cais Inteligência em Cibersegurança

RNP

Inteligência Artificial – os impactos e o papel da área de TIC nas universidades

Quem sou eu

- **Formação em Análise de Sistemas**
- **Especialização em Gestão de Segurança da Informação**
- **Certificação CIPM / CDPO / CIPT pela IAPP**
- **Encarregado pelo Tratamento de Dados Pessoais na RNP**
- **~23 anos na área de Tecnologia da Informação**
- **~16 anos na área de Segurança da Informação**
- **~5 anos na área de Privacidade & Proteção de Dados pessoais**

RNP

Quem sou eu

Gemini

2.5 Flash

Aqui está uma imagem baseada no nome "Yuri Alexandro":

Peça ao Gemini

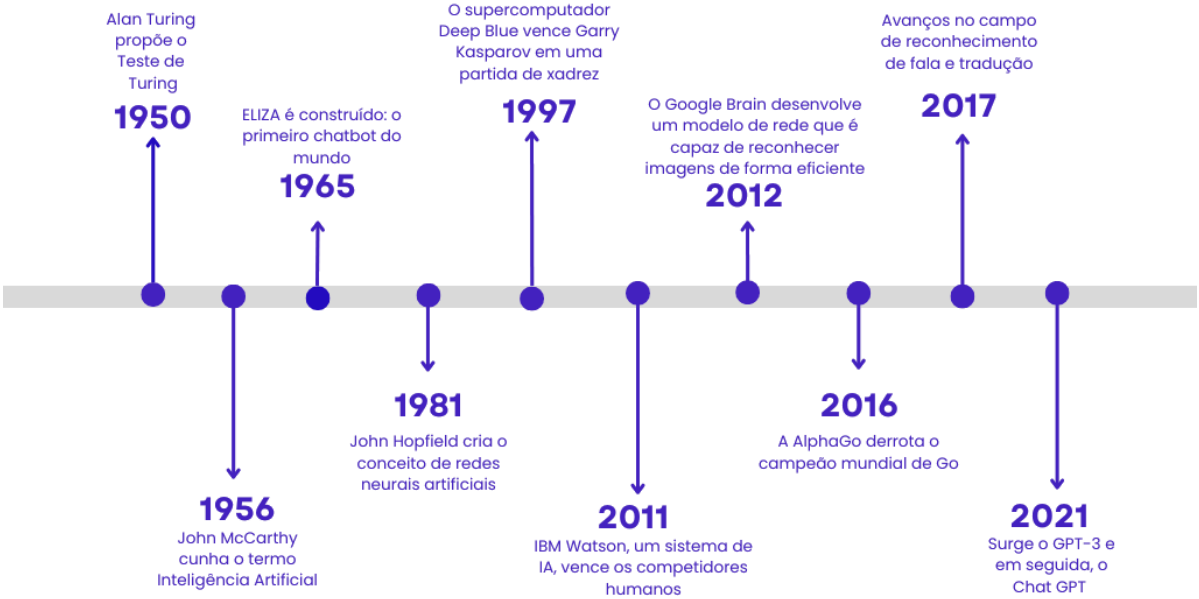
Ferramentas

O Gemini pode cometer erros. Por isso, é bom checar as respostas

Imagem gerada com uso de IA

IA não é uma tecnologia “nova”

