b/luz

JULHO 2023

COMO CRIAR UMA GOVERNANÇA DE INTELIGÊNCIA ARTIFICIAL NA MINHA EMPRESA?

Autora:
Bruna Castanheira
Revisores:
Pedro Ramos
Vanessa Pirró

SUMÁRIO

Este índice é navegável!

voltar para o início

1. INTRODUÇÃO

Este é um guia desenvolvido pelo **b/luz** para empresas que utilizam soluções de Inteligência Artificial (IA) no fornecimento de produtos e/ou serviços aos seus clientes. O intuito é auxiliar as empresas a implementarem uma governança de IA de maneira eficaz no desenvolvimento de seus negócios.

1.1. O QUE É GOVERNANÇA DE IA?

Uma governança corporativa de IA estabelece políticas, processos e estruturas para uso ético, seguro e responsável de IA. Pode objetivar a transparência, explicabilidade e responsabilidade nas decisões algorítmicas, entre outros, considerando aspectos como a privacidade, segurança e conformidade jurídica.

Um programa de governança pode incluir políticas claras, controle de dados, auditorias e melhoria contínua. É uma ferramenta prática para auxiliar na implementação da tecnologia de forma ética, transparente e alinhada aos valores da empresa, mitigando riscos e promovendo confiança. Ainda, contribui para sustentabilidade e competitividade, permitindo benefícios responsáveis ao longo do tempo.

voltar para o início

1.2. O QUE DIZ A LEI BRASILEIRA?

Apesar de ainda não possuir uma lei única, o uso da IA já é regulado no Brasil.

Existem tentativas de centralizar essa regulação em normas únicas, como o Projeto de Lei n. 21/20 (que é mais genérico e principiológico) e o Projeto de Lei n. 2.338/2023, que é baseado no relatório final da comissão de juristas responsável por subsidiar a elaboração de substitutivo sobre IA (CJUSBIA). A Estratégia Brasileira de Inteligência Artificial, publicada em 2021 e elaborada pelo Ministério da Ciência, Tecnologia e Inovação (MCTI), também merece destaque por ser o documento norteador das ações do governo federal no desenvolvimento de soluções em IA.

Fato é que diversas leis vigentes já impactam o tema direta ou indiretamente, como é o caso do Marco Civil da Internet (MCI), Lei Geral de Proteção de Dados Pessoais (LGPD), Código de Defesa do Consumidor (CDC). Ao lado, seguem algumas dessas normas:

TABELA DE REGULAÇÃO SETORIAL DE INTELIGÊNCIA ARTIFICIAL

Código de Defesa do Consumidor (Lei 8.078/90)	Política Nacional de Informática (Lei 7.232/84)	Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018)
Regulamento do E-commerce (Decreto 7.962/2013)	Marco Civil da Internet e sua regulação (Lei n. 12.965/2014 Decreto n. 8.771/2016)	Código Civil e Direitos da Personalidade (Lei n. 10.406/2002
Lei Carolina Dieckmann (Lei 12.737/2012)	Lei de acesso à informação (Lei 12.527/2011	Lei de Direitos Autorais (Lei n. 9.510/1998)
Política Nacional de Segurança da Informação (Decreto n. 10.641/2021)	Lei de Software (Lei n. 9.609/1998)	Código Penal (Decreto-lei n. 2.848/1940)
Regulamento do uso de IA no Judiciário (Portaria n. 271/ 2020)	Estratégia Brasileira de Inteligência Artificial (Portaria MCTI n. 4.617/2021)	Resolução que disciplina uso de IA no CNJ (Resolução n. 332/2020)
Padrões ISO e IEE	Lei de Propriedade Industrial (Lei n. 9279/1996)	Estratégia de Governo Digital (Decreto n. 10.332/2020)

Internacionalmente, existem organizações que propõe modelos de governança para empresas que querem ter maior segurança ética e legal na implementação de sistemas de IA em seus negócios.

Em especial, o World Economic Forum (WEF) tem realizado um relevante trabalho na recomendação de melhores práticas para a utilização de IA por organizações. Por meio de diversos materiais publicados, recomendam que as empresas adotem uma abordagem baseada em risco para a governança de IA, que seja proporcional ao potencial de dano da solução tecnológica implementada.

Por isso, recomendamos que, ao utilizar este material em sua empresa, leve em conta o contexto e mercado no qual seu serviço é prestado, bem como, os riscos que as soluções de IA apresentam para o público.

1.3. CENÁRIO INTERNACIONAL

União Europeia (UE): a Comissão Europeia propôs um regulamento abrangente para IA, com o objetivo de promover a confiança e a responsabilidade na utilização dessa tecnologia. A norma aborda diferentes aspectos da IA incluindo classificação de riscos, requisitos de transparência, uso de dados, supervisão e aplicação de sanções. A previsão é de que, até o fim de 2023, o "AI Act" seja publicado.

