watsonx.governance™

Governança da IA

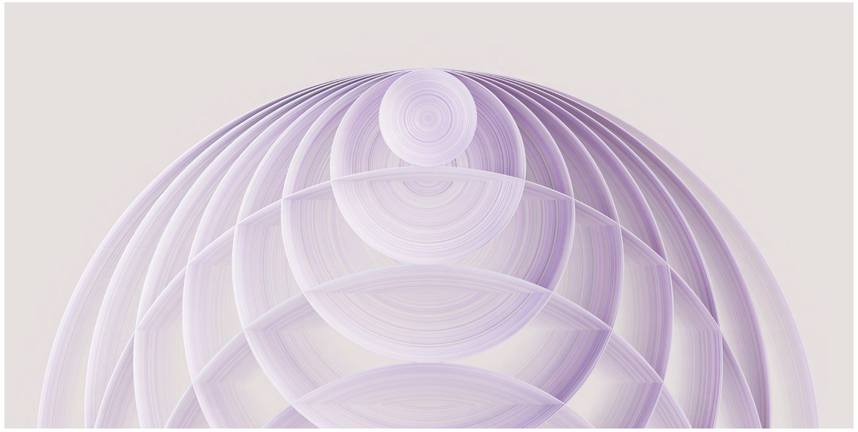
↪ para a empresa

IBM

Índice

01
Introdução

A governança viabiliza a IA no nível empresarial



Seus colegas estão pressionando você para operacionalizar a IA? Tanta ansiedade tem motivo.

Segundo a Harvard Business Review[1], “chamar a IA generativa de revolucionária não é exagero. Ela tem o potencial de melhorar a produtividade em qualquer função que envolva tarefas cognitivas.”

É inegável que a IA promete, e também é inegável que os riscos da IA são reais. Com uma abordagem ponderada à governança, todos podem prosseguir nessa jornada.

Tendo a governança como rede de segurança, não há motivo para negligenciar os aspectos revolucionários da IA.

Acelere os caminhos da sua empresa.

Continue ler na íntegra o artigo; ou avalie o watsonx.governance sem custo.

Espera-se que o tamanho do mercado da IA generativa tenha uma taxa anual de crescimento de 24,40%.[2]

02
Os desafios na expansão da IA

A influência da IA cresce exponencialmente à medida que lideranças organizacionais implementam a tecnologia em quase todos os setores.

Ao mesmo tempo, funcionários e lideranças de várias dessas organizações têm dificuldade com os seguintes aspectos da implementação da IA.

É difícil operacionalizar a IA com confiança

Há uma enorme gama de ferramentas para governança da IA — porém, os modelos muitas vezes são construídos sem a devida clareza, monitorização ou catalogação. Sem o uso de processos automatizados para monitorar todo o ciclo de vida da IA, a escalabilidade e os processos transparentes saem prejudicados. Os resultados explicáveis são enganosos.

Talvez você já tenha ouvido falar dos “modelos caixa preta”, que preocupam cada vez mais os stakeholders da IA. Os modelos de IA são criados e implementados, mas nem sempre é fácil rastrear como e por que as decisões foram tomadas, mesmo para o cientista de dados que as criou. Esses desafios levam a ineficiências, resultando em desvios no escopo; modelos atrasados ou nunca colocados em produção; ou modelos com qualidade inconsistente e riscos não percebidos.

Leia as principais conclusões de uma pesquisa com tomadores de decisão seniores globais de TI sobre o ritmo de adoção da IA.

IBM Global AI Adoption Index 2022 →

É difícil gerenciar os riscos e a reputação
Você sempre ouve por aí dos modelos de IA parciais, inexplicáveis ou tendenciosos em produção. As suposições e decisões incorretas resultantes podem afetar os clientes e prejudicar sua marca.

Com processos e resultados explicáveis, tanto auditores quanto clientes ficam sabendo como os resultados específicos foram obtidos das análises dos dados. Esses processos garantem resultados sem viés quanto a raça, sexo, idade e outros fatores-chave. São processos críticos ao diagnóstico e ao plano de tratamento dos pacientes; à analise das transações consideradas suspeitas; e à revisão de solicitações de empréstimo negadas.

