

IBM® watsonx.governance para modelos de aprendizado de máquina

Acelere os fluxos de trabalho
com uma IA responsável, transparente e explicável

Destaques

Automatize o controle da IA em todo o ciclo de vida do modelo de aprendizado de máquina

Detecte e mitigue proativamente os riscos de acordo com a prioridade

Melhore as políticas de conformidade, as normas do setor e as regulamentações quanto à IA

Os modelos de aprendizado de máquina (ML) usam análise preditiva para identificar tendências e padrões nos dados, assim, aprendem a tomar decisões de análises mais precisas a partir da experiência. Os casos de uso de ML incluem análise e diagnóstico de imagens médicas, reconhecimento de fala, processamento de linguagem natural (PNL), classificação de textos, análise de sentimento e detecção de fraudes. Infelizmente, a falta de uma plataforma automatizada, com ferramentas e processos otimizados para a IA, a falta de transparência e de resultados explicáveis, as ferramentas inadequadas para se comunicar e colaborar com os stakeholders, tudo isso faz com que seja difícil garantir a precisão e a imparcialidade dos modelos.

O IBM® watsonx.governance automatiza os processos dos modelos em todo o ciclo de vida da IA, com um rigor de nível empresarial e supervisão humana sobre como os modelos são criados e implementados, tanto no local quanto em nuvem. Com ele, as organizações fazem frente aos crescentes desafios nos modelos de ML em uma plataforma unificada e integrada para controlar o ML e a IA generativa.



Abrangente. Traz controle ao ML e à IA generativa em uma plataforma híbrida e integrada



De ponta a ponta. Inclui controle do ciclo de vida e a gestão dos riscos para viabilizar a conformidade com as políticas internas, as normas do setor e regulamentações da IA



Aberto. Funciona com ferramentas externas (como AWS, Microsoft e Google) nos modelos de ML em vigor — você não precisa retirar nem trocar nada

Automatize o controle da IA em todo o ciclo de vida do modelo de ML

Controle do ciclo de vida: acelere a criação de modelos em escala. Automatize e consolide diversas ferramentas, aplicações e plataformas, enquanto documenta a origem dos conjuntos de dados, modelos, pipelines e metadados associados.

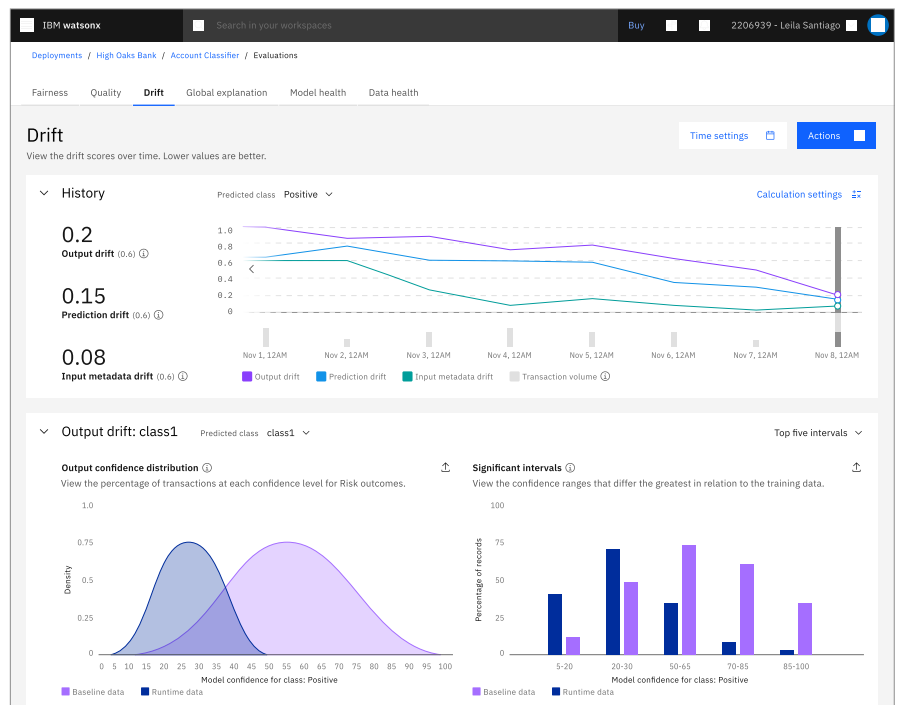
- Monitore, catalogue e controle os modelos em todo o ciclo de vida da IA, onde você estiver. Libere tempo e automatize o fluxo de trabalho para criar e implementar os modelos em escala.
- Capture os metadados dos modelos para gerar os relatórios sem complicações.
- Use o recurso “Fichas técnicas” para que os validadores e aprovadores dos modelos tenham uma visão precisa e em tempo real dos detalhes do ciclo de vida dos modelos.
- Identifique proativamente tendências, desvios e oportunidades de reciclagem, a fim de aumentar a precisão das previsões.
- Use ferramentas e dashboards personalizáveis para melhorar a comunicação e a colaboração com os stakeholders.