Estados Unidos (EUA): não há legislação específica sobre IA nos EUA. Porém, existem normas setoriais que regem o uso da IA em determinados contextos. Por exemplo, "AI in Government Act of 2020" e "Executive Order 13960", que regem o uso da tecnologia no governo.

China: existem propostas de regulação de IA tramitando e o país publicou diretrizes para promover o desenvolvimento ético e seguro da tecnologia. Elas abrangem áreas como governança, segurança, privacidade e responsabilidade social.

Outros países: Canadá, Austrália, Japão e Singapura também estão desenvolvendo estratégias e políticas de governança de IA, embora não tenham implementado regulamentações específicas até o momento.

voltar para o início

1.4. POR QUE CRIAR UMA GOVERNANÇA DE IA?

Diversas empresas já estão desenvolvendo políticas e sistemas de governança de IA. Inclusive, o *Berkman Klein* Center tem mapeado tais iniciativas[1]. Nota-se que não apenas as "big techs" ou empresas que desenvolvem soluções de IA tem implementado sistemas internos de governança, mas especialmente **empresas consumidoras de IA.**

Isso porque, assim como as empresas fornecedoras de sistemas de IA, as empresas que contratam soluções de IA (ou seja, que são "operadoras de sistemas de IA") também estão expostas a riscos éticos e regulatórios envolvendo a tecnologia.

Por isso, uma vez implementada, a governança pode ajudar a organização a atingir diversos objetivos, como:

segurança jurídica: mesmo com o vácuo regulatório, a governança de IA permite que sua empresa defina os princípios éticos no uso da tecnologia, considerando as normas já existentes (p. ex., Código de Defesa do Consumidor – CDC, Lei Geral de Proteção de Dados Pessoais - LGPD) e ajudando a evitar o uso indevido ou prejudicial da IA;

gestão de riscos: a governança de IA permite identificar e gerenciar os riscos associados ao uso da tecnologia. Isso inclui avaliar os impactos potenciais da IA em diferentes áreas, como privacidade, segurança, viés e conformidade regulatória. Ao implementar práticas de governança adequadas, sua empresa pode mitigar os riscos e tomar medidas proativas para lidar com eles;

proteção de dados e privacidade: a governança de IA é mais uma ferramenta para auxiliar no tratamento adequado de dados pessoais em sua empresa;

transparência e confiança: estabelecer uma estrutura de governança transparente ajuda a criar confiança com seus stakeholders (parceiros, fornecedores, clientes etc.). Isso envolve fornecer informações claras sobre como a IA é usada, quais dados são coletados e como as decisões são tomadas;

qualidade e desempenho: uma governança eficaz pode ajudar a garantir a qualidade e o desempenho dos sistemas de IA. Isso envolve estabelecer padrões de qualidade, realizar testes e validações adequados, e monitorar o desempenho dos modelos de IA ao longo do tempo;

reputação e competitividade: adotar uma abordagem responsável e transparente para a IA pode fortalecer a reputação de sua empresa e diferenciá-la no mercado. À medida que as preocupações com a ética e a governança da IA aumentam, empresas com uma estrutura sólida de governança podem ganhar a confiança dos clientes e se destacar da concorrência.

1 https://cyber.harvard.edu/publication/2020/principled-ai

2. COMO CRIAR UMA GOVERNANÇA?

Considerando o vácuo regulatório, o crescente número de produções internacionais sobre o tema tem fornecido subsídios para o desenvolvimento de metodologias autônomas para organizações e empresas.

Mais especificamente, instituições como a International Organization for Standardization (ISO) e o Institute of Electrical and Electronics Engineers (IEEE) já publicaram documentos com padrões técnicos para o desenvolvimento de IA[2]. Em especial, documentos publicados pelo WEF apresentam uma série de perguntas a serem feitas pelas empresas para que estas possam se guiar na identificação dos pontos de melhoria e realizar a adequação no uso de sistemas de IA no oferecimento de seus produtos e/ou serviços.

A seguir, reunimos um caminho metodológico a ser adotado pelas empresas, bem como, um compilado das melhores práticas identificadas e que possuem maior adequação com o cenário brasileiro.

2.1. POR ONDE COMEÇAR

O objetivo desse primeiro passo é estabelecer bases sólidas para a criação de um programa abrangente de governança de IA. Essas etapas iniciais ajudarão a definir a visão e os princípios que guiarão suas práticas de governança e a garantir que todos os membros da empresa estejam cientes dos aspectos éticos e impactos da IA em seu mercado.