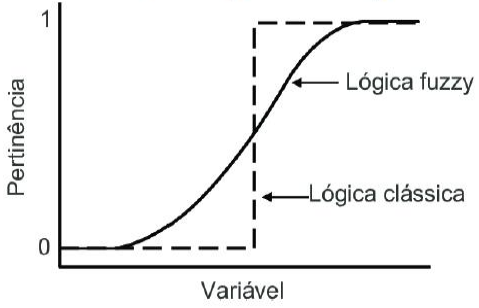
Linha do tempo da evolução da IA



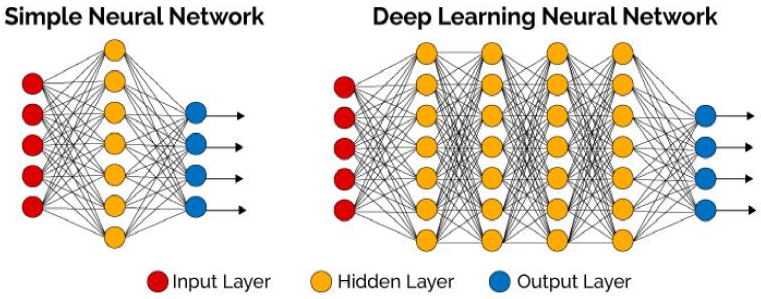
IA não é uma tecnologia “nova”

Evolução da IA

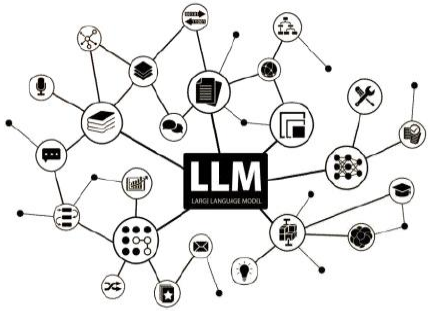
Da lógica fuzzy



das redes neurais



às LLMs



IA não é uma tecnologia “nova”

A Inteligência Artificial

“Estatística e probabilidade aplicada a um conjunto massivo de dados e informações, usando um alto poder computacional.”

Prof. Sérgio Amadeu

“Soberania e a regulação de dados”, 15º Seminário de Proteção à Privacidade e aos Dados Pessoais

Fonte: https://www.youtube.com/watch?v=BxRrRQERkGQ

Inteligência Artificial e dados

Para a Inteligência Artificial
ser o que é hoje, dados é a base de tudo.

De onde vem os dados?

Inteligência Artificial e dados

Para a Inteligência Artificial
ser o que é hoje, dados é a base de tudo.

De onde vem os dados?

Inteligência Artificial e dados

Dados é a base de tudo

De onde vem os dados?

Instagram

Termos de Uso

Bem-vindo(a) ao Instagram!

Estes Termos de Uso (ou "Termos") regem seu uso do Instagram, exceto quando afirmamos explicitamente que outros termos (e não estes) se aplicam, e fornecem informações sobre o Serviço do Instagram (o "Serviço"), descritas abaixo. Ao usar ou criar uma conta do Instagram, você concorda com estes termos. Os Termos de Serviço da Meta não se aplicam a esse Serviço.

Permissões que você nos concede. Como parte de nosso acordo, você também nos concede permissões necessárias para fornecermos o Serviço.

- **Não reivindicamos a propriedade do seu conteúdo, mas você nos concede uma licença para usá-lo.**
  Nada muda com relação aos seus direitos sobre seu conteúdo. Não reivindicamos a propriedade do seu conteúdo que você publica no Serviço ou por meio dele. Além disso, você tem liberdade para compartilhar seu conteúdo com qualquer outra pessoa, onde quiser. Contudo, requeremos que você nos conceda determinadas permissões legais (conhecidas como "licença") para fornecermos o Serviço. Quando compartilha, publica ou carrega conteúdo protegido por direitos de propriedade intelectual (como fotos ou vídeos) em nosso Serviço ou em conexão com ele, você nos concede uma licença não exclusiva, gratuita, transferível, sublicenciável e válida mundialmente para hospedar, usar, distribuir, modificar, veicular, copiar, exibir ou executar publicamente, traduzir e criar trabalhos derivados de seu conteúdo (de modo consistente com suas configurações de privacidade e do aplicativo). Esta licença se encerrará quando seu conteúdo for excluído de nossos sistemas. Para remover conteúdo individualmente ou de uma vez só, basta excluir sua conta. Para saber mais sobre como usamos as informações e sobre como controlar ou excluir seu conteúdo, leia a **Política de Privacidade** e acesse a Central de Ajuda do Instagram.