Tome medidas para criar sistemas com uma IA transparente, explicável, imparcial e inclusiva. Assim, você preserva a privacidade, a segurança, a fidelidade e a confiança dos clientes.

Os regulamentos que envolvem IA estão sempre mudando
Uma IA bem-sucedida exige o cumprimento de leis e regulamentos — locais, regionais e nacionais —, que proliferam a um ritmo rápido. O descumprimento pode custar dezenas de milhões de dólares em multas à sua organização — é o que mostram alguns dos regulamentos de IA mais rigorosos debatidos em todo o mundo, como a proposta da Lei da UE para IA. O atual projeto da lei da UE para IA contempla multas de até 30 milhões de euros, ou 6% da receita global de uma empresa.

A documentação do modelo é crucial — e é uma área com aspectos que podem passar despercebidos para os cientistas de dados pressionados por prazos e cuja organização carece de requisitos claros.

Não ignore esse passo: as novas regulamentações exigirão uma documentação-modelo para os metadados e a linhagem.

Cronograma da regulamentação global para IA

2017

Canadá:
estratégia pan-canadense para IA

Japão:
estratégia para a tecnologia da IA

2018

Emirados Árabes Unidos:
estratégia para IA

União Europeia:
GDPR
↓
Multa: $20 milhões ou 4% do faturamento anual da empresa

2019

Alemanha:
estratégia para IA

Coreia do Sul:
estratégia para IA

Índia:
estratégia nacional para IA

Colômbia:
política nacional para transformação digital e IA

2020

Austrália:
framework para ética na IA

Noruega:
estratégia nacional para IA

Sérvia:
estratégia para o desenvolvimento da IA

2021

Estados Unidos:
iniciativa nacional de inteligência artificial

União Europeia:
Lei IA
↓
Multa: $30 milhões ou 6% da receita global da empresa

2022

Estados Unidos:
NIST publica um framework para a gestão dos riscos na IA

Reino Unido:
política de regulamentação da IA

China:
regulamentos para a gestão algorítmica dos serviços de informações da internet (IISARM)

Canadá:
projeto de lei C27, Lei de IA e Dados
↓
Multa:
US$ 25 milhões ou 5% da receita global bruta da empresa