2 Os materiais específicos podem ser conferidos em: <https://www.iso.org/search.html?q=artificial%20intelligence> e <https://standards.ieee.org/search/?q=artificial%20intelligence&topic=%7CArtificial%20Intelligence%20(AI)&type=%7CStandar>.

voltar para o início

2.1.1. COMO ORGANIZAR A IMPLEMENTAÇÃO DO PROGRAMA DE GOVERNANÇA DE IA EM SUA EMPRESA: PLANEJAMENTO

Organizar e planejar a implementação de uma governança de IA em uma empresa requer uma abordagem estruturada. A seguir, descrevemos as fases desse projeto:

definir objetivos e princípios claros: identifique os objetivos específicos que deseja alcançar com a governança de IA. Isso pode incluir garantir a transparência e explicabilidade dos sistemas de IA, mitigar riscos éticos, promover a conformidade com regulamentações, entre outros. No capítulo seguir, fornecemos algumas orientações para a definição dos princípios éticos em IA;

avaliar o contexto da sua empresa: compreenda o contexto em que a IA será utilizada na sua empresa. Considere fatores como o setor em que atua, os tipos de dados que serão utilizados, os processos existentes e as partes interessadas envolvidas;

mapear e avaliar os riscos: realize uma análise de risco abrangente para identificar os riscos associados ao uso da IA na sua empresa. Isso envolve avaliar aspectos como privacidade, viés algorítmico, segurança, conformidade regulatória e impactos nas partes interessadas;

formar uma equipe multidisciplinar: monte uma equipe responsável por liderar a implementação da governança de IA (p. ex., um comitê) composta por profissionais de diferentes áreas, como jurídico, ética, TI, segurança da informação e compliance.[3] Também:

- identifique um líder para supervisionar e coordenar as atividades relacionadas à governança de IA. Essa pessoa deve ter conhecimento em IA, compreender as questões éticas e de conformidade envolvidas; e
- estabeleça papéis e responsabilidades claras para a equipe de governança de IA e para outras partes interessadas relevantes na empresa. Isso inclui definir quem será responsável por aspectos como ética, conformidade, segurança, privacidade, gerenciamento de riscos e tomada de decisões relacionadas à IA.

3 A FGV SP publicou um check-list para auxiliar na criação de um comitê de ética: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/33736/FGV_Checklist_Framework_Comites_Etica_IA_versao_mai2023.pdf?sequence=3&isAllowed=y

definir políticas e diretrizes: desenvolva políticas e diretrizes claras que orientem o uso responsável e ético da IA na sua empresa. Isso pode incluir diretrizes para a coleta e uso de dados, práticas de explicabilidade e transparência, e requisitos de conformidade;

estabelecer processos de tomada de decisão: defina processos claros para a tomada de decisões relacionadas à IA. Isso inclui a definição de responsabilidades, a designação de papéis e a criação de fluxos de trabalho para revisão e aprovação de projetos de IA;

implementar mecanismos de monitoramento e auditoria: estabeleça mecanismos de monitoramento contínuo para avaliar o desempenho dos sistemas de IA e garantir a conformidade com as políticas e diretrizes estabelecidas. Realize auditorias periódicas para verificar a conformidade e identificar áreas de melhoria;

fomentar a conscientização e a capacitação: promova a capacitação em IA entre os funcionários da empresa:

- treine e conscientize a sua equipe sobre os desafios e os impactos da IA em sua empresa. Isso envolve fornecer treinamento adequado sobre ética e governança de IA, bem como compartilhar informações sobre as implicações da IA nos processos, produtos e serviços de sua organização;
- promova uma cultura de conscientização e aprendizado contínuo sobre a IA. Isso pode incluir a criação de recursos internos, como documentos informativos, diretrizes de melhores práticas e estudos de caso relevantes; e
- incentive a participação e o envolvimento de todos os funcionários na discussão e implementação da governança de IA. Isso ajuda a garantir que todos compreendam a importância da governança de IA e sejam capazes de tomar decisões informadas e éticas no contexto da tecnologia.

estabelecer canais de comunicação e prestação de contas: crie canais de comunicação para que os funcionários possam relatar preocupações, sugestões ou incidentes relacionados à IA. Em conjunto com o seu time de ***compliance,*** garanta a existência de mecanismos para investigar e responder aos questionamentos.

2.1.2. PRINCÍPIOS

O planejamento da implementação de uma governança de IA em sua empresa deve ser feita em conjunto com a definição de conjuntos éticos que serão adotados no uso de IA. **Em resumo, a definição de princípios norteará de que maneira a governança e o fornecimento de seus serviços serão realizados.**

Como dito acima, recomenda-se estruturar uma equipe multidisciplinar (por exemplo, um comitê), para liderar a implementação da governança de IA e realizar a definição de princípios. Importante que profissionais de diferentes áreas e olhares diversos, como jurídico, ética, TI, segurança da informação e compliance façam parte desta equipe.