The screenshot displays the IBM watsonx Governance web application. The interface is divided into a left-hand navigation menu and a main content area. The navigation menu includes sections for 'Governance', 'Foundation model', 'Prompt template', 'Prompt parameters', 'Evaluation', 'Develop', 'Test', 'Validate', 'Operate', 'Additional details', and 'Attachments'. The main content area is titled 'Governance' and shows the details for an AI use case named 'OCCS Crew Communication System'. The use case is marked as 'Approved' and has a unique ID: '7c8c14b2-a25f-4e5a-a1ce-c97660ccd191'. The description states: 'The On-board Crew Communication ML Model is an advanced machine learning solution designed to enhance and streamline communication between crew and service providers. Leveraging natural language processing (NLP) techniques, this system aims to facilitate efficient and personalized interactions, ultimately improving the overall guest experience.' Below the description, there are tags for 'Q&A', 'Communication', and 'LLM'. The 'Approach' section identifies the model as 'Flan-UL2-12345' and notes that it is suited for this task. The 'Version' section shows '0.2.21' and includes a note: 'I compared this prompt with the other variants. This works better for me. Looking forward to assessment.' At the bottom, a 'Lifecycle' bar shows three stages: '01 Develop' (active), '02 Validate', and '03 Operate'.

Detecte e mitigue proativamente os riscos de acordo com a prioridade

Crie modelos com IA responsável, explicável e de alta qualidade; e automatize a documentação da linhagem e dos metadados dos modelos. Monitore a imparcialidade, o viés e os desvios; e estabeleça uma tolerância aos alertas para mitigar os riscos na hora certa.

- Use um toolkit automatizado e escalável para controlar os riscos e a conformidade (GRC) da IA.
- Use o retreinamento ou a reconstrução dos modelos para se ajustar às mudanças nos padrões e nos perfis comportamentais e, assim, garantir decisões imparciais.
- Use os recursos “Fichas técnicas”, a captura de fatos e a automação da documentação para que os validadores e aprovadores dos modelos tenham uma visão precisa e em tempo real da explicabilidade dos resultados dos modelos.
- Aumente a visibilidade dos dashboards dinâmicos baseados em usuários, dos gráficos e relatórios dimensionais para os stakeholders. Disponibilize resultados explicáveis e com uma visão dos riscos em toda a empresa para todas as unidades de negócios, parceiros e fornecedores.



Melhere as políticas de conformidade, as normas do setor e as regulamentações da IA

Para cumprir a conformidade regulatória, use salvaguardas e validação para criar e implementar modelos imparciais, transparentes e em conformidade. Documente automaticamente os fatos dos modelos para auxiliar as auditorias.

- Transforme os regulamentos externos sobre IA em políticas gerais com aplicação automatizada.
- Use o recurso “Fichas técnicas” para criar uma documentação que melhore a conformidade para fins de auditoria e relatórios.
- Acesse uma plataforma GRC automatizada e escalável para gerenciar os riscos na TI e na segurança com eficácia, além de reduzir custos e atender aos requisitos de conformidade.
- Vincule as políticas e práticas internas de GRC ao ambiente regulatório externo.



