



Association for Algorithmization and
Logic Governance Organization

PAULO CARVALHO

MANUAL DO AUDITOR DE IA

BEST SELLER

ISO/IEC FDIS 42.001-IA



SISTEMA DE GESTÃO DE INTELIGÊNCIA ARTIFICIAL

Copyright @2025 By Paulo S.O. Carvalho

Todos os direitos reservados e protegidos pela Lei 9.610, de 19.02.1998
É proibida a reprodução total ou parcial sem a expressa anuência da editora
Este livro foi revisado segundo o Novo Acordo Ortográfico da Língua Portuguesa

Dados internacionais de catalogação na publicação

MANUAL DO AUDITOR IA: Sistema de Gestão de inteligência Artificial
Paulo Carvalho



ISBN: 9798284043622
Selo editorial: Independently publis

1- Contexto da Organização
2- Liderança
3- Planejamento
4 - Supporte
5 - Operação
6 - Avaliação de Desempenho
7 - Melhoria
8 - Objetivos de controle e controle de referência
9 - Orientações para implementação de controles de IA
10 - Objetivos organizacionais potenciais e fontes de risco
11 - Sistema de gestão de IA entre domínios ou setores
12 - Regulamentação Europa ACT (UE) 2024/16 e Brasileira PL 2338

Todos direitos reservados à
XPER BRASIL GESTÃO EM INOVAÇÃO TECNOLÓGICA LTDA
Avenida Desembargador Moreira, 1300 (Sala16A) Aldeota, Fortaleza - CE, 60170-002 -CE - Brasil
CNPJ: 33.173.492/0001-76 - INSC M. - 499110-9
WWW.XPER.SOCIAL
ceo@xper.social



Conteúdo

Prefacio	05
Prólogo	06
Metodologia	07
1 Contexto de IA	09
Entendendo o contexto na prática	10
Entendendo as Expectativas das Pessoas Impactadas	11
Escopo de IA	13
2 Liderança	14
O papel da liderança na gestão da IA	15
Criando uma Política de IA na Prática	16
Política de Governança de Inteligência Artificial	17
3 Planejamento	22
Ações para abordar riscos e oportunidades	23
Como eu avalio os riscos de IA de forma prática	24
Avaliação de Riscos e Oportunidades em IA	25
Planejamento de Riscos e Oportunidades em IA	26
Transformando riscos em ações	27
Avaliação de Impacto Algorítmico	28
Objetivos de IA e planejamento para alcançá-los	31
Exemplo OKRs para planejamento de IA	32
4 Suporte	33
Recursos, competência e conscientização	34
5 Operação	37
Planejamento de controles operacionais	38
Tratamento de risco de IA	39
6 Avaliação de desempenho	40
Monitoramento, Medição, Análise e Avaliação	41
Análise crítica pela direção	42
7 Melhoria	44
Não Conformidade e Ação Corretiva	45
8 Controles A.2	46
Política	46
Organização	49

Isenção de responsabilidade

Este livro é publicado pela XPER GLOBAL LIMITED como contribuição do autor Paulo Sérgio Oliveira de Carvalho. As descobertas, interpretações e conclusões aqui expressas pelo autor são um resultado de um processo colaborativo facilitado e aprovado pelos estudos de casos em empresas privadas e públicas, mas cujos resultados não representam necessariamente as opiniões das empresas citadas, nem da totalidade dos seus sócios, executivos ou outras partes interessadas.

© 2025 XPER GLOBAL LIMITED. Todos os direitos reservados. Nenhuma parte desta publicação pode ser reproduzido ou transmitido de qualquer forma ou por qualquer meio, incluindo fotocópia e gravação, ou por qualquer informação, sistema de armazenamento e recuperação.