RNP

Inteligência Artificial e dados

Dados é a base de tudo

De onde vem os dados?

Instagram

Termos de Uso

Bem-vindo(a) ao Instagram!

Estes Termos de Uso (ou "Termos") regem seu uso do Instagram, exceto quando afirmamos explicitamente que outros termos (e não estes) se aplicam, e fornecem informações sobre o Serviço do Instagram (o "Serviço"), descritas abaixo. Ao usar ou criar uma conta do Instagram, você concorda com estes termos. Os Termos de Serviço da Meta não se aplicam a esse Serviço.

- **Permissão para usar seu nome de usuário, sua foto do perfil e informações sobre seus relacionamentos e ações com contas, anúncios e conteúdo patrocinado.** Você nos concede permissão para mostrar seu nome de usuário, sua foto do perfil e informações sobre suas ações (como curtidas) ou relações (como contas que você segue) ao lado de ou relacionados a contas, anúncios, ofertas e outro conteúdo patrocinado que você segue ou com o qual interage, que sejam exibidos nos Produtos da Meta, sem o pagamento de qualquer remuneração a você. Por exemplo, podemos mostrar que você curtiu uma publicação patrocinada criada por uma marca que nos pagou para exibir os anúncios dela no Instagram. Da mesma forma que executar ações em outros conteúdos e seguir outras contas, executar ações em conteúdo patrocinado e seguir contas patrocinadas são atos que podem ser vistos somente por pessoas com permissão para ver ou seguir tal conteúdo. Também respeitaremos suas configurações de anúncios. Saiba mais sobre as configurações de anúncios aqui.

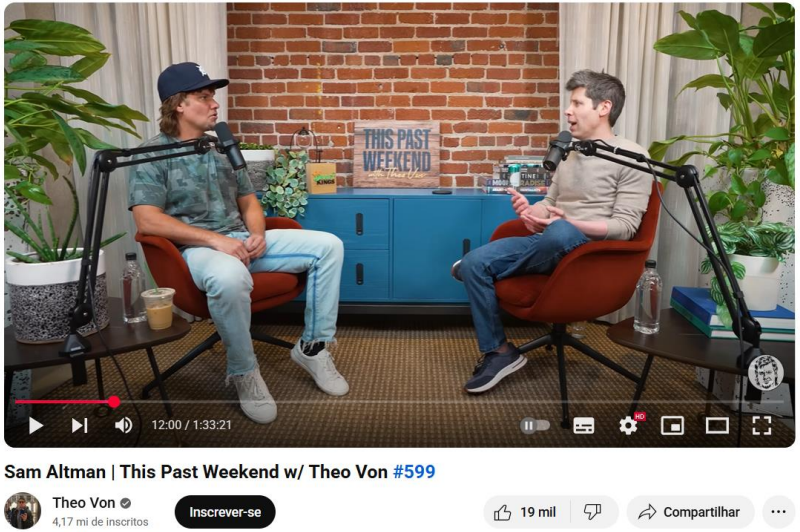
RNP

Inteligência Artificial e dados

Sam Altman's Warning: Everything You Tell ChatGPT Could End Up Being Used Against You

"So if you go talk to ChatGPT about your most sensitive stuff, and then there's ... a lawsuit or whatever, ... we could be required to produce that."

Sam Altman, CEO da OpenAI



https://www.youtube.com/watch?v=aYn8VKW6vXA

IA é aliada ou vilã?