Em geral, constatamos que o mercado tem adotado dois parâmetros gerais para a implementação de IA:

- empresas que utilizam IA em tomadas de decisões devem garantir que este processo seja explicável, transparente e justo; e
- as soluções de IA devem ser centradas no ser humano. Ou seja, como a IA é usada para ampliar as capacidades humanas, a proteção dos interesses dos seres humanos, incluindo seu bem-estar e segurança, deve ser a principal consideração no design, desenvolvimento e implementação da IA.

A Personal Data Protection Comission of Singapore (PDPC), órgão pioneiro na produção de metodologias de governança em IA, compilou uma série de princípios que já vem sendo adotados por diversas organizações e que podem ajudar a guiar as empresas. A definição dos princípios prioritários em sua empresa facilitará o direcionamento e desenvolvimento de uma governança. Os princípios já desenvolvidos por empresas, como as citadas anteriormente, também são benchmarks valiosos:

precisão: identificar, registrar e articular as fontes de erro e incerteza ao longo do algoritmo e de suas fontes de dados, para que as implicações esperadas e os piores casos possam ser compreendidos e informar os procedimentos de mitigação;

auditabilidade: permitir que terceiros interessados investiguem, compreendam e revisem o comportamento do algoritmo por meio da divulgação de informações que possibilitam o monitoramento, verificação ou crítica;

explicabilidade: garantir que as decisões automatizadas e algorítmicas, assim como os dados associados a essas decisões, possam ser explicados aos usuários finais e demais partes interessadas de forma não técnica;

Equidade:

- buscar uma distribuição equitativa dos benefícios das práticas de dados e evitar práticas de dados que desfavoreçam desproporcionalmente grupos vulneráveis;
- buscar criar o maior benefício possível do uso de dados e técnicas avançadas de modelagem;
- engajar em práticas de dados que incentivem a prática de virtudes que contribuam para o florescimento humano, dignidade humana e autonomia humana;
- dar peso aos julgamentos considerados das pessoas ou comunidades afetadas pelas práticas de dados e estar alinhado com os valores e princípios éticos das pessoas ou comunidades afetadas;
- tomar decisões que não devem causar danos previsíveis ao indivíduo, ou pelo menos minimizar tais danos;
- permitir que os usuários mantenham o controle sobre os dados utilizados, o contexto em que esses dados estão sendo usados e a capacidade de modificar esse uso e contexto; e
- garantir que o bem-estar geral do usuário seja central para a funcionalidade do sistema de IA.

alinhamento aos direitos humanos: garantir que o design, desenvolvimento e implementação de tecnologias não infrinjam os direitos humanos internacionalmente reconhecidos[4];

- manter registros detalhados dos processos de design e tomada de decisão de IA.

robustez e segurança: os sistemas de IA devem ser seguros e protegidos, não vulneráveis a manipulações ou comprometimentos dos dados em que são treinados;

sustentabilidade: favorecer implementações que prevejam efetivamente o comportamento futuro e gerem insights benéficos ao longo de um período razoável.

4 Nesse sentido, o Lapin publicou um documento que auxilia na avaliação de impacto algorítmico para a proteção de direitos fundamentais: https://lapin.org.br/2023/04/13/avaliacao-de-impacto-algoritmico-para-protecao-dos-direitos-fundamentais/

voltar para o início

2.2. COMO IDENTIFICAR OS RISCOS ENVOLVIDOS NA IMPLEMENTAÇÃO E USO DE SISTEMAS DE IA

Ao identificar os riscos associados à implementação e uso de sistemas de IA em seus processos e ao considerar possíveis riscos éticos, legais, técnicos e de segurança, sua empresa estará mais bem preparada para desenvolver estratégias e medidas de mitigação adequadas.

Em linhas gerais, para identificar os riscos, é importante adotar um olhar abrangente quanto às operações da empresa. Ou seja:

- considerando os princípios éticos no uso de IA definidos em sua empresa, realize uma avaliação abrangente dos riscos relacionados à implementação e uso de sistemas de IA em seus processos. Isso envolve identificar os possíveis impactos negativos que a IA pode ter em suas operações, produtos, serviços e partes interessadas;

- leve em conta os riscos técnicos, como falhas nos algoritmos, desempenho inadequado, falta de explicabilidade e vieses algorítmicos;
- avalie também os riscos de integração da IA com os sistemas existentes, escalabilidade, interoperabilidade e segurança dos dados;
- além disso, analise os riscos operacionais, como a dependência excessiva da IA, falta de habilidades e capacitação adequadas para gerenciar a IA, mudanças organizacionais necessárias e possíveis resistências internas;
- avalie os riscos de conformidade, considerando as obrigações legais e regulatórias relacionadas à privacidade, proteção de dados, segurança da informação, direitos do consumidor e outras leis aplicáveis em seu setor.