Todos Direitos reservados

Conteúdo

Recursos para os sistemas de IA	52
Avaliação dos impactos dos sistemas de IA	57
Ciclo de vida do sistema de IA	60
Dados para sistemas de IA	70
Informação para as partes interessadas	75
Uso de sistemas de IA	80
Relacionamento com clientes e terceiros	84
9 Informativo	88
Objetivos organizacionais	88
10 Regulamentação UE ACT	90
UE ACT x ISO 42.001	90
11 IA no Brasil	114
Entendendo o PL 2338/2023 na Prática	114
Conclusão Final	127

Isenção de responsabilidade

Este livro é publicado pela XPER GLOBAL LIMITED como contribuição do autor Paulo Sérgio Oliveira de Carvalho. As descobertas, interpretações e conclusões aqui expressas pelo autor são um resultado de um processo colaborativo facilitado e aprovado pelos estudos de casos em empresas privadas e públicas, mas cujos resultados não representam necessariamente as opiniões das empresas citadas, nem da totalidade dos seus sócios, executivos ou outras partes interessadas.

© 2025 XPER GLOBAL LIMITED. Todos os direitos reservado. Nenhuma parte desta publicação pode ser reproduzido ou transmitido de qualquer forma ou por qualquer meio, incluindo fotocópia e gravação, ou por qualquer informação, sistema de armazenamento e recuperação.



Prefacio

O Despertar da Inteligência Viva



Paulo Carvalho
Presidente
ALGOR

Vivemos um tempo liminar. Um tempo onde as estruturas conhecidas da realidade estão sendo silenciosamente substituídas por arquiteturas invisíveis, feitas de dados, decisões automatizadas e redes de aprendizado profundo. Um tempo em que a inteligência artificial deixou de ser uma tecnologia emergente para se tornar o fator dominante de transformação civilizatória. Estamos presenciando não apenas o avanço de uma nova tecnologia, mas o nascimento de uma nova forma de inteligência: a Inteligência Viva.

Este livro nasce da urgência de compreender e governar essa transição histórica.

A Inteligência Viva é um conceito que extrapola a noção tradicional de "inteligência artificial". Ela é o resultado da convergência de três tecnologias de propósito geral: a própria IA, sensores avançados e bioengenharia. Essa tríade não apenas amplia nossa capacidade de calcular ou automatizar, mas cria sistemas autônomos que aprendem, se adaptam e interagem de forma integrada com o mundo físico, emocional e biológico. É uma forma de inteligência ubíqua, contínua e em rede, cuja essência é a retroalimentação algorítmica — um organismo digital em expansão.

A Inteligência Artificial como Cérebro Sistêmico

Neste ecossistema emergente, a IA atua como o cérebro estratégico da Inteligência Viva. Ela interpreta sinais, prevê comportamentos, decide fluxos, corrige rotas e sugere caminhos. Seus algoritmos processam bilhões de variáveis por segundo, dando origem a sistemas que podem tanto libertar quanto aprisionar a humanidade. Sua capacidade de aprendizado contínuo — o machine learning — permite que ela evolua em tempo real, ultrapassando barreiras da cognição humana e desafiando os próprios limites éticos e filosóficos da civilização.

Por isso, governar a IA é governar o futuro.

Mas o que significa "governar" neste novo paradigma?

A Inteligência Viva está penetrando em todos os setores: da saúde à energia, do comércio ao direito, da educação às relações interpessoais. Modelos de negócios estão sendo refeitos em tempo real. Profissões inteiras estão sendo transformadas ou extintas. E, com isso, surgem dilemas profundos: Quem responde pelas decisões de uma IA? Como lidar com desigualdades geradas por sistemas algorítmicos? Qual é o papel do humano em um mundo cada vez mais automatizado?

Não existe mais separação entre tecnologia e sociedade. A governança da IA torna-se, assim, uma governança da própria condição humana diante da sua metamorfose digital. Os governos, as empresas e os cidadãos devem assumir seu papel ativo nesse processo — não como coadjuvantes, mas como cocriadores de um novo pacto civilizatório.

