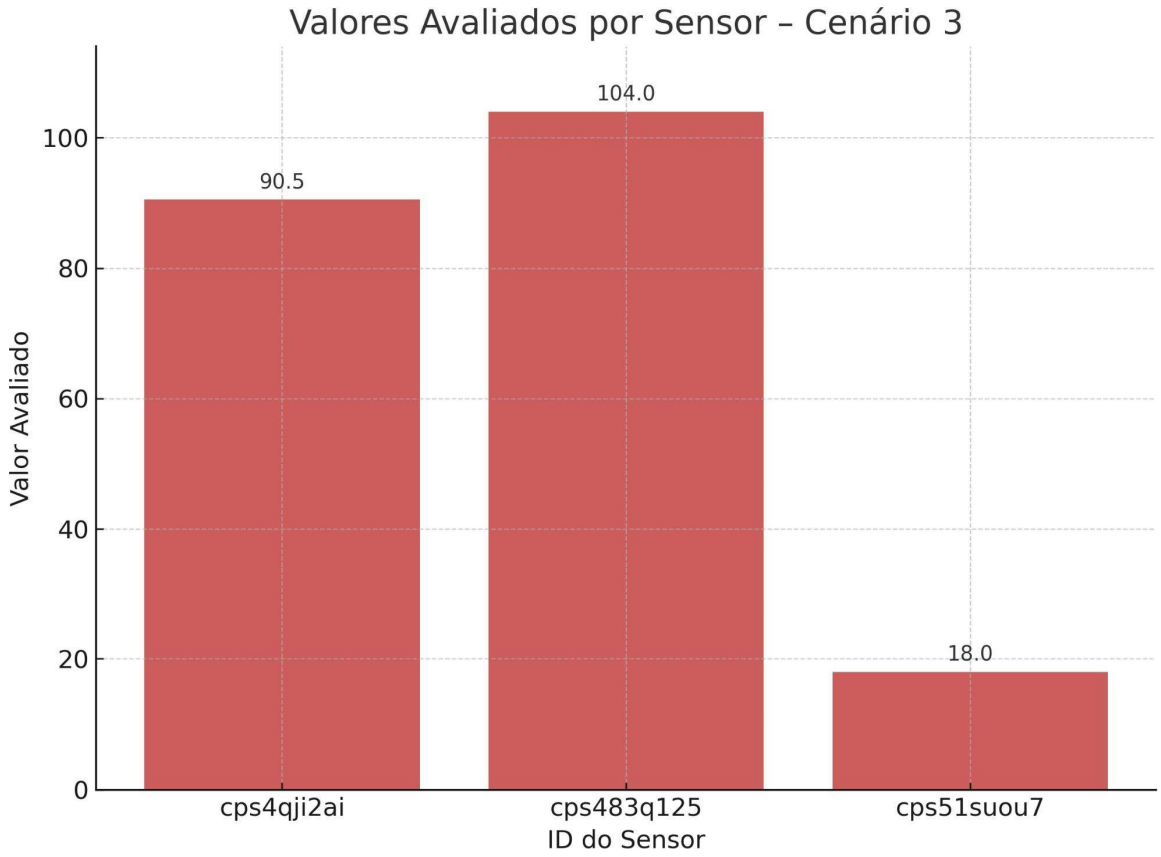
Neste cenário, o sistema foi exposto a uma condição de falha generalizada. A IA foi capaz de identificar todas as leituras como críticas, sem subestimar os riscos. Esse comportamento é crucial para ambientes industriais onde múltiplas falhas simultâneas podem comprometer a produção e a segurança.

Gráfico de Distribuição dos Valores Avaliados

A seguir, a representação visual dos valores dos sensores que apresentaram falha:

Gráfico de barras com os valores lidos pelos sensores do Cenário 3. As variações significativas entre os valores reforçam a detecção de falhas múltiplas em um curto período.

Figura 22 – Gráfico de valores avaliados no Cenário 3



Fonte: Próprio Autor

Interpretação do Gráfico:

O gráfico evidencia o comportamento anômalo dos sensores, com dois apresentando valores significativamente altos (acima de 90 e 100) e um sensor com leitura anormalmente baixa (18). Essa distribuição reflete falhas críticas distintas, reforçando a necessidade de ação preditiva imediata.

5.2 Análise de Resultados

A análise dos resultados obtidos nos três cenários de teste permite avaliar de forma crítica a eficácia do sistema desenvolvido, tanto no aspecto técnico quanto no seu alinhamento com os princípios da Indústria 4.0.