Em termos mais específicos, para realizar este mapeamento, o WEF[5] sugere a análise de quatro áreas-chave:

01

estruturas e medidas de governança interna

02

determinação do nível de envolvimento humano na tomada de decisões com auxílio de IA

03

gestão das operações

04

interação e comunicação com as partes interessadas

Para cada uma das áreas, são sugeridas perguntas a serem respondidas pelas empresas para auxiliar na identificação dos vácuos a serem endereçados. No Anexo I, elencamos estas perguntas e realizamos adequações para considerar o cenário brasileiro.

5 https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGIsago.pdf

voltar para o início

2.3. ENDEREÇANDO OS RISCOS IDENTIFICADOS

Finalizada a análise dos pontos listados acima, caso sejam identificados riscos ou vulnerabilidades no uso de IA por sua empresa é importante tomar medidas adequadas para mitigar esses riscos. Abaixo, algumas ações que podem ser tomadas:

- √ **avaliar e compreender os riscos:** realize uma análise detalhada dos riscos identificados, incluindo sua gravidade e probabilidade de ocorrência. Compreenda os impactos potenciais desses riscos nas partes interessadas (e.g., clientes, parceiros etc.) e no negócio como um todo;

- √ **revisar e atualizar políticas e práticas:** verifique se as políticas e práticas existentes estão alinhadas com as melhores práticas de governança de IA estruturadas em sua empresa. Faça as atualizações necessárias para abordar os riscos identificados;

- √ **referências:** busque estratégias, referências e políticas de melhores práticas e padrões internacionais de governança de IA e outras referências relevantes em sua indústria;

- √ **fortalecer a governança:** reforce a estrutura de governança de IA da empresa, garantindo que haja responsabilidades claras e definidas para a gestão dos riscos no uso dessa tecnologia. Isso pode incluir a designação de uma equipe ou indivíduo responsável por supervisionar e gerenciar os riscos;

- √ **melhorar a transparência e a explicabilidade:** adote práticas que tornem os sistemas de IA mais transparentes e explicáveis, de modo que os usuários e outras partes interessadas possam entender como as decisões são tomadas. Isso inclui, por exemplo, fornecer explicações claras sobre o funcionamento dos modelos de IA e os dados utilizados;

- √ **implementar mecanismos de monitoramento contínuo:** estabeleça sistemas de monitoramento contínuo para detectar e avaliar os riscos de IA em tempo real. Isso pode envolver a coleta e análise de dados para identificar quaisquer problemas ou desvios no desempenho dos sistemas de IA;

- √ **treinar e capacitar a equipe:** assegure-se de que a equipe envolvida no desenvolvimento, implementação e uso dos sistemas de IA esteja devidamente treinada, atualizada e capacitada;

voltar para o início

3. PRÓXIMOS PASSOS

Uma vez implementada uma governança de IA em sua empresa e realizado o endereçamento de riscos, é importante realizar algumas ações para garantir a eficácia contínua e o aprimoramento do programa de governança:

monitorar e avaliar o desempenho: estabeleça mecanismos de monitoramento contínuo para acompanhar o desempenho dos sistemas de IA e a conformidade com as políticas estabelecidas. Avalie regularmente se os objetivos da governança de IA estão sendo alcançados e identifique áreas que requerem melhorias;

realizar auditorias regulares: realize auditorias periódicas para revisar os processos, políticas e práticas implementadas. Isso ajudará a identificar lacunas, inconsistências ou possíveis problemas e permitirá ajustes e aprimoramentos necessários. No capítulo a seguir, oferecemos algumas orientações para o desenvolvimento de uma auditoria em IA;

manter-se atualizado com regulamentações e melhores práticas: acompanhe as mudanças nas regulamentações relacionadas à IA e as melhores práticas emergentes na área de sua empresa;

promover a conscientização e a capacitação: continue promovendo a conscientização sobre a governança de IA entre os funcionários e forneça treinamentos regulares para manter todos atualizados sobre os princípios éticos, políticas e práticas relacionadas à IA;

realizar revisões e atualizações periódicas: faça revisões regulares das políticas, diretrizes e processos de governança de IA. Atualize-os conforme necessário com base no aprendizado adquirido, nas mudanças no ambiente operacional e nas normas publicadas;

integrar a governança de IA com outras áreas: certifique-se de que a governança de IA esteja integrada a outras estruturas e processos de governança existentes em sua empresa, como governança de dados, segurança da informação e conformidade regulatória.

voltar para o início

3.1. AUDITORIA DE IA

Realizar auditorias de IA pode ajudar a avaliar a conformidade dos sistemas de IA com políticas, regulamentações e padrões estabelecidos, bem como identificar riscos e áreas de melhoria. Para realizar uma auditoria, algumas orientações gerais:

1. **elaboração de um plano de auditoria**

   - defina os objetivos da auditoria, que podem incluir avaliar a conformidade com as políticas e diretrizes estabelecidas, identificar lacunas na governança de IA e avaliar o desempenho dos sistemas de IA em relação aos resultados esperados;
   - identifique as partes interessadas relevantes que devem ser envolvidas na auditoria, como membros da equipe de governança de IA, comitê, profissionais de auditoria interna ou externa e especialistas técnicos.