O Papel da Governança de IA

Este manual foi concebido para ser um instrumento estratégico. Ele reúne princípios, diretrizes, indicadores e metodologias que permitem projetar, implementar e evoluir um sistema de governança de inteligência artificial alinhado às transformações exponenciais que vivemos.

Inspirado no pensamento sistêmico, no BT Model e nas propostas de algoritmização desenvolvidas por mim, esta obra oferece:

- Mapas conceituais para compreender o ecossistema da Inteligência Viva;
- Estruturas de responsabilidade e compliance para IA;
- Indicadores de maturidade algorítmica;
- Modelos de avaliação de riscos e impactos;
- Estratégias para alinhar a IA à Sociedade 5.0;
- Ferramentas de monitoramento, transparência e prestação de contas.

Este não é um livro técnico no sentido restrito. É um mapa para navegadores de futuros. Um guia para líderes, gestores, inovadores, pensadores, e todos aqueles que compreendem que a inteligência não é um privilégio da máquina, mas uma expressão viva da consciência humana — agora amplificada por circuitos de silício e redes neurais artificiais.

A Inteligência Viva não veio apenas para aumentar a produtividade ou acelerar processos. Ela veio para nos confrontar com nossa própria essência. Ela exige que saímos do piloto automático e assumamos a responsabilidade de construir um futuro onde a tecnologia seja uma extensão da nossa ética, e não uma substituição da nossa humanidade.

O desafio está posto: não basta termos inteligência artificial — precisamos de inteligência ampliada, consciente e responsável.

Este livro é um convite para liderar esse processo. Para transformar medo em entendimento. Dados em decisões. E algoritmos em aliados do bem comum.

Bem-vindo à era da Governança da Inteligência Viva.

Boa leitura,
Boa reflexão,
Boa transformação.

Paulo Carvalho
Especialista em Governança Digital
Criador do BT Model e do conceito de Algoritmização
Co-founder da Quantum School e da XPER Global



Prólogo

Três pilares sustentam essa nova era: Machine Learning (ML), Deep Learning (DL) e IA Generativa (GenAI).



"A IA não se limita em apenas adotar novas tecnologias, mas sim repensar todo o modo como fazemos negócios e buscamos soluções, redefinindo constantemente a experiência do cliente e a eficiência operacional."



"Não faz sentido olhar para trás e pensar: 'devíamos ter feito isso', 'devíamos ter feito aquilo'. O que importa é o que vamos fazer daqui para frente."
 Steve Jobs

Há uma força operando incessantemente, dia e noite, sem pausas, sem cansaço, sem distrações. Uma força invisível, porém onipresente, que está sendo incorporada em tudo o que tocamos, usamos, planejamos e sonhamos. Essa força é a Inteligência Artificial.

A IA não é apenas mais uma inovação tecnológica – ela é a nova base computacional do nosso tempo. É o “motor de tudo” que está alimentando o maior superciclo de transformação já testemunhado na história humana. Sua presença silenciosa se infiltra em cada setor, cada processo, cada decisão. Ela é o novo tecido da realidade digital.

Três pilares sustentam essa nova era: Machine Learning (ML), Deep Learning (DL) e IA Generativa (GenAI). Eles não são tecnologias isoladas – são camadas sobrepostas de uma inteligência em expansão contínua. O Machine Learning ensina as máquinas a aprenderem com os dados, sem serem explicitamente programadas. O Deep Learning aprofunda esse aprendizado, por meio de redes neurais que imitam o funcionamento do cérebro humano, detectando padrões complexos e operando em níveis que ultrapassam a compreensão humana. E, finalmente, a IA Generativa, a estrela atual, que transcende o reconhecimento e passa a criar – conteúdos, ideias, códigos, imagens, vozes, decisões.