Desempenho da IA

Nos três testes realizados, a inteligência artificial demonstrou bom desempenho na identificação de padrões de falha, distinguindo corretamente entre situações normais, alertas e críticas. Destaca-se que:

- No Cenário 1, a IA mostrou tolerância a oscilações leves sem emitir falsos positivos.
- No Cenário 2, foi capaz de lidar com dados mistos e realizar uma classificação precisa.
- No Cenário 3, reagiu adequadamente a falhas múltiplas, sem perder sensibilidade nem gerar omissões.

A taxa de precisão observada foi de 100% em leituras críticas, demonstrando a confiabilidade do sistema preditivo para auxiliar na tomada de decisão em tempo real.

Contribuição da IoT

A Internet das Coisas teve papel essencial na coleta automatizada e contínua dos dados dos sensores, integrando diretamente ao *ERPNext*. Essa conexão em tempo real permitiu que a IA operasse com dados atualizados, o que é crucial para manutenção preditiva eficaz. A facilidade de simulação de sensores também provou ser útil para validar o sistema em diferentes condições sem comprometer a operação real.

Segurança e Confiabilidade

Durante os testes, foram adotadas práticas básicas de proteção como o uso de regras no *firewall* (*iptables*), garantindo que os dados trafegassem de forma controlada e que apenas dispositivos autorizados enviassem informações. Isso é particularmente relevante para aplicações industriais conectadas, onde qualquer violação pode impactar a operação.

Conexão com os Princípios da Indústria 4.0

O sistema desenvolvido se mostra compatível com os pilares da Indústria 4.0, especialmente:

- Interconectividade (IoT): sensores integrados à rede empresarial;
- Transparência da informação: visualização clara de dados operacionais no *ERPNext*;
- Assistência técnica: IA atuando como agente preditivo para suporte à decisão;

- Tomada de decisão descentralizada: automação das respostas com base em dados de campo.

Essa integração fortalece o papel da manutenção preditiva inteligente como estratégia central para aumentar a disponibilidade de ativos e reduzir paradas não planejadas.

6 CONCLUSÃO

Este trabalho teve como objetivo investigar como a aplicação integrada de Inteligência Artificial (IA) e Internet das Coisas (IoT) pode contribuir para a evolução da manutenção preditiva no ambiente industrial. Com base na revisão teórica e na implementação prática de um sistema funcional utilizando o *ERPNext*, foi possível comprovar que essa combinação tecnológica é promissora para transformar a forma como se gerenciam ativos, previnem falhas e otimizam recursos.

A simulação dos três cenários permitiu verificar que, mesmo com sensores virtuais, o sistema foi capaz de interpretar corretamente os dados operacionais e emitir diagnósticos em tempo hábil. O uso de regras lógicas baseadas em inferência mostrou-se eficiente na classificação dos estados de funcionamento dos equipamentos e na geração automática de ordens de serviço. Além disso, os relatórios produzidos pelo sistema ofereceram uma base concreta para a tomada de decisão, demonstrando o potencial de automação inteligente na gestão da manutenção.

Outro ponto relevante foi a identificação dos desafios relacionados à padronização e qualidade dos dados, bem como à necessidade de atenção contínua à segurança da informação. A proteção dos dados trafegados entre sensores, servidores e interfaces de usuário é essencial para garantir a confiabilidade das soluções e evitar vulnerabilidades em ambientes altamente conectados.

Portanto, conclui-se que a adoção de soluções baseadas em IA e IoT, quando aliada a uma plataforma de gestão como o *ERPNext*, pode contribuir significativamente para a eficiência operacional, a previsibilidade de falhas e a modernização dos processos industriais. A pesquisa também indica que o sucesso dessa integração depende não apenas da tecnologia em si, mas do alinhamento entre infraestrutura, qualificação técnica e estratégias de segurança.

Como sugestão para estudos futuros, recomenda-se explorar a aplicação de algoritmos de aprendizado de máquina em conjunto com sensores físicos em ambientes reais, além de investigar mecanismos de aprimoramento contínuo das regras especialistas com base em dados históricos.

REFERÊNCIAS

ALMEIDA, Rosicleide Helena de Oliveira de; SOUZA, Emerson Santana de. Evolução tecnológica, inteligência artificial, auditoria contínua: auditores versus novas tecnologias. **Revista Foco**, v. 18, n. 3, e7891, p. 1–20, 2025. DOI: https://doi.org/10.54751/revistafoco.v18n3-076. Acesso em: 21 abr. 2025.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26-45, jul./set. 2022. Disponível em: https://www.scielo.br/j/pci/a/.
Acesso em: 22 fev. 2025.