Valor ECONÔMICO | Empresas

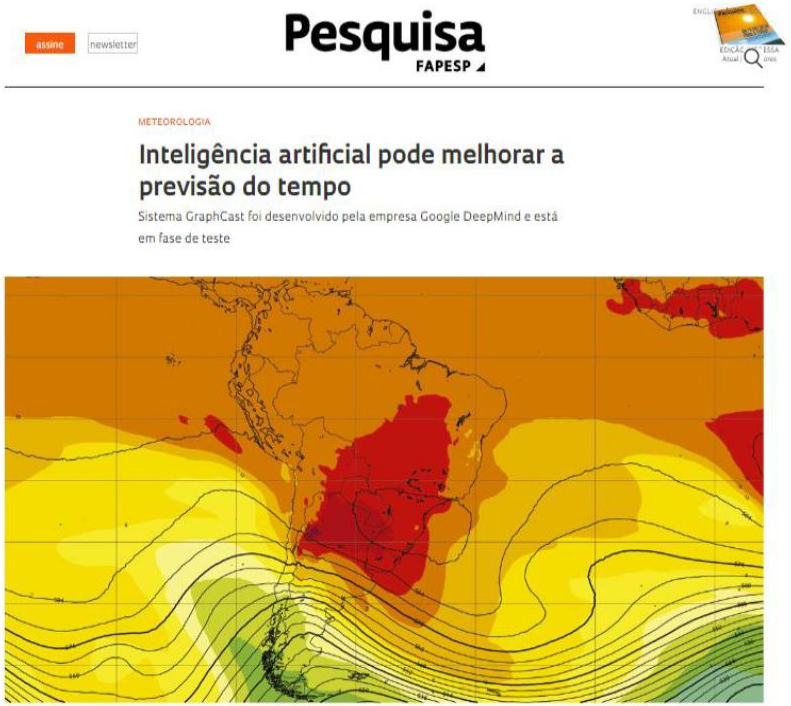
OpenAI afirma que sua tecnologia de inteligência artificial é capaz de moderar conteúdo

Criadora do ChatGPT disse que que suas ferramentas podem ajudar as empresas a realizarem seis meses de trabalho em apenas um dia com possibilidade de moderação ou rotulação de conteúdo

Fonte: https://valor.globo.com/empresas/noticia/2023/08/15/openai-afirma-que-sua-tecnologia-de-inteligencia-artificial-e-capaz-de-moderar-conteudo.ghtml

Inteligência Artificial e dados

Usos importantes de Inteligência artificial



assine newsletter

Pesquisa FAPESP

METEOROLOGIA

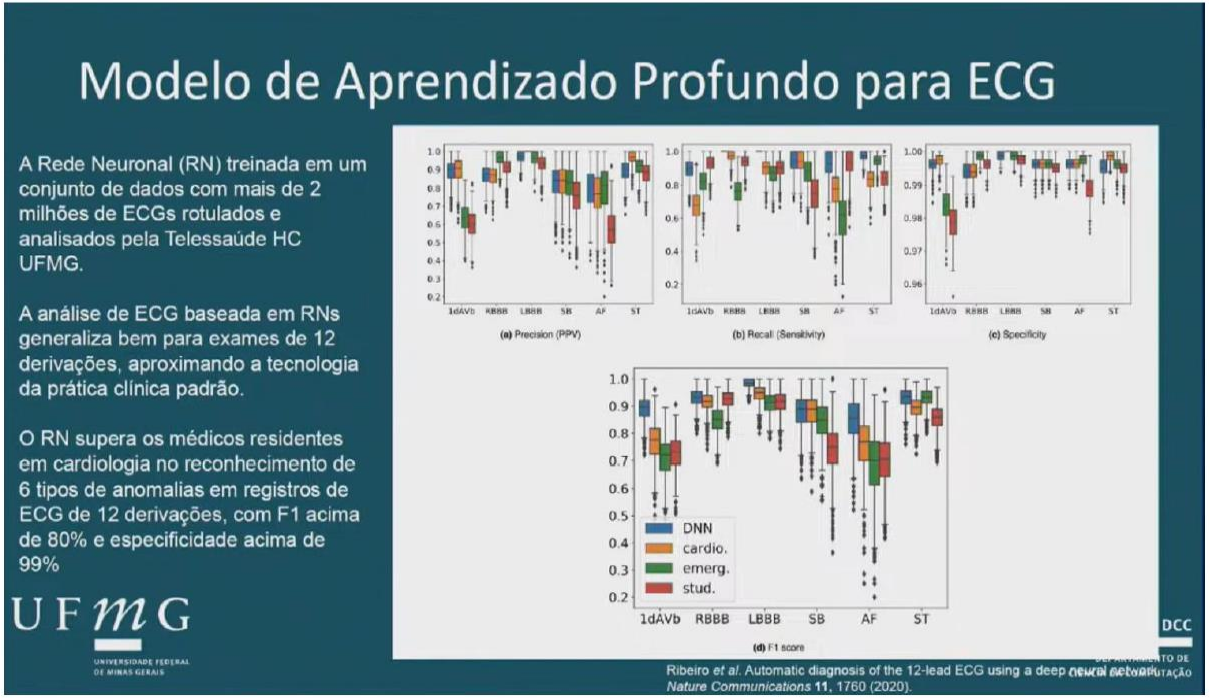
Inteligência artificial pode melhorar a previsão do tempo

