Empresas & Negócios

Matéria de capa

GNEPPHOTO_CANVA

COMO BLINDAR

NOVE RISCOS DA UTILIZAÇÃO DA IA NAS EMPRESAS

Especialista em Inteligência Artificial ensina como blindar o seu negócio

A Inteligência Artificial Generativa está sendo adotada em uma velocidade recorde no Brasil. Contudo, essa adoção rápida está acontecendo, muitas vezes, sem a devida governança, expondo as empresas a riscos críticos que ameaçam desde a privacidade de dados até a própria segurança operacional.

Baseada em referências internacionais e na realidade brasileira, marcada pela rápida adoção de ferramentas generativas sem políticas de governança, Victoria Luz, especialista em IA e autora do best-seller "Além do Hype: Implementando IA com Propósito e Impacto", lista os nove principais riscos do uso da IA nas empresas e um guia prático e responsável sobre como se preparar.

1 Alucinações

Em termos técnicos, são "afirmações plausíveis, porém falsas", produzidas pela IA.

Como evitar: Peça à IA que cite fontes e confira essas referências em materiais originais. Seja específico no prompt, como, por exemplo: "Liste x fontes confiáveis que comprovem sua resposta". Opte por utilizar versões mais recentes, como GPT-4.5 ou GPT-5, alucinam bem menos, e sempre revise e confira os resultados.

2 Exposição de dados pessoais

No Brasil, os consumidores usam IA com entusiasmo, mas têm muita preocupação com o uso de seus dados:

- Para 55% dos brasileiros, a privacidade é valor essencial, então deixe visível suas políticas (como aviso de LGPD) e use linguagem simples;
- Descarte identificadores pessoais antes de enviar dados à IA. Arquive poucos dados sensíveis. Assim, mesmo em caso de vazamento, não há tanta informação pessoal exposta;
- 95,5% dos brasileiros querem "limites éticos" para a IA. Crie comitês de revisão ou contrate consultorias especializadas em ética em IA. Promova treinamento da equipe para que todos entendam a Lei Geral de Proteção de Dados (LGPD) e a importância do consentimento.

3 Deepfakes e mídias sintéticas

Ataques digitais usando deep fakes têm crescido rapidamente no Brasil: entre 2022 e 2023 houve aumento de 830% em crimes com deepfake.

Como evitar: Confirme as comunicações suspeitas por outro canal, adote assinaturas digitais (C2PA) em conteúdos oficiais e realize simulações internas de detecção de deepfakes.

Yuuji_CANVA

> "A inovação não pode se tornar sua maior vulnerabilidade. Implemente e use a IA com propósito, segurança e impacto sustentável na sua empresa.

Por aqui, empresas já enfrentam fraudes via WhatsApp com voz e vídeo falsos. Portanto, a cultura de verificação precisa ser tão comum quanto o antivírus.

4 Prompt Injection e vazamentos de dados

Invasor manipula instruções em um modelo para fazê-lo revelar dados confidenciais ou executar ações não autorizadas.

Como evitar: Proíba funcionários de inserir dados sensíveis, seja de clientes, finanças ou até mesmo código-fonte, em modelos externos. Prefira soluções corporativas seguras, como OpenAI GPT Enterprise ou Azure OpenAI, que não usam inputs dos usuários para treinar o modelo e oferecem criptografia de ponta a ponta. Além disso, implemente mecanismos de Data Loss Prevention (DLP) adaptados para IA: monitores podem detectar e bloquear padrões suspeitos de consulta a informações privilegiadas

5 Shadow AI

Uso de ferramentas ou serviços de IA sem aprovação nem supervisão do departamento de TI.

Quando um analista usa um chatbot público para gerar um relatório sensível, ou um gestor insere dados confidenciais em uma ferramenta de IA sem respaldo da TI, mesmo motivado pela eficiência, esse uso não autorizado pode expor segredos comerciais e causar descumprimento de normas internas.