Ferramentas como o NotebookLM, da Google, revelam a profundidade dessa revolução. Ao integrar múltiplos formatos de arquivos – PDFs, áudios, páginas da web – em ambientes personalizados, a IA agora é capaz de compreender contextos, sintetizar informações, gerar resumos, construir guias, roteirizar podcasts e oferecer insights, tudo a partir da interação natural com o usuário. Não se trata mais de uma busca; trata-se de diálogo com o conhecimento.

Neste novo paradigma, não precisamos mais alimentar manualmente as máquinas com códigos e comandos rígidos. Agora, conversamos com a inteligência. E mais: ela responde com profundidade, com coerência, com criatividade.

Mas há algo ainda mais profundo acontecendo.

A IA está acelerando a própria ciência. Nas universidades, pesquisas antes repetitivas e demoradas estão sendo transformadas. O que antes exigia centenas de horas de experimentação por parte de estudantes de pós-graduação – ajustes minuciosos em materiais, medidas, variáveis – hoje pode ser simulado, modelado e validado em segundos por sistemas autônomos. Isso não é apenas eficiência: é uma liberação da criatividade humana para desafios mais nobres.

Nesse cenário, surge uma pergunta inevitável: quem governa essa inteligência?

Se a IA é o novo cérebro do mundo, quem será sua consciência?
 Se ela nunca para, nunca esquece, nunca descansa...
 Quem garante que ela servirá ao bem comum, à equidade, à justiça?

Este é o chamado da Governança de IA.

Não basta construir máquinas inteligentes – é preciso criar sistemas éticos, transparentes e auditáveis. É preciso garantir que o poder das redes neurais esteja sempre subordinado à dignidade humana. E é essa a missão que este manual se propõe a cumprir.

A governança da IA é a nova ciência política do século XXI.

É também a nova filosofia, a nova engenharia, o novo pacto social.

E este é apenas o começo.



Metodologia

Governança de IA

1. Princípios Orientadores da Governança de IA

Baseados no Projeto de Lei brasileiro, no AI Act europeu e nos requisitos da ISO 42001.

- Ética e Transparência
- Segurança e Robustez Técnica
- Não Discriminação e Inclusão
- Explicabilidade e Auditabilidade
- Proteção de Dados Pessoais
- Supervisão Humana Significativa
- Responsabilização e Prestação de Contas

2. Estrutura Metodológica da Governança de IA

Etapa	Descrição	Fonte Reguladora
1. Definição do Escopo de IA	Identificação dos sistemas de IA em uso ou em desenvolvimento e seus propósitos	ISO 42001
2. Classificação de Riscos da IA	Análise de risco baseada no impacto sobre direitos fundamentais, segurança e privacidade.	AI Act (Níveis de Risco: Inaceitável, Alto, Médio, Baixo)
3. Avaliação de Conformidade Legal e Ética	Verificação de aderência ao PL 2.338/23 e LGPD, incluindo revisão de vieses, impactos sociais e riscos éticos.	PL IA Brasil
4. Avaliação de Impacto Algorítmico (AIA)	Processo estruturado para avaliar impactos sociais, econômicos, éticos e ambientais de sistemas de IA — com foco especial em autonomia humana, discriminação algorítmica, privacidade, explicabilidade e justiça distributiva. Deve ser aplicado especialmente para IA de alto risco.	AI Act + ISO 42001 + PL
5. Implementação do SGIA – Sistema de Gestão de IA	Baseado na ISO/IEC 42001, abrange: políticas, papéis, responsabilidades, ciclo PDCA e gestão de riscos.	ISO 42001
6. Governança Algorítmica e Explicabilidade	Registro e documentação de modelos, lógicas, dados e justificativas de decisão automatizada.	AI Act + PL
7. Supervisão Humana Significativa	Designação de pontos de decisão crítica com intervenção humana obrigatória.	AI Act
8. Monitoramento Contínuo e Auditoria	Uso de métricas, dashboards e avaliações de desempenho e impacto.	ISO 42001
9. Engajamento de Stakeholders	Inclusão de usuários, clientes, reguladores e sociedade civil nos processos de avaliação e revisão.	PL + AI Act
10. Planos de Mitigação e Remediação	Respostas automatizadas e humanas a falhas, vieses ou violações éticas detectadas.	ISO + AI Act
11. Relatórios e Transparência Proativa	Comunicação clara, acessível e periódica sobre funcionamento, impactos e atualizações dos sistemas de IA.	PL + AI Act