AI use case	
Name	Insurance claims processing
ID	3508656-6-0181-44a-8f9-231102a625
Status	Developed Dimitri Hoffmann (DHOFF@de.ibm.com) Nov 12 2023, 12:32 PM GMT
Description	This is a demo use case where we would like to automatically process claims from our customers about their car insurance cases. With the help of AI we would like to automate transcription of customer written claims in a standardized way. Additionally, we want to make use of AI to provide next steps for our internal support teams.
Risk level	medium
Tags	CTA (Prompt engineering) (Demo)
Created by	Dimitri Hoffmann (DHOFF@de.ibm.com)
Created	Nov 08 2023, 13:54 PM GMT
Last modified	Nov 16 2023, 13:39 PM GMT
Approaches used in this AI use case	
Approach name	Description
Prompt Engineering (LangChain)	This approach tackles the use case with prompt engineering of the LangChain foundation model.
Additional AI use case details	
Risk level: Model purpose: Supporting documentation:	
AI asset instance tracking	
This AI use case tracks 2 AI asset versions: 1. "Insurance claim aggregated next steps" with instances in 3 environments of Sprint Production 2. "Insurance claim summarization" with instances in 3 environments of Sprint Development, Pre-production, Production	



Conclusão

O IBM® watsonx.governance acelera a IA responsável, transparente e explicável, com ferramentas e processos automatizados e desenvolvidos para direcionar, gerenciar e monitorar modelos em todo o ciclo de vida da IA. Ele detecta e mitiga os riscos de forma proativa e atende melhor aos requisitos de conformidade, incluindo políticas internas, normas do setor e o dinâmico cenário regulatório. O IBM® watsonx.governance traz controle aos modelos tradicionais de ML e IA generativa, tudo em uma plataforma aberta e integrada, tanto no local quanto em nuvem.

Por que a IBM?

O IBM® watsonx é nossa plataforma de última geração para dados e IA corporativa. Ele inclui o IBM® watsonx.data, o IBM® watsonx.ai e o IBM® watsonx.governance, todos voltados para expandir e acelerar o impacto da IA na sua empresa. O IBM® watsonx gerencia as aplicações mais críticas para os negócios tanto em nuvem quanto no local.

Saiba mais

Para saber mais sobre o watsonx.governance, procure um representante ou parceiro de negócios da IBM; ou acesse ibm.com/br-pt/products/watsonx-governance.

© Copyright IBM Corporation 2023

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo, SP
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produzido nos
Estados Unidos da América
Novembro de 2023

IBM e o logotipo da IBM são marcas comerciais ou marcas registradas da International Business Machines Corporation, nos EUA e/ou em outros países. Os nomes dos demais produtos e serviços podem ser marcas registradas da IBM ou de outras empresas. Confira a lista atualizada das marcas registradas da IBM em ibm.com/br-pt/trademark.

Este documento é atual na data de sua publicação inicial, podendo ser alterado pela IBM a qualquer momento. Nem todas as ofertas estão disponíveis em todos os países em que a IBM opera.

Todos os exemplos de clientes citados ou descritos são apresentados como ilustrações da forma como alguns clientes utilizaram produtos da IBM e os resultados que podem ter alcançado. Os custos e características de desempenho ambientais reais vão variar, dependendo das configurações e condições específicas dos clientes. Geralmente, os resultados esperados não podem ser fornecidos, pois os resultados de cada cliente dependerão inteiramente dos sistemas e serviços adquiridos. É responsabilidade do usuário avaliar e verificar a operação de qualquer outro produto ou programa com produtos e programas IBM.

AS INFORMAÇÕES CONTIDAS NESTE DOCUMENTO SÃO FORNECIDAS NO ESTADO EM QUE SEM ENCONTRAM, SEM QUALQUER GARANTIA, EXPRESSA OU IMPLÍCITA, INCLUSIVE SEM QUALQUER GARANTIA DE COMERCIALIZAÇÃO, ADEQUAÇÃO A DETERMINADO FIM E QUALQUER GARANTIA OU CONDIÇÃO DE NÃO INFRAÇÃO.

Os produtos da IBM têm garantia de acordo com os termos e condições dos contratos sob os quais são fornecidos.

Declaração de boas práticas de segurança: nenhum sistema ou produto de TI deve ser considerado completamente seguro, e nenhuma medida exclusiva de produto, serviço ou segurança pode ser completamente eficaz na prevenção de uso ou acesso inadequado. A IBM não garante que nenhum dos seus sistemas, produtos ou serviços estejam imunes nem que deixarão sua empresa imune a condutas maliciosas ou ilegais por parte de terceiros.