Como evitar: Governança de IA não é burocracia mas, sim, sustentabilidade. Por isso, estabeleça um programa de governança de IA: liste e avalie as ferramentas de IA em uso (inclusive as não-oficiais), determine quais são aprovadas e bloqueie as demais via políticas de rede ou proxies.

6 Viés em modelos

Sistemas enviesados produzem resultados que refletem e perpetuam desigualdades sociais históricas e atuais. Na área de segurança pública, por exemplo, algoritmos de policiamento preditivo reforçam padrões discriminatórios de prisões. Em negócios, sistemas de recomendação de anúncios do Google já mostraram ofertas de empregos melhor remunerados mais frequentemente para homens do que para mulheres.

Como evitar: Garanta diversidade nos dados de treinamento e elimine atributos sensíveis (como etnia, gênero ou orientação sexual) de modelos que tomam decisões críticas, a menos que haja base legal ou justificativa.

Utilize ferramentas de fairness para detectar e medir viés, por exemplo, bibliotecas de código aberto como IBM AI Fairness 360, Microsoft Fairlearn ou Google What-If Tool, executando testes de impacto para diferentes grupos.

7 Vazamento de propriedade intelectual

A IA generativa abre riscos para segredos comerciais e propriedade intelectual. Funcionários podem, inadvertidamente, inserir informações confidenciais em prompts (como código-fonte exclusivo, fórmulas de pesquisa ou planos estratégicos), que poderão ser regurgitados em outras respostas ou até reentrar no treino do modelo.

Como evitar: Crie políticas rígidas sobre o que pode ser digitado em IAs não corporativas: rotinas internas devem proibir colocar nomes de produtos futuros, código confidencial ou informações de clientes em chatbots abertos. Prefira sempre soluções empresariais de IA que garantam privacidade (por exemplo, ChatGPT Business, Azure OpenAI etc.), pois elas não treinam a partir dos prompts dos usuários. Quando for necessário usar IA pública, remova ou anonimize dados sensíveis do texto fornecido.

8 Conformidade Regulatória (LGPD, PL2338)

Se um chatbot corporativo utiliza dados de clientes sem consentimento, a empresa pode violar a LGPD. Transparência é outro ponto crítico: os usuários têm direito de saber como decisões automatizadas são tomadas. Em nível legislativo, o PL 2338/2023 (Lei Geral de IA) está em tramitação e visa estabelecer princípios éticos, como responsabilidade e explicabilidade, no uso da IA.