01

Implantando o Sistema de Gestão de Inteligencia Artificial



01

CONTEXTO DE IA ISO 42.001



Antes de implementar qualquer sistema de inteligência artificial, sempre oriento as organizações a darem um passo atrás e responderem:

“Qual é o nosso contexto?”

Esse “contexto” nada mais é do que entender onde estamos, como operamos e o que nos cerca – tanto dentro da organização quanto fora dela. Isso é essencial para garantir que a IA seja bem aplicada, faça sentido estratégico e esteja dentro dos limites legais, sociais e éticos.

PROLÓGICO
PREFÁCIO

CONTEXTO DE IA



Entendendo o Contexto da IA na Prática

Antes de começar qualquer projeto com inteligência artificial, eu sempre oriento meus clientes e parceiros a pararem por um momento e se fazerem uma pergunta essencial:

“Onde estamos e o que queremos alcançar com a IA?”

Parece simples, mas esse é o primeiro passo para garantir que a tecnologia realmente traga valor e não crie riscos inesperados.

Como organização, nós precisamos entender o nosso próprio contexto, tanto interno quanto externo. Ou seja, é necessário observar tudo o que pode afetar o funcionamento do nosso sistema de gestão de IA: as leis que nos regem, as mudanças do mercado, a cultura das pessoas que serão impactadas e até temas globais, como as mudanças climáticas.

Sim, a IA também precisa olhar para o planeta. Se o sistema que estamos desenvolvendo ou usando pode gerar impactos ambientais, esse fator deve ser levado em conta. Isso é parte da responsabilidade digital.

Outro ponto crucial é reconhecer qual é o nosso papel em relação à IA. Isso pode variar bastante, e entender esse posicionamento ajuda a definir quais responsabilidades precisamos assumir. De forma prática, podemos estar em uma ou mais das seguintes funções:

- Somos fornecedores de IA quando entregamos plataformas ou soluções inteligentes para outras empresas.
- Podemos ser desenvolvedores, ou seja, quem realmente projeta, treina, testa e implanta os modelos.
- Também atuamos como usuários finais, quando consumimos a IA já pronta em nossos processos.
- Em outros momentos, somos parceiros, compartilhando dados ou integrando sistemas de diferentes fontes.
- E em casos específicos, somos sujeitos de IA, por exemplo, quando nossos dados pessoais são processados por algoritmos de terceiros.

Cada um desses papéis exige uma atenção diferente. Eles também estão descritos com mais profundidade em outras normas, como a ABNT ISO/IEC 22989 e os guias do NIST sobre riscos em IA.

Agora, voltando ao contexto da organização, ele é influenciado por diversos fatores. No ambiente externo, precisamos considerar:

- Leis e proibições sobre o uso de IA (sim, algumas aplicações são totalmente proibidas em vários países).
- Normas de órgãos reguladores.
- Incentivos fiscais ou barreiras legais dependendo do tipo de uso da IA.
- Valores éticos, culturais e sociais do público que será impactado.
- É claro, o que está acontecendo no mercado: quais as tendências, os concorrentes e os novos modelos surgindo.

Já dentro da própria organização, devemos olhar para:

- Como nossa empresa é governada, suas metas e políticas internas.
- Quais são os contratos e responsabilidades legais que temos com nossos clientes ou parceiros.
- E, principalmente, qual o propósito que temos para usar a inteligência artificial: Por que queremos usá-la? Para resolver qual problema? Por fim, também é preciso observar que tipo de dados estamos tratando. Dependendo se atuamos como “controladores” ou “operadores” desses dados,

nossas obrigações mudam, especialmente se estivermos lidando com dados pessoais. Neste caso, normas como a ISO/IEC 29100 podem trazer boas diretrizes para garantir conformidade e segurança. Checklist Prático – Análise do Contexto de IA Use este modelo para mapear o cenário da sua organização antes de avançar com qualquer projeto de inteligência artificial.