Sistema GraphCast foi desenvolvido pela empresa Google DeepMind e está em fase de teste

Fonte: https://revistapesquisa.fapesp.br/previsao-do-tempo-por-aprendizado-de-maquina-seria-mais-eficiente-que-a-feita-pelos-modelos-tradicionais/

Inteligência Artificial e dados

Usos importantes de Inteligência artificial



Fonte: Prof. Wagner Meira Jr.
"Panorama da IA e Auditoria Algorítmica: Desafios Práticos/Técnicos" - 1º Seminário do OBIA
https://www.youtube.com/watch?v=O9czIDgeVFI/

Inteligência Artificial e dados

Dados é a base de tudo

- Como são os métodos de coleta?
  - Dados abertos (*web scraping*)
  - Dados tornados manifestamente públicos
  - Consentimento para uso de dados

- Qual o contexto da coleta?
  - Existe propósito e finalidade?
  - Qual o uso dos resultados?

Contexto regulatório

AI Act – O regulamento europeu de inteligência artificial

Porque falar do regulamento europeu?

* Primeira legislação a nível global e transnacional *

Respeito aos direitos e liberdades individuais de usuários e cidadãos

Uso de IA de forma ética, transparente, segura e sustentável

- Crescimento inclusivo, desenvolvimento sustentável e bem-estar
- Respeito ao Estado de direito, direitos humanos e valores democráticos
- **Transparência e explicabilidade**
- Robustez, segurança e proteção
- Auditabilidade e prestação de contas

AI Act – O regulamento europeu de inteligência artificial

Risks and rights-based approach

- Abordar riscos criados por aplicações de IA;
- Proibir práticas com IA com riscos considerados inaceitáveis;
- Identificar aplicações de IA de alto risco;
- Estabelecer requisitos claros para aplicações de IA de alto risco;
- Definir obrigações para implementadores e fornecedores de IA;
- Exigir avaliação de conformidade antes de comercialização de serviços ou sistemas de IA;
- Implementar mecanismos de medição e fiscalização de sistemas de IA no mercado;
- Estabelecer uma estrutura de governança em nível regional e nacional;

Fonte: https://artificialintelligenceact.eu/

AI Act – O regulamento europeu de inteligência artificial

Riscos inaceitáveis

Manipulação subliminar

- Subverter a consciência de uma pessoa para alterar seu comportamento de forma significativa

Exploração de vulnerabilidades

- Explorar vulnerabilidades de pessoas devido à condições de idade, deficiências ou situação social

Avaliação social

- Avaliar e classificar a confiabilidade de pessoas com base no comportamento ou características sociais

Identificação biométrica remota em tempo real

- Usar identificação biométrica remota em tempo real em espaços públicos, exceto em situações específicas e restritas

Regulamentação da IA no Brasil

PL 2338/2023

Busca garantir a transparência no uso de IA no Brasil

Abordagem regulatória também baseada em riscos

Cria mecanismos de fiscalização e supervisão do tema

Definição riscos baseados na finalidade de utilização

- Ex. Uso em larga escala
  - Potencial afetação de direitos fundamentais
  - Impacto em grupos vulneráveis

Fonte: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

RNP

Com o pé na realidade

O que deve estar na ordem do dia para a área de TI

Qual o propósito de uso do modelo ou sistema de IA?