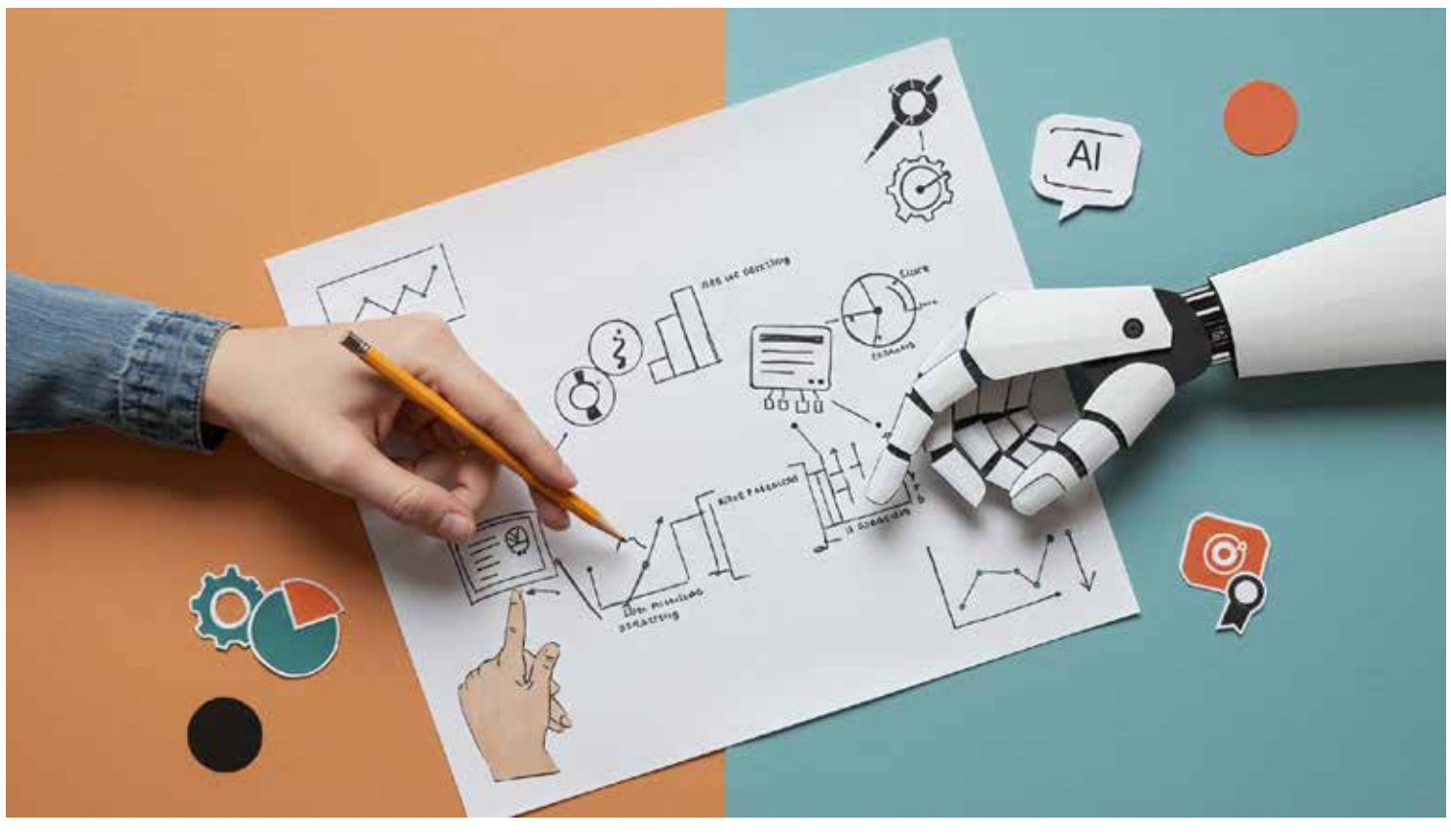
Como evitar: Nomeie um encarregado (DPO) ou equipe responsável por IA para zelar pelo cumprimento da LGPD nas soluções de IA. Estabeleça políticas claras de consentimento e uso de dados, assegurando que informações sensíveis só sejam utilizadas quando houver base legal explícita. Utilize técnicas de privacy by design, como anonimização de dados pessoais antes de alimentar modelos, e aplique criptografia durante o armazenamento e transferência de dados entre sistemas.

9 Vulnerabilidades de terceiros

Ferramentas e serviços de IA quase sempre envolvem terceiros (fornecedores de software, APIs de nuvem, bibliotecas open source), o que amplia a superfície de ataque. Brechas em componentes externos podem expor toda a organização. Estudos mostram que cerca de 30% das violações de dados corporativos tiveram origem em vulnerabilidades de fornecedores ou serviços de nuvem de terceiros.

Como evitar: Gerenciamento de riscos de terceiros - use Software Bill of Materials (SBOM) para manter Inventário dos componentes de software de IA e identificar atualizações críticas. Adote ferramentas de análise de vulnerabilidades em dependências (por exemplo, scanners Snyk, WhiteSource) para detectar e corrigir falhas conhecidas antes do uso em produção. Exija que provedores de IA demonstrem certificações de segurança (como SOC 2, ISO 27001) e ofereçam auditorias.

A inovação não pode se tornar sua maior vulnerabilidade. Implemente e use a IA com propósito, segurança e impacto sustentável na sua empresa.



Stock_Dignity_CANVA