2. **avaliação da conformidade**

   - verifique se as políticas, diretrizes e procedimentos estabelecidos para a governança de IA estão sendo seguidos adequadamente;
   - analise os processos de desenvolvimento e implementação de IA para identificar possíveis falhas ou lacunas em relação às melhores práticas e requisitos legais e éticos;
   - realize revisões documentais, entrevistas e análise de dados para obter evidências de conformidade;
   - examine os conjuntos de dados utilizados para treinar os modelos de IA. Verifique se os dados são relevantes, representativos, completos, precisos e atualizados.
   - Identifique possíveis vieses nos dados que possam afetar as decisões tomadas pelo sistema de IA;
   - analise os algoritmos e modelos utilizados nos sistemas de IA. Avalie sua precisão, confiabilidade e interpretabilidade. Verifique se os algoritmos estão em conformidade com as políticas estabelecidas e se os resultados são consistentes e justificáveis;
   - avalie a transparência dos modelos de IA, ou seja, a capacidade de entender e explicar como eles chegam a determinadas decisões. Verifique se são fornecidas explicações adequadas sobre as decisões do sistema de IA e se os processos são compreensíveis para as partes interessadas;
   - verifique se os sistemas de IA estão em conformidade com as regulamentações relevantes, como leis de proteção de dados pessoais.

3. monitoramento e avaliação do desempenho da governança de IA

- identifique métricas e indicadores relevantes para medir o desempenho da governança de IA. Isso pode incluir métricas relacionadas à qualidade dos dados, transparência, privacidade, explicabilidade, precisão e mitigação de viés. No Anexo II, incluímos a sugestão de algumas métricas;
- colete dados e informações necessárias para calcular essas métricas e indicadores. Isso pode envolver revisão de relatórios, análise de dados de desempenho dos modelos de IA, entrevistas com os responsáveis pela implementação de IA e revisão de resultados de testes e validações;
- compare os resultados obtidos com as metas estabelecidas e as melhores práticas de governança de IA. Identifique áreas de melhoria e desenvolva ações corretivas, se necessário.

4. relatório de auditoria e acompanhamento

- prepare um relatório que inclua os resultados da auditoria, contendo recomendações de melhorias e riscos identificados, bem como ações corretivas sugeridas;
- compartilhe o relatório com as partes interessadas relevantes, como a equipe de governança de IA, comitê, a alta administração e outras partes envolvidas na governança de IA;
- acompanhe a implementação das ações corretivas e verifique periodicamente o progresso para garantir que as melhorias estejam sendo efetivamente implementadas.

É importante destacar que a auditoria de IA deve ser realizada de forma contínua e regular, acompanhando o desenvolvimento e a evolução dos sistemas de IA em sua empresa. Além disso, é recomendado buscar a orientação de profissionais especializados em auditoria e governança de IA para garantir a eficácia do processo de auditoria.

ANEXO I

LISTA DE PERGUNTAS PARA AUXILIAR NO MAPEAMENTO DE RISCOS NA IMPLEMENTAÇÃO DE SISTEMAS DE IA[6]

6 Elaborado com base em: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/SGIsago.pdf

1. ESTRUTURAS E MEDIDAS DE GOVERNANÇA INTERNA

- sua organização já possui uma estrutura de governança que pode ser aproveitada para supervisionar o uso de IA pela organização?
  - se sua organização não possui uma estrutura existente, sua organização estabeleceu uma nova estrutura de governança para supervisionar o uso de IA?
- a diretoria e/ou a alta administração de sua organização patrocinaram, apoiaram e participaram da governança de IA da sua organização?
- as responsabilidades das pessoas envolvidas nos diversos processos de governança de IA estão claramente definidas?
- as pessoas envolvidas nos diversos processos de governança de IA:
  - estão plenamente cientes de suas funções e responsabilidades?
  - estão devidamente capacitadas?
  - possuem os recursos e orientações necessários para desempenhar suas funções?
- a equipe responsável pelos sistemas de IA recebeu treinamento adequado para interpretar as decisões do modelo de IA, bem como para detectar e gerenciar viés nos dados?
- os demais funcionários que interagem com o sistema de IA estão cientes e sensíveis aos riscos relevantes ao usar IA? Eles sabem a quem comunicar essas questões (por exemplo, especialistas no assunto dentro de suas organizações)?
- sua organização já possui um sistema de gerenciamento de riscos existente que pode ser expandido para incluir riscos relacionados à IA?
  - sua organização implementou um sistema de gerenciamento de riscos para lidar com os riscos envolvidos na implementação da solução de IA identificada (por exemplo, risco de pessoal ou mudanças nos objetivos comerciais)?