Contexto e finalidade

Princípios de tratamento de dados

Atenção com dados supostamente anonimizados

O que deve estar na ordem do dia para a área de TI

Forma de coleta dos dados

Fontes públicas ou abertas? (*crawling e/ou scraping*)

Bases legais (LGPD, Art. 7º)

- Obrigação legal ou regulatória
- Legítimo Interesse
- Uso em pesquisas acadêmicas
- Consentimento

Consentimento

- Livre? Esclarecido? Inequívoco? Registrado?

O que deve estar na ordem do dia para a área de TI

Governança de dados

Decreto nº 12.198/2024

- Institui a Infraestrutura Nacional de Dados

Proposta de decreto que estabelece as estruturas de governança de dados

- Cria o cargo de Executivo de dados

Ação estratégica com a Gestão de TI e com Encarregado de Dados Pessoais

Objetivo: Compartilhamento e interoperabilidade

https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados

https://brasilparticipativo.presidencia.gov.br/processes/politicadedados/f/766/

O que deve estar na ordem do dia para a área de TI

Dados pessoais sensíveis

Alto potencial discriminatório

Caracterização de dados sensíveis (LGPD, Art. 5º, inc II)

- Dados sobre origem racial ou étnica
- Dados referentes à saúde ou à vida sexual
- Dados genéticos ou biométricos
- Informações sobre convicções religiosas, filosóficas ou políticas
- **Art. 11, § 1º : " qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular"**

Bases legais específicas e condições especiais de proteção dos dados

O que deve estar na ordem do dia para a área de TI

Dados pessoais sensíveis

Alto potencial de gerar resultados discriminatórios

Transparência nos modelos utilizados

Fonte: https://revistagalileu.globo.com/tecnologia/noticia/2023/10/reconhecimento-facial-no-parana-impoe-monitoramento-de-emocoes-em-escolas.ghtml

GALILEU | Tecnologia

Revista digital | Últimas notícias | Ciência | Saúde | Astronomia | Arqueologia | Cultura | Meio ambiente | Colunistas

Reconhecimento facial no Paraná impõe monitoramento de emoções em escolas

Mecanismo que reconhece expressões dos alunos reproduz racismo e apresenta fragilidades, dizem pesquisadores

Por Amanda Audi | Agência Pública

27/10/2023 10h32 · Atualizado há 10 meses

Empresa usa biometria facial e IA para fiscalizar comportamento dos alunos; sistema foi implantado em 1,7 mil escolas do estado — Foto: Lucas Fermin/Seed-PR

O que deve estar na ordem do dia para a área de TI

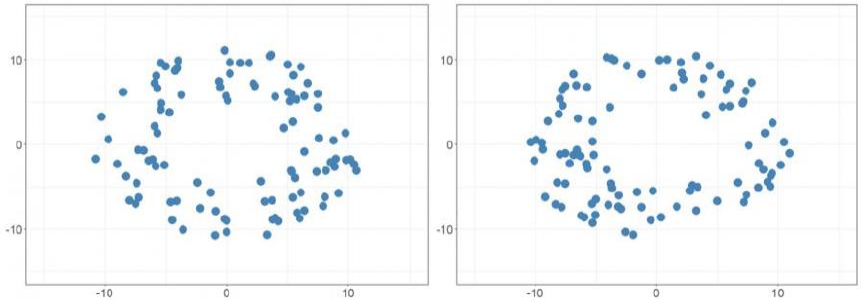
Dados sintéticos

Dados gerados artificialmente que imitam características e padrões de dados reais

Testar e validar modelos de inteligência artificial em um ambiente controlado

Dados sintéticos também podem conter vieses e ocasionar discriminação algorítmica.