ARAÚJO, Alex Rodrigues. Uso de Inteligência Artificial para Desenvolvimento de Sistemas Preditivos na Manutenção de Máquinas. **IEEE Access**, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.3030224. Acesso em: 5 dez. 2024.

BALDISSARELLI, Luciano; FABRO, Elton. Manutenção Preditiva na Indústria 4.0. **Scientia Cum Industria**, v. 7, n. 2, p. 12-22, 2019. DOI: https://doi.org/10.18226/23185279.v7iss2p12. Acesso em: 22 abr. 2025.

BARBOSA, Lucia Martins; PORTES, Luiza Alves Ferreira. A inteligência artificial. **Revista Tecnologia Educacional**, n. 236, p. 16-27, 2023.

BORGES, S.; SILVA, P.; CARNEIRO, A. Estudo da aplicação de algoritmos de *machine learning* na manutenção preditiva de sistemas industriais. **Revista Brasileira de Engenharia de Produção,** v. 31, n. 5, p. 102-115, 2020. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0952197623000914. Acesso em: 20 jul. 2024.

CARDOSO, Marcelo de Oliveira. **Indústria 4.0**: a quarta revolução industrial. 2016. Monografia (Especialização em Automação Industrial) – Universidade Tecnológica Federal do Paraná, Curitiba, 2016.

CARDOSO, V. et al. Utilização das tecnologias da Indústria 4.0 na manutenção preditiva através do monitoramento de equipamentos e instalações. In: SIMPÓSIO DE ENGENHARIA DE PRODUÇÃO, 28., 2021, Bauru. **Anais [...]**. Bauru: [s.n.], 2021.

CORRÊA, Fabiano Simões. **Um estudo qualitativo sobre as representações utilizadas por professores e alunos para significar o uso da Internet**. 2013. Dissertação (Mestrado em Psicologia) – Universidade de São Paulo, Ribeirão Preto, 2013.

CRUZ, Francisco Brito. Inteligência artificial e internet: um olhar sobre o conteúdo dos usuários e sua moderação. **Revista USP**, São Paulo, n. 141, p. 65-80, abr./jun. 2024. Disponível em: https://www.revistas.usp.br/revusp/article/view/213450. Acesso em: 21 abr. 2025.

FERREIRA, D. P.; RIBEIRO, R. J.; LIMA, P. M. Aplicação de algoritmos de *machine learning* em sistemas de manutenção preditiva: um estudo de caso em equipamentos de indústria de transformação. **Revista Brasileira de Engenharia e Computação**, v. 25, n. 2, p. 40-50, 2018. DOI: https://doi.org/10.1016/j.jiec.2018.03.004. Acesso em: 20 jul. 2024.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

KAUFMAN, Dora. Inteligência artificial e os desafios éticos: a restrita aplicabilidade dos princípios gerais para nortear o ecossistema de IA. **Revista de Comunicação da FAPCOM,** São Paulo, n. 9, p. 73–84, 2021. Disponível em: https://revistadecomunicacao.fapcom.edu.br. Acesso em: 21 abr. 2025.

KIPPER, Liane M. et al. A revolução da Indústria 4.0: transformando desafios em oportunidades. **Revista de Gestão e Projetos,** v. 15, n. 6, p. 1–13, 2024.

LERNER, Arthur Frederico; FLACH, Leonardo. Auditoria assistida por inteligência artificial com ajustes personalizados e proteção de dados. **Revista Inovação, Projetos e Tecnologias – IPTEC,** v. 12, n. 2, p. 1–18, jul./dez. 2024. DOI: https://doi.org/10.5585/iptec.v12i2.27075. Acesso em: 21 abr. 2025.

LIMA, Faíque Ribeiro; GOMES, Rogério. Conceitos e tecnologias da Indústria 4.0: uma análise bibliométrica. **Revista Brasileira de Inovação,** v. 19, p. 1-30, 2020. DOI: https://doi.org/10.20396/rbi.v19i0.8658766. Acesso em: 22 abr. 2025.

MACÊDO, L. C. **Manutenção preditiva no contexto da Indústria 4.0**: um modelo preditivo em uma fábrica do ramo metalúrgico. 2020. Monografia (Bacharelado em Engenharia Metalúrgica) – Instituto Federal do Espírito Santo, Vitória, 2020.