2. DETERMINAÇÃO DO NÍVEL DE ENVOLVIMENTO HUMANO NA TOMADA DE DECISÕES COM AUXÍLIO DE IA

- sua organização realizou uma avaliação de impacto (por exemplo, probabilidade e/ou gravidade do dano) em indivíduos e organizações afetados pela solução de IA?
- com base na avaliação, sua organização implementou o nível apropriado de envolvimento humano na tomada de decisões com auxílio de IA?
- após a implantação, sua organização continuamente identificou, revisou e mitigou os riscos do uso da solução de IA?
- para sistemas críticos de segurança, sua organização garantiu que:
  - a equipe responsável é capaz de assumir o controle do sistema de IA quando necessário?
  - a solução de IA fornece informações suficientes para ajudar a equipe a tomar uma decisão informada e tomar as medidas adequadas?

3. GESTÃO DAS OPERAÇÕES

- sua organização implementou práticas baseadas em responsabilidade na gestão e proteção de dados pessoais previstas na LGPD?
- sua organização implementou medidas para rastrear a linhagem dos dados (ou seja, *backward data lineage, forward data lineage e end-to-end data lineage)?*[7]
- se sua empresa obteve conjuntos ou bases de dados de terceiros, foi avaliado e gerenciado os riscos de usar esses conjuntos de dados?
- sua organização é capaz de verificar a precisão do conjunto de dados em termos de quão bem os valores no conjunto de dados correspondem às características verdadeiras do grupo descrito pelo conjunto de dados?
- o conjunto de dados usado é completo em termos de atributos e itens?
- o conjunto de dados usado é credível e proveniente de uma fonte confiável?
- o conjunto de dados usado está atualizado?
- o conjunto de dados usado é relevante?
- quando dados pessoais estiverem envolvidos, eles foram coletados para os fins pretendidos, de acordo com a LGPD?
- o conjunto de dados usado está bem estruturado e em um formato compreensível para máquina?
- se o conjunto de dados usado foi unido a partir de vários conjuntos de dados, as operações de extração, transformação e outras operações relevantes foram realizadas corretamente?
- se algum humano filtrou, aplicou rótulos ou editou os dados, sua empresa implementou medidas para garantir a qualidade do conjunto de dados usado?
- sua organização tomou medidas para mitigar vieses não intencionais no conjunto de dados usado para o modelo de IA, especialmente vieses de estereótipo?
- sua organização usou um conjunto de dados completo, não removendo atributos de dados prematuramente para minimizar o risco de viés inerente?
- sua organização tomou medidas para mitigar vieses que podem resultar de dispositivos de coleta de dados (por exemplo, câmeras e sensores)?
- o conjunto de dados usado para produzir o modelo de IA é totalmente representativo dos dados reais ou do ambiente em que o modelo de IA pode ser recebido ou funcionar?
- sua organização usou conjuntos de dados diferentes para treinamento, teste e validação do modelo de IA?
- sua organização testou o modelo de IA em diferentes grupos demográficos para mitigar vieses sistemáticos?
- sua organização dividiu um grande conjunto de dados em subconjuntos para mitigar os riscos de viés sistemático ao validar o modelo de IA?

7 Para mais informações sobre: https://en.wikipedia.org/wiki/Data_lineage

- sua organização revisa e atualiza periodicamente os conjuntos de dados para garantir sua precisão, qualidade, atualidade, relevância e confiabilidade?
- sua organização implementou medidas para minimizar vieses?
- sua organização identificou recursos ou funcionalidades relevantes que têm o maior impacto para seus clientes, parceiros e demais stakeholders?
- sua organização identificou quais medidas serão mais eficazes para construir confiança com seus clientes, parceiros e demais stakeholders?
- sua organização é capaz de explicar como o modelo de IA implementado funciona e chega a uma determinada previsão?
- quando a explicabilidade não pode ser alcançada de forma prática, sua empresa considerou alternativas menos complexas?
- sua empresa garantiu que o modelo de IA implementado é suficientemente robusto?
- sua organização realiza monitoramento ativo, revisão e ajuste regular do modelo quando apropriado (por exemplo, mudanças no comportamento do cliente, objetivos comerciais, riscos e valores corporativos)?
- os testes do modelo de IA refletem o ambiente de produção real em que se supõe que ele opere?
- sua empresa avaliou o grau em que a solução de IA identificada se generaliza bem e falha de maneira adequada?
- sua organização documentou as informações relevantes, como conjuntos de dados e processos que resultam nas decisões dos modelos de IA, de maneira facilmente compreensível?
- sua organização envolveu uma equipe independente para verificar se eles podem produzir os mesmos ou resultados muito semelhantes usando o mesmo método de IA com base na documentação relacionada ao modelo feita por sua empresa?
- sua organização implementou documentação, procedimentos e processos relevantes que facilitam as avaliações internas e externas do sistema de IA?