Cingapura:
lança o IA Verify – um framework com toolkit para testes

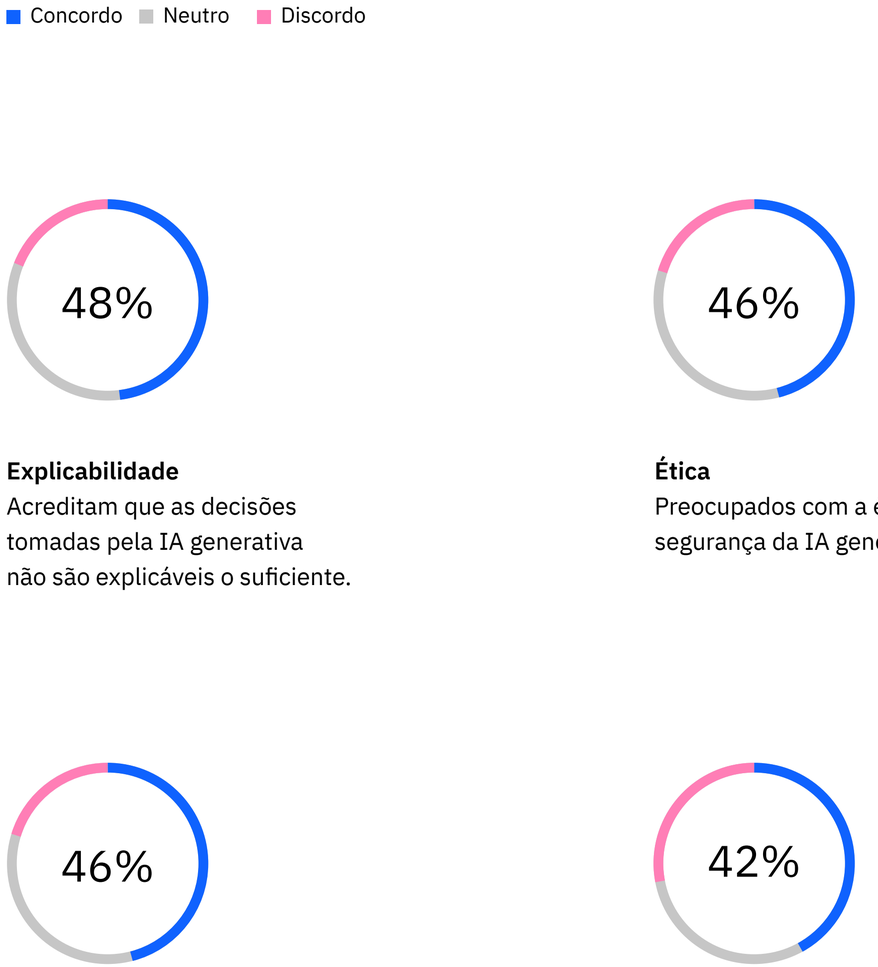
2023

Cidade de Nova York:
lei de contratação com IA

Europa: lei da UE sobre IA; o parlamento chegou a um acordo provisório

Estados Unidos:
decreto presidencial sobre o uso seguro e confiável da IA

80% das lideranças empresariais veem pelo menos uma destas questões éticas como grande preocupação[3]



03

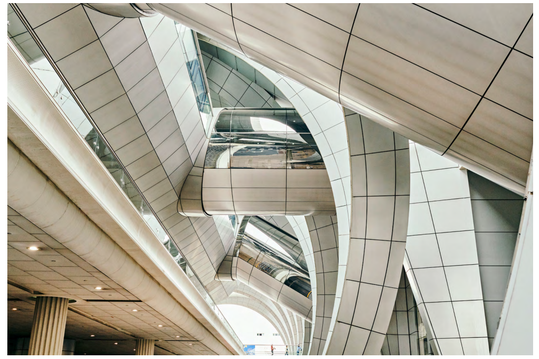
Todos os modelos precisam de governança

Os modelos de IA não são criados da mesma forma, mas todos devem ser governados.

Em 2023, a maioria das organizações emprega o aprendizado de máquina tradicional, e os líderes estão passando a adotar a IA generativa.

Modelos de aprendizado de máquina
Os modelos de ML usam a análise preditiva para identificar tendências e padrões nos dados. Eles aprendem com as experiências e, assim, se aprimoram e tomam decisões mais precisas com base nos dados. Esses modelos são criados com algoritmos treinados por dados classificados, não classificados ou mistos. Com o ML, os modelos aprendem automaticamente, sem intervenção humana.

O aprendizado de máquina usa diferentes algoritmos de acordo com os objetivos, como classificação ou modelagem de previsão. Ou seja, os cientistas de dados usam algoritmos diferentes como base para modelos diferentes. Ao serem introduzidos em um algoritmo específico, os dados são modificados para gerenciarem melhor uma tarefa específica e acabam virando um modelo de aprendizado de máquina.



Modelos generativos
Estes modelos de IA englobam tanto modelos de base (FMs) quanto modelos de linguagem de grande escala (LLMs). Eles têm o potencial de liberar bilhões em valor econômico, pois turbinam a produtividade graças ao notável desempenho e porque podem ser estendidos para uma vasta gama de tarefas.

São modelos altamente personalizáveis, escaláveis e econômicos. Eles consultam enormes volumes de dados e estão sempre aprendendo. As aplicações generativas "prontas para uso" exigem pouco conhecimento e podem eliminar muitas tarefas entediantes e demoradas.