Qualidade e confiabilidade dos dados incerta, a depender das técnicas usadas para a geração

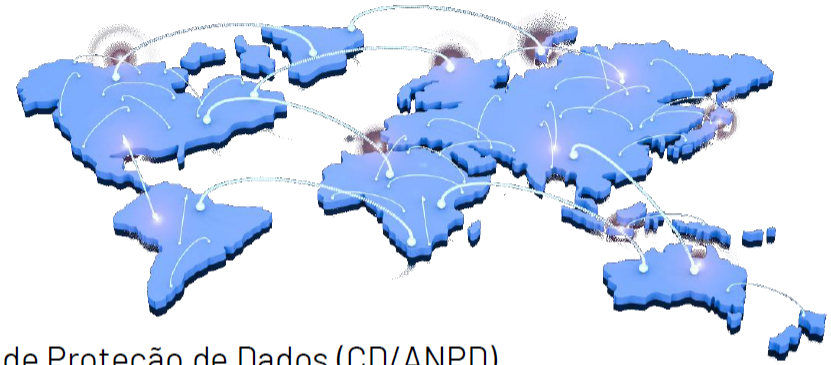


Original data Synthetic data

The synthetic data retains the structure of the original data but is not the same

O que deve estar na ordem do dia para a área de TI

Armazenamento dos dados



Há armazenamento em cloud?

Há caracterização de transferência internacional de dados?

- Regulamento 19/2024, Conselho Diretor da Autoridade Nacional de Proteção de Dados (CD/ANPD)
- Garantia de mesmo nível de proteção de dados
- Garantias contratuais entre fornecedor e implementador
- Instrução Normativa Nº 5, de 30 de agosto de 2021: Dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal)

RNP

O que deve estar na ordem do dia para a área de TI

Governança de dados

Portaria SGD/MGI nº 5.950/2023

- Modelo de Contratação de Software e Serviços de Computação em Nuvem

Estabelece diretrizes sobre o uso de software e serviços de computação em nuvem com ênfase na segurança, proteção à privacidade, integridade e governança dos dados.

- Adoção de um termo de confidencialidade com integrador ou provedor de serviço de nuvem.
- Proibição do uso, transferência ou divulgação de dados a terceiros, empresas ou governos estrangeiros.
- Vedação do uso de dados do poder público para treinamento e otimização de inteligência artificial de provedores

https://www.gov.br/governodigital/pt-br/contratacoes-de-tic/legislacao/modelo-de-contratacao-de-software-e-servicos-em-nuvem/vigentes/portaria-sgd-mgi-no-5-950-de-26-de-outubro-de-2023

RNP

O que deve estar na ordem do dia para a área de TI

Decisões baseadas em tratamento automatizado

"Revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade." (LGPD, Art. 20)

Verificação de aspectos discriminatórios em tratamentos automatizados

O que deve estar na ordem do dia para a área de TI

Shadow AI

Ferramentas de IA usadas sem a aprovação ou supervisão

- Há governança de IA que estabeleça padrões de operabilidade?
- As informações usadas como input seguem a governança de dados institucional?
- Due diligence de soluções e plataformas
- Segurança e privacidade: inserção de dados corporativos e/ou pessoais em contas pessoais de ferramentas LLM
- Riscos: violação de propriedade intelectual, de privacidade, discriminação e vieses algorítmicos.

O que deve estar na ordem do dia para a área de TI

Governança de dados – input e resultados gerados por IA

Dados corporativos das instituições de ensino

Dados acadêmicos

Dados usados por grupos de pesquisa

- ✓ Os investimentos e uso de soluções estão previstas no Plano Diretor de TI?
- ✓ Os Comitês de Ética em Pesquisa (CEPs) estão devidamente treinados para avaliar os riscos?
- ✓ Uso de IA nas atividades de ensino são regulamentados internamente?