4. INTERAÇÃO E COMUNICAÇÃO COM AS PARTES INTERESSADAS

- sua organização identificou as várias partes interessadas internas e externas que estarão envolvidas e/ou impactadas pela implantação da solução de IA?
- sua empresa considerou o propósito e o contexto nos quais a explicação é necessária?
- sua organização adaptou a estratégia de comunicação e/ou explicação de acordo com o público, propósito e contexto?
- sua organização informou as partes interessadas relevantes que a IA é usada em seus produtos e/ou serviços?

- em circunstâncias em que a explicação técnica/explicita pode não ser útil para o público, sua organização forneceu explicação implícita (por exemplo, contrafactuais)?
- sua organização divulgou a forma como uma decisão de IA afeta indivíduos e se a decisão pode ser revertida?
- sua organização avaliou se sua estrutura de governança de IA e processos estão em conformidade com os padrões em constante mudança?
- sua organização disponibilizou o resultado da avaliação para as partes interessadas relevantes?
- sua organização desenvolveu uma política sobre as explicações a serem fornecidas às pessoas e implementou a política de acordo?
- sua organização abordou problemas de usabilidade e testou se as interfaces de usuário atendiam aos seus propósitos pretendidos?
- sua organização informou aos usuários que eles estão interagindo com IA e que suas respostas seriam usadas para treinar o modelo de IA?
  - se as respostas dos usuários forem usadas para treinar o modelo de IA, sua empresa implementou medidas para filtrar respostas enganosas e/ou imprecisas?
- sua organização ofereceu a opção de escolher não usar a solução de IA por padrão (opt-out) ou apenas mediante solicitação?
- sua organização forneceu um canal de feedback para comentários ou dúvidas?
  - o canal de feedback é gerenciado por uma equipe adequada?
- sua organização forneceu um meio para os usuários solicitarem uma revisão das decisões de IA relevantes que os afetaram?

ANEXO II

MÉTRICAS PARA MONITORAR E AVALIAR O DESEMPENHO DA GOVERNANÇA DE IA

Existem várias métricas que podem ser usadas para monitorar e avaliar o desempenho da governança de IA. Abaixo, algumas sugestões:

- Qualidade dos dados
  - precisão dos dados: mede a precisão e confiabilidade dos dados utilizados nos modelos de IA;
  - integridade dos dados: avalia se os dados estão completos, sem duplicações ou valores ausentes; e
  - consistência dos dados: verifica se os dados estão em conformidade com os padrões estabelecidos e não possuem inconsistências.
- Transparência e explicabilidade
  - explicabilidade do modelo: avalia a capacidade de compreender e explicar como o modelo de IA toma decisões;
  - transparência dos algoritmos: mede a clareza e a compreensão dos algoritmos utilizados nos sistemas de IA;
  - acesso à informação: verifica se as informações sobre os modelos de IA, seus dados de treinamento e limitações são facilmente acessíveis.
- Privacidade e segurança
  - conformidade com a proteção de dados: avalia se os sistemas de IA estão em conformidade com as leis e regulamentações de proteção de dados, como o LGPD;
  - segurança dos dados: verifica se são implementadas medidas de segurança adequadas para proteger os dados utilizados nos sistemas de IA contra acesso não autorizado, violações ou ataques cibernéticos.
- Viés e equidade
  - mitigação de viés: avalia se são adotadas medidas para minimizar viés injusto nos modelos de IA, a fim de evitar discriminação ou tratamento injusto;
  - equidade: mede se os sistemas de IA são projetados e implementados de maneira justa e igualitária para todas as partes interessadas envolvidas.
- Desempenho do modelo
  - precisão do modelo: verifica a precisão e o desempenho geral dos modelos de IA em relação aos resultados esperados;
  - taxa de erro: mede a taxa de erros ou falhas na tomada de decisões dos sistemas de IA.
- Aceitação e satisfação do usuário
  - feedback do usuário: coleta e analisa o feedback dos usuários para avaliar a usabilidade, eficácia e satisfação com os sistemas de IA;
  - taxa de adoção: mede a taxa de adoção e utilização dos sistemas de IA pelos usuários.

Essas métricas são apenas exemplos e podem variar dependendo do contexto e dos objetivos da governança de IA em sua empresa. É importante adaptar as métricas às necessidades e especificidades do seu negócio. Além disso, é recomendado estabelecer metas e benchmarks claros para cada métrica, permitindo uma comparação e acompanhamento adequados ao longo do tempo.

b/luz

deixa com a gente

https://baptistaluz.com.br/