No campo da estatística, os modelos generativos são usados para analisar dados numéricos há anos. Recentemente, o deep learning viabilizou esses modelos para gerarem imagens, música, fala, vídeo, texto e até código. Os casos de uso abrangem marketing, serviço ao cliente, varejo e educação.

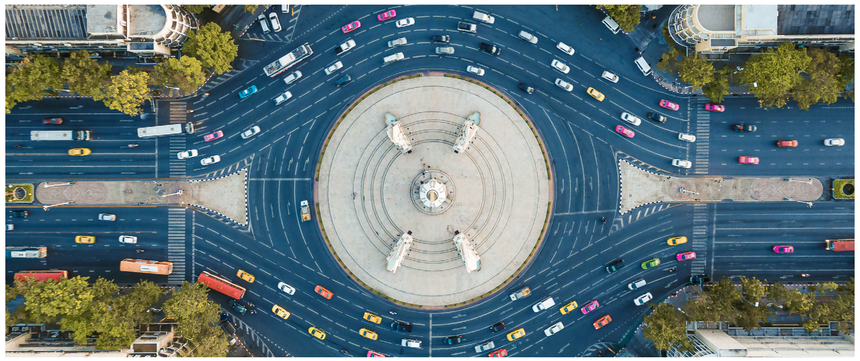
Os modelos generativos colocaram a IA na pauta da maioria das lideranças empresariais, mas os recursos desses modelos trazem uma nova complexidade que representa riscos tanto para as organizações quanto para a sociedade.

Aprenda a expandir a IA de forma responsável.

Leia o blog →

04
Governança holística da IA

Assim como em qualquer outra iniciativa, a governança da IA depende de um conjunto de pessoas, processos e tecnologia.



Para implementar a IA, você precisa de uma equipe sólida e multifuncional. A IA é um imperativo estratégico para muitos líderes, e parece que a lista de stakeholders cresce a cada dia. Alguns deles ainda não entendem o conceito de ciclo de vida da IA; já outros têm novos motivos para se envolver nos esforços de IA.