MANCINI, Mônica. **Internet das coisas**: história, conceitos, aplicações e desafios. São Paulo: MM Project, 2017.

MAYARA, F. et al. Estudo da aplicação de algoritmos de *machine learning* para a manutenção preditiva em IoT. **IEEE** Transactions on Industrial Informatics, v. 14, n. 6, p. 1234-1245, 2020. DOI: https://doi.org/10.1109/TII.2020.3030243. Acesso em: 5 dez. 2024.

MOURA FILHO, F. L.; PEREIRA, A. G.; LIMA, M. F. Diagnóstico de falhas e faltas elétricas em motores de indução utilizando árvores de decisão e redes neurais. **Revista Brasileira de Engenharia Elétrica,** v. 32, n. 4, p. 217-230, 2020. Acesso em: 20 jul. 2024.

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. **Lei Geral de Proteção de Dados (LGPD) e repositórios institucionais**: reflexões e adequações. Em Questão, v. 29,
e127314, 2023. DOI: https://doi.org/10.1590/1808-5245.29.127314. Acesso em: 22 fev. 2025.

PEREIRA JÚNIOR, Muniz Araújo; STAKOVLAK JÚNIOR, Paulo Bell Moura. A Lei Geral de Proteção de Dados no Ensino Superior. **Revista Humanidades e Inovação,** v. 9, n. 47, 2022. Disponível em: https://revista.unitins.br/index.php/humanidadeseinovacao/article/view/8078/4512. Acesso em: 22 fev. 2025.

REYES, Alejandro. **Estrategias de IA aplicada a la auditoría informática**. Technology Rain Journal, v. 2, n. 2, e18, 2023. Disponível em: https://technologyrain.com.ar/index.php/trj/article/view/18. Acesso em: 21 abr. 2025.

ROCHA, Claudionor; LINS, Bernardo Felipe Estellita. **A evolução da Internet**: uma perspectiva histórica. Cadernos ASLEGIS, v. 48, p. 11-38, 2013.

SICHMAN, Jaime Simão. **Inteligência Artificial e sociedade**: avanços e riscos. Estudos Avançados, v. 35, n. 101, p. 37-50, 2021. DOI: https://doi.org/10.1590/s0103-4014.2021.35101.004. Acesso em: 22 abr. 2025.

SILVA, João Francisco da; SANTOS, Fabiana de Almeida; PEREIRA, Juliana Carla. Cibersegurança nos dispositivos IoT de uso doméstico: uma revisão sistemática da literatura. In: CONGRESSO NACIONAL DE PESQUISA E ENSINO EM TECNOLOGIA (CONAPET), 2022. **Anais [...]**. Disponível em: https://conapet.ifpb.edu.br/anais/article/view/259. Acesso em: 21 abr. 2025.

TAKAYAMA, Alessandro; PANHAN, Andre M. Indústria 4.0: desafios e oportunidades para a indústria brasileira. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 8, n. 5, p. 1797–1822, 2022. DOI: 10.51891/rease.v8i5.5591.

TEIXEIRA, João. O que é inteligência artificial. 3. ed. São Paulo: e-galáxia, 2019. Acesso em: 20 jan. 2025.

TORTORELLI, Fernando de F. et al. Adoção da Indústria 4.0: planejamento e desafios. **Revista Prociências**, v. 6, n. 2, 2024. DOI: 10.15210/prociencias.v6i2.25943.

VERA ESTRADA, Víctor Miguel et al. Seguridad en dispositivos IoT: retos y soluciones en un mundo conectado. **Revista G-ner@ndo,** v. 5, n. 2, p. 1835–1844, 2024. Disponível em: https://revistagenerando.com/index.php/revista/article/view/2024. Acesso em: 21 abr. 2025.

ZHANG, Y. et al. **Deep learning for industrial IoT**: opportunities and challenges. IEEE Access, v. 8, p. 213148-213159, 2020. DOI: https://doi.org/10.1109/ACCESS.2020.3030224. Acesso em: 5 dez. 2024.