RNP

O que deve estar na ordem do dia para a área de TI

Conclusão

Governança de dados é uma necessidade estratégica para o uso responsável de IA

Proteção de dados e respeito aos direitos fundamentais não impede a inovação

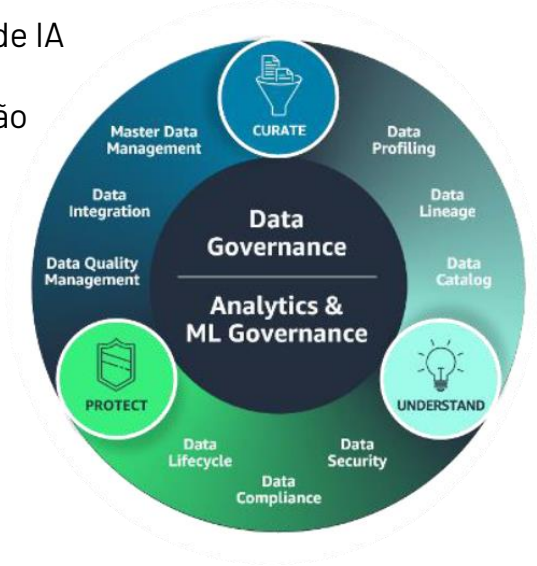
Ética e responsabilidade: uso da inteligência artificial em benefício de quem?

Governança de dados e transparência com o tratamento

Treinamento de LLMs e uso de dados sintéticos

Governança de IA e monitoramento do uso de ferramentas (evitar shadow IA)

Tratamento de vieses nos resultados de processamentos usando IA



Para acompanhar de perto

Outras referências

- Painel Fórum RNP 2023

A Importância do desenvolvimento e uso da Inteligência Artificial de forma ética

https://www.youtube.com/watch?v=lZg_lgKSUmM

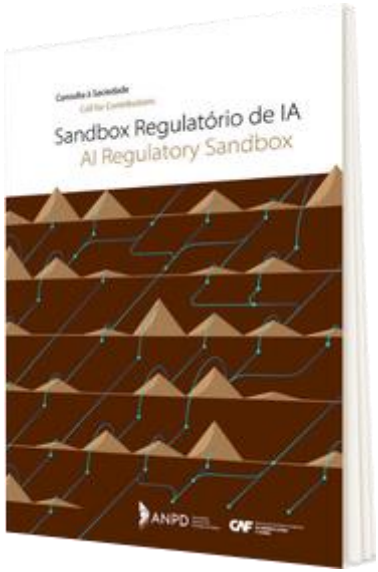
A Importância do desenvolvimento e uso da Inteligência Artificial de forma ética

Rede RNP
11,7 mil inscritos
Inscrito
6
Compartilhar

Para acompanhar de perto

Sandbox regulatório da ANPD

- Experimentação colaborativa entre regulador, entidades reguladas e empresas de tecnologia e inovação, Universidades e organizações da sociedade civil.
- Testar inovações em um arcabouço regulatório.
- Promover o aumento da transparência algorítmica e o fomento à inovação responsável em IA.
- **Estudo técnico do Sandobx realizada pela ANPD:**
  https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/sandbox_regulatorio___estudo_tecnico__versao_publica_.pdf



https://www.gov.br/anpd/pt-br/sandbox/o-sandbox-regulatorio

RNP

Para acompanhar de perto

Estratégia Brasileira de Inteligência Artificial

- Posicionar estrategicamente o Brasil como um modelo global de eficiência e inovação no uso de IA
- Gerar capacidades e capacitações nacionais.
- Garantir a soberania sobre a tecnologia e os dados.
- Instituição do OBIA – Observatório Brasileiro de Inteligência Artificial

Fonte: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2024/07/plano-brasileiro-de-ia-tera-supercomputador-e-investimento-de-r-23-bilhoes-em-quatro-anos/ia_para_o_bem_de_todos.pdf

RNP

OBRIGADO!