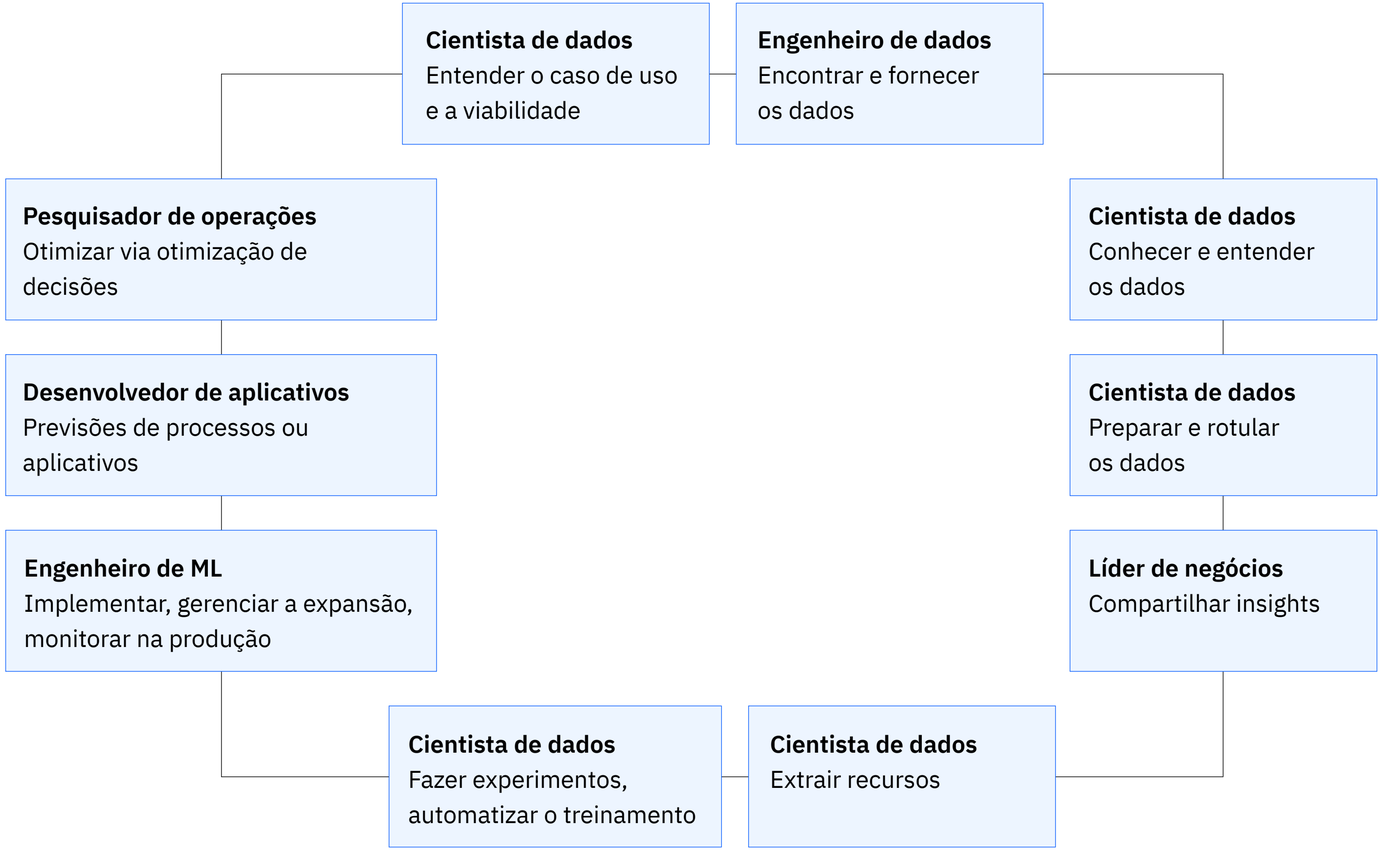
Procure atender às necessidades de todos esses grupos, mas sem sobrecarregar seus cientistas de dados, que têm pouco tempo para encaminhar ou gerenciar as aprovações e as solicitações de informações.

Comece alinhando seus stakeholders. Garanta a adesão das partes interessadas e as incentive a participarem da concepção, a alinharem os resultados e a adotarem uma IA responsável. Em seguida, tome medidas para que o conjunto correto de métricas, KPIs e metas seja definido de acordo com os controles e regulamentos da sua empresa. Também é bom monitorar as métricas que foram identificadas especificamente para os modelos de IA.

Aprenda a criar uma abordagem holística na governança da IA

Leia o blog →

Funções em todo o ciclo de vida da IA



Incentivar a colaboração
com os principais stakeholders
e entender as principais preocupações deles:

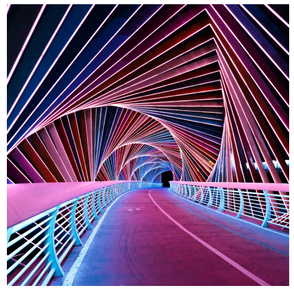
- CFO: riscos à lucratividade
- CMO: riscos à marca
- CRO: riscos à empresa
- CDO: operações eficientes com os dados
- CHRO: potenciais impactos sobre os talentos
- CEO: responsabilização organizacional
- CPO: responsabilização regulatória

Processo
A governança da IA rastreia e documenta a origem dos dados, dos modelos e metadados associados e dos pipelines gerais dos dados, para fins de auditoria. Sua documentação deve incluir as técnicas que treinaram cada modelo, os hiperparâmetros utilizados e as métricas das fases de teste. Isso traz mais transparência e visibilidade entre os stakeholders sobre o comportamento do modelo ao longo do ciclo de vida, incluindo os dados que influenciaram o desenvolvimento e os possíveis riscos do modelo.