APÊNDICE A – Script de Instalação do ERPNext com NVM

```
#!/bin/bash

echo "Atualizando pacotes..."

sudo apt update && sudo apt upgrade -y


echo "Instalando dependências do sistema..."

sudo apt install -y python3-dev python3.10-dev build-essential
\

libssl-dev libffi-dev python3-pip python3-setuptools \

libmysqlclient-dev wkhtmltopdf git curl redis-server \

xvfb libfontconfig mariadb-server supervisor \

python3-venv


echo "Removendo instalações antigas de Node.js e Yarn..."

sudo apt remove nodejs yarn cmdtest -y

sudo npm uninstall -g yarn || true


echo "Instalando NVM (Node Version Manager)..."

curl                                                    -o-
https://raw.githubusercontent.com/nvm-sh/nvm/v0.39.7/install.s
h | bash


echo "Carregando NVM no shell atual..."

export NVM_DIR="$HOME/.nvm"

source "$NVM_DIR/nvm.sh"


echo "Instalando Node.js 18 via NVM..."

nvm install 18
```

```
nvm use 18
nvm alias default 18

echo "Instalando Yarn..."
npm install -g yarn

echo "Verificando versões..."
node -v
yarn -v

echo "Configurando MariaDB..."
sudo systemctl enable mariadb
sudo systemctl start mariadb

sudo tee /etc/mysql/mariadb.conf.d/50-server.cnf > /dev/null
<<EOF
[mysql]
default-character-set = utf8mb4

[mysqld]
character-set-client-handshake = FALSE
character-set-server = utf8mb4
collation-server = utf8mb4_unicode_ci
EOF
sudo systemctl restart mariadb

echo "Criando banco de dados e usuário..."
sudo mysql -u root <<EOF
```

```
CREATE DATABASE erpnextdb;
CREATE USER 'erpnext'@'localhost' IDENTIFIED BY 'senha123';
GRANT ALL PRIVILEGES ON erpnextdb.* TO 'erpnext'@'localhost';
FLUSH PRIVILEGES;
EOF

echo "Instalando Bench CLI..."
sudo pip3 install frappe-bench

echo "Criando ambiente Bench..."
rm -rf ~/frappe-bench
mkdir -p ~/frappe-bench && cd ~/frappe-bench

bench init erpnext --frappe-branch version-14
cd erpnext

echo "Criando site do ERPNext..."
bench new-site meu_site.local --mariadb-root-password senha123
--admin-password admin123

echo "Instalando o app ERPNext..."
bench get-app erpnext --branch version-14
bench --site meu_site.local install-app erpnext

echo "Instalação concluída com sucesso."
echo "Para iniciar o servidor, execute:"
echo "cd ~/frappe-bench/erpnext && bench start"
echo "Acesse: http://localhost:8000"
```

APÊNDICE B – Script de Simulação de Manutenção Preditiva com IA

```
import frappe

from datetime import datetime



def simular_ia_manutencao(cenario="default"):

    try:

        leituras = frappe.get_all(

            "SensorLeitura",

                            fields=["name", "valor_da_leitura",
"tipo_do_sensor", "data_hora", "unidade"]

        )

        if not leituras:

                    frappe.throw("Nenhuma leitura de sensor foi
encontrada.")

    except Exception as e:

          frappe.throw(f"Ocorreu um erro ao recuperar os dados
do SensorLeitura: {str(e)}")



    tipos_validos = ["Temperatura", "Pressão", "Vibração"]



    for leitura in leituras:

        if leitura["tipo_do_sensor"] not in tipos_validos:
```

```
            continue

        if leitura["tipo_do_sensor"] == "Temperatura":

             status = "Ok" if leitura["valor_da_leitura"] < 70
else "Alerta"

        elif leitura["tipo_do_sensor"] == "Pressão":

             status = "Ok" if leitura["valor_da_leitura"] < 120
else "Alerta"

        elif leitura["tipo_do_sensor"] == "Vibração":

             status = "Ok" if leitura["valor_da_leitura"] < 15
else "Alerta"



        manutencao = frappe.get_doc({

            "doctype": "ManutencaoPreditiva",

            "sensor": leitura["name"],

            "datahora_da_analise": datetime.now(),

            "status_previsto": status,

                            "comentario": f"Análise do sensor
{leitura['tipo_do_sensor']} em {cenario}",

            "valor_avalidado": leitura["valor_da_leitura"],

        })



        manutencao.insert(ignore_permissions=True)
```

```
        log = frappe.new_doc("LogExecucaoIA")
        log.data_hora_execucao = datetime.now()
        log.usuario = frappe.session.user
        log.cenario = cenario
        log.status = "Ok"
        log.insert()

        frappe.db.commit()

        print("Simulação com regras avançadas e auditoria concluída.")
```