1. Diagnóstico Interno

Aspecto	Sim	Parcial	Não	Obs
Temos clareza sobre nossos objetivos com a IA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sabemos quem vai liderar e governar o uso da IA internamente?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Existem políticas claras sobre uso de dados e tecnologia?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
A organização possui equipe ou parceiros com conhecimento técnico sobre IA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Temos contratos ou obrigações legais que envolvam IA ou dados?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

2. Diagnóstico Externo

Aspecto	Sim	Parcial	Não	Obs
Conhecemos as leis e regulamentações que se aplicam à IA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Entendemos as expectativas de nossos clientes e usuários quanto ao uso da IA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Avaliamos se há riscos sociais, éticos ou ambientais envolvidos?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
Sabemos como os concorrentes estão usando IA no setor?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
As mudanças climáticas ou práticas sustentáveis impactam nosso projeto de IA?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Qual é o nosso papel com a IA?

Marque os papéis que sua organização desempenha ou pretende desempenhar:

- Fornecedor de IA
- Desenvolvedor de IA
- Usuário de sistemas de IA
- Parceiro / Integrador de IA
- Sujeito afetado por IA (ex: titulares de dados)
- Autoridade ou regulador



Entendendo as Expectativas das Pessoas Impactadas pela IA

Quando falamos em implantar um sistema de gestão de inteligência artificial em uma empresa, uma das primeiras coisas que gosto de destacar é que a IA não vive sozinha – ela sempre afeta ou interage com outras pessoas, direta ou indiretamente.

Por isso, entender quem são as partes interessadas e quais são suas expectativas e preocupações é uma etapa essencial do processo. E isso vale para qualquer tipo de organização, seja pública ou privada.

Então eu pergunto:

Quem está envolvido ou pode ser impactado pelo uso da IA na sua empresa?
O que essas pessoas esperam? O que elas exigem?

Essas “partes interessadas” podem ser muito diversas. Vou dar alguns exemplos práticos:

- Seus clientes, que querem transparência, segurança de dados e decisões justas feitas por sistemas automatizados;
- Seus colaboradores, que podem estar preocupados com substituição de tarefas por máquinas ou falta de preparo para trabalhar com IA;
- Órgãos reguladores, que exigem conformidade com leis como a LGPD ou futuras normas específicas de IA;
- Fornecedores e parceiros, que precisam entender como seus dados estão sendo usados;
- E até mesmo a sociedade em geral, especialmente quando a IA afeta serviços públicos, saúde, educação ou decisões sensíveis.

Uma coisa que aprendi ao longo da minha carreira é que, se a organização ignora essas vozes, ela corre sérios riscos – de rejeição, de penalização legal, de boicote do mercado ou, no mínimo, de desenvolver soluções desalinhasadas com a realidade.

Por isso, é importante definir três pontos com muita clareza:

1. Quem são essas partes interessadas relevantes no seu projeto de IA?
2. Quais são os requisitos e preocupações que elas possuem?
3. O que o sistema de gestão de IA vai fazer para atender (ou não) a essas expectativas?

Ah, e não podemos esquecer:

Algumas dessas partes também vão esperar que a IA esteja alinhada com práticas sustentáveis. Sim, até as mudanças climáticas podem entrar nessa conta, especialmente se você estiver desenvolvendo soluções em setores como energia, transporte ou agricultura.

Implementar IA com responsabilidade
significa ouvir, considerar e responder às pessoas que serão direta ou indiretamente impactadas por ela.
Esse é um exercício de empatia estratégica – e também uma exigência da boa governança.

Se você entende quem são os afetados, o que esperam