Primeiro, é bom comparar e avaliar a tecnologia de IA e os processos com IA vigentes na sua organização. Alguns processos e stakeholders já podem estar alinhados e podem ser estendidos, enquanto outros talvez precisem ser trocados. Em seguida, crie um conjunto de fluxos automatizados de trabalho de governança alinhados aos requisitos de conformidade. Os modelos novos e antigos de IA podem adotar esses fluxos de trabalho, que devem evitar atrasos nos processos já mencionados. Por fim, estabeleça um framework para alertar proprietários e usuários quando as métricas de um modelo excederem os limites.

Tecnologia
Estabelecer uma IA planejada, executada e controlada do jeito certo exige blocos tecnológicos específicos de construção. Procure uma solução que governe o ciclo de vida da IA de ponta a ponta e que:

- Integre dados de vários tipos e origens em diversas implementações
- Seja aberta e flexível e que funcione com as suas ferramentas
- Dê acesso ao autoatendimento com controles de privacidade e uma forma de monitorar a linhagem
- Automatize a criação, implementação, expansão, treinamento e monitoramento dos modelos
- Ligue os vários stakeholders em um fluxo de trabalho personalizável
- Use os metadados da governança para viabilizar um fluxo de trabalho personalizado para diferentes perfis



Framework para uma IA responsável e governada

	Operacionalize com confiança	Gerencie os riscos e a reputação	Fortaleça a conformidade	Atenda às demandas dos stakeholders
Planejar	Defina métricas mensuráveis de desempenho para o uso da IA na sua organização	Revise os processos que já monitoram a imparcialidade e a explicabilidade	Conduza uma análise das lacunas quanto às regulamentações atuais e potenciais sobre a IA	Revise as qualificações existentes e a demanda pela IA responsável e alinhe com as metas de negócios
Desenvolva	Faça a rastreabilidade e a auditabilidade dos processos atuais	Operacionalize processos e checkpoints atualizados ao longo do ciclo de vida da IA	Deixe a documentação do modelo acessível	Especifique as novas funções, qualificações e pautas de aprendizagem necessárias para implementar uma IA responsável
Crie	Crie a documentação automática da linhagem do modelo e dos metadados	Viabilize modelos com IA imparcial, explicável e de qualidade, que minimizem os desvios e façam uma revisão das políticas de forma regular	Fortaleça a conformidade regulatória nas equipes de ciência de dados, mas sem sobrecarregar	Estabeleça um fluxo de trabalho reproduzível e completo, já com as aprovações dos stakeholders, para reduzir riscos e aumentar a expansão

05

watsonx.governance em prol da IA responsável, transparente e explicável.

Conheça o toolkit para a governança da IA.
Com a abordagem do IBM watsonx.governance, você direciona, gerencia e monitora as atividades com IA na sua organização.

Desenvolvido na plataforma de dados e de IA IBM watsonx™, este toolkit emprega a automação dos softwares para você cumprir melhor os requisitos regulatórios e lidar com as questões éticas. Você tem uma governança abrangente da IA sem os custos excessivos de mudar da sua plataforma de ciência de dados atual.

Antes de ser colocado em produção, o modelo é validado para avaliar os riscos aos negócios. Ao entrar em operação, o modelo é continuamente monitorado quanto à imparcialidade, à qualidade e aos desvios. Os reguladores e auditores têm acesso à documentação, que traz explicações sobre o comportamento e as previsões do modelo.

Você dá visibilidade a como o modelo funciona e quais processos e treinamento o modelo recebeu. O watsonx.governance abrange todo o ciclo de vida, e suas equipes recebem assistência enquanto projetam, criam, implementam, monitoram e centralizam os fatos para facilitar a explicabilidade da IA.

Com este toolkit de governança, as auditorias ficam mais fáceis. Rastreie e documente a origem dos dados, os modelos e os metadados e pipelines associados.

A documentação inclui as técnicas que treinaram cada modelo, os hiperparâmetros utilizados e as métricas das fases de teste.

Espere mais transparência no comportamento de cada modelo ao longo do ciclo de vida, além do conhecimento dos dados que influenciaram o desenvolvimento do modelo e a capacidade de determinar possíveis riscos.

