SHEET 01 · COVER

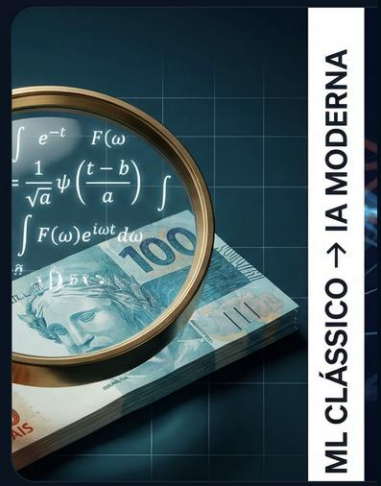
PROVA DE CONCEITO · PESQUISA × PRODUÇÃO SEGURA

Da classificação de notas a uma tese sobre IA segura em produção.

Este material traduz a prova de conceito da Líder Projetos para um formato de artigo editorial. A ambição aqui não é apenas mostrar bons números, e sim explicar por que validação, observabilidade e disciplina DevSecOps se tornaram fundamentais quando IA entra em fluxos críticos.

UNIFOR · Engenharia da Computação

Classificadores implementados do zero



Pesquisa, narrativa e governança na mesm

SHEET 02 · STRUCTURED ABSTRACT

02

Resumo para que entender poucos n perder de

CONTEXTO **A adoção de IA em engenharia crítica avançou mais rápido do que a cultura de validação.**
A pesquisa parte de um problema clássico de classificação de notas bancárias e amplia a discussão para governança, métricas e homologação de IA em pipelines sensíveis.

OBJETIVO **Traduzir um experimento acadêmico em um argumento prático para DevSecOps orientado a IA.**
O foco não é apenas provar desempenho de classificadores, e sim mostrar como precisão, rastreabilidade e tempo de resposta mudam decisões de arquitetura.

MÉTODO **Cinco classificadores implementados do zero sobre o dataset Banknote Authentication.**
O estudo utiliza validação cruzada 10-folds, comparação entre famílias K-NN e Naive Bayes e leitura crítica de correlações entre features.

RESULTADO **Precisão máxima convive com trade-offs claros de velocidade e operação.**
K-NN atingiu 100% de acurácia em dois cenários, enquanto Naive Bayes Multivariado chegou a 98,54% com uma vantagem operacional muito maior em latência.

Se um classificador clássico só merece confiança depois de validação séria, uma IA que gera código, automatiza decisão ou influencia fluxo crítico também
nível de disciplina.

SHEET 03 · QUANTITATIVE CORE

03

Os núme
servem a
impressio
mudam a
arquitetu

Leitura central do experimento

O dataset Banknote Authentication reúne 1.372 amostras e quatro features derivadas de Transformada Wavelet. A comparação entre K-NN e Naive Bayes mostrou um ponto importante: precisão máxima e prontidão operacional nem sempre apontam para a mesma solução.

100%
acurácia com K-NN Euclidiana e Chebyshev

98,54%
acurácia com Naive Bayes Multivariado

140x
ganho de velocidade do Naive Bayes sobre K-NN Euclidiana

1.372
amostras no dataset de autenticação de notas

Ranking de decisão

K-NN Euclidiana

Escolha para cenários altamente controlados com tolerância zero a er

K-NN Chebyshev

Empata em precisão máxima e reforça a força discriminativa das featu

Naive Bayes Multivariado

Melhor equilíbrio entre confiança estatística, latência e escala operaci

SHEET 04 · MARKET SIGNALS

04

O contex
mercado
mensage
segura d
menos d
mais de
madura.

Adoção | Atritos | IA segura

Sinal de mercado

DevSecOps já existe em muitos ambientes, mas prioridade e maturidade ainda são desiguais.

A leitura mais honesta não é que DevSecOps seja raro. É que adoção, prioridade estratégica e maturidade operacional caminham em ritmos diferentes.

ARXIV 2025 · SURVEY COM PMES

68%

das 405 PMEs pesquisadas disseram já ter implementado

ARXIV 2025 · EXPECTATIVA DE IMPACTO

82%

dos líderes técnicos esperam ganho de 25% a 50% em

GITLAB 2024 DEVELOPER SURV

17%

citaram plataformas DevSecO

SHEET 05 · WHY SPECIALISTS MATTER

05

Profissio
DevSecO
entram s
“colocar
Eles des
processo
erro boni
risco real

Definem critérios antes do entusiasmo

Profissionais maduros de DevSecOps evitam que a equipe trate resposta bonita como evidência. Eles começam por métricas, casos de borda, política de contexto e evidências de aprovação.

Redesenham o pipeline para reduzir atrito

Quando segurança parece travar entrega, o problema quase se
esteira, na ordem dos gates e na experiência operacional do tim

Criam rastreabilidade para auditoria e confiança

Sem trilha de decisão, histórico de prompts, contexto, políticas e logs, IA em produção vira caixa-preta. Com trilha, vira engenharia governável.

Transformam pesquisa em padrão reutilizável

O ganho não é só resolver um caso. É criar um modelo de hom
em copilots, agentes, detecção e automações futuras.

SHEET 06 · OPERATING FRAMEWORK

06

Um frame simples p prompt ir chegar a governar e trilha a

01
Hipótese

Formalizar o problema, o risco e o que realmente será medido antes de colocar IA no fluxo.

02
Dataset e contexto

Separar base de teste, prompts, políticas, edge cases e material adversarial para evitar falsa sensação de segurança.

03
Gates

Rodar testes funcionais, test e revisão humana onde o im

04
Observabilidade

Registrar versão, entrada, saída, falhas, drift e custo operacional para não perder governança depois da publicação.

05
Decisão

Escolher entre rejeitar, ajustar, liberar parcialmente ou escalar, com base em sinal mensurável e não em percepção.

06
Aprendizado contínuo

Realimentar a base com nov e mudanças regulatórias par

SHEET 07 · STRATEGIC IMPACT

07

O valor d
está em
pesquisa
pode vira
público, a
técnico e
produto.

Pesquisa científica

A prova de conceito mostra como uma base acadêmica séria pode evoluir para um argumento público mais forte, sem perder responsabilidade metodológica.

Grandes empresas

A tese vale para ambientes regulados, times distribuídos e operações onde geração de código, automação e revisão precisam conviver com trilhas auditáveis.

Centros acadêmicos

Também abre caminho para
e validação experimental co
pesquisa e laboratório.

Em vez de tratar IA como espetáculo, a proposta da Líder Projetos é trabalhar com uma camada mais madura: pesquisa que vira interface, interface que vi
argumento que se sustenta por método.

SHEET 08 · REFERENCES AND ASSETS

08

Referênc
e links pr
publicaçã
executiva
no Linke

GitLab 2024 Developer Survey

Base para os sinais de investimento em plataforma DevSecOps e automação entre profissionais de segurança.
https://about.gitlab.com/resources/developer-survey/2024/

GitLab Press Release · 25 Jun 2024

Resumo executivo oficial com a leitura da tensão entre produtividade, IA e segurança nas organizações.
https://about.gitlab.com/press/releases/2024-06-25-gitlab-survey-reveals-tension-around-ai-security-and-developer-productivity-within-organizations/

Black Duck 2024 DevSecO

Fonte para os indicadores d
e baixa confiança na validaç
https://www.blackduck.com/t
report.html

A Survey on DevSecOps Practices in Small and Medium Enterprises

Estudo com 405 PMEs usado para contextualizar adoção, obstáculos e expectativa de ganho operacional.
https://arxiv.org/abs/2503.22612