Princípios da IBM para a IA responsável

O propósito da IA é ampliar a inteligência humana

Os dados e insights pertencem ao criador

Os sistemas de IA devem ser transparentes e explicáveis

Considere estes componentes:

Conformidade regulamentar

Gerencie a IA para atender às futuras regulamentações e políticas de segurança e transparência em todo o mundo: uma "tabela nutricional" para a IA.

- Transforme os regulamentos externos sobre IA em políticas de aplicação automatizada
- Melhore a adesão aos regulamentos para fins de auditoria e conformidade
- Use dashboards dinâmicos para dar conformidade às políticas e regulamentos

Metadados automáticos
Transformação de dados e captura da linhagem via notebooks Python.

Gestão dos riscos

Detecte e mitigue os riscos de forma proativa, monitorando a imparcialidade, o viés, os desvios e as novas métricas da LLM.

- Automatize os fatos e os fluxos de trabalho para fins de conformidade com as normas da empresa
- Identifique, gerencie e comunique os riscos e a conformidade em larga escala
- Use dashboards dinâmicos para gerar resultados claros, concisos e personalizáveis
- Melhore a colaboração entre várias regiões e geografias

Aberto
Viabilize a governança dos modelos construídos e implementados em ferramentas externas.

Governança do ciclo de vida

Gerencie, monitore e governe modelos de IA da IBM, comunidades de código aberto e outros provedores de modelo.

- Monitore, catalogue e governe modelos de IA onde eles residem
- Automatize a captura de metadados dos modelos
- Aumente a precisão das previsões, identificando como a IA é usada e onde ela é deficiente

Abrangente
Governe o ciclo de vida da IA de ponta a ponta.

06

A governança da IA em ação

IBM Chief Privacy Officer ↷

Expandir a automação para lidar com os requisitos regulatórios quanto à IA
Com base na framework da IA da empresa para lidar com os requisitos regulatórios quanto à IA, o Chief Privacy Office (CPO) da IBM tomou medidas impactantes para colocar em prática os melhores recursos do setor para a IA e os dados, construídos para combinar privacidade, segurança, governança da IA, ética, processos, tecnologia e ferramentas.

Com o respaldo do IBM AI Ethics Board, o IBM CPO desenvolveu um conjunto de processos aprimorados para fazer um monitoramento mais detalhado da conformidade com as normas e os requisitos legais vigentes.

O framework e o processo de governança integrados da IBM gerenciam e monitoram o desenvolvimento e o uso da IA em toda a empresa para que as equipes:

- Usem as ferramentas da IBM para criarem um fluxo de trabalho robusto, que colete, consolide, mostre e monitore o fluxo de trabalho
- Automatizem a captura e a integração dos fatos do ciclo de vida da IA, a fim de acelerar a manutenção do inventário global da IA

Saiba mais →

07
Próximos passos

Descubra como o toolkit watsonx.governance acelera a criação de fluxos de trabalho com IA responsável, transparente e explicável, sem os custos de trocar sua atual plataforma de ciência de dados.

- Operacionalize a governança da IA
- Gerencie riscos e reputação
- Promova a conformidade regulamentar

Comece já

Solicite uma demonstração →
Saiba mais sobre o toolkit de governança →
Avalie sem custo →

1. “How to capitalize on generative AI,” Harvard Business Review, 2023.

2. “Generative AI worldwide,” Statista, 2023.

3. “Generative AI: The state of the market,” IBM Institute for Business Value, 2023.

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

Produzido nos Estados Unidos da América
Novembro de 2023

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 nos quais 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.

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 de seus sistemas, produtos ou serviços estejam imunes nem que tornarão sua empresa imune a condutas maliciosas ou ilegais por parte de terceiros.

O cliente é responsável por garantir o cumprimento de todas as lei e regulamentações aplicáveis. A IBM não fornece conselho jurídico tampouco representa ou garante que seus serviços ou produtos garantirão que o cliente esteja em conformidade com qualquer lei ou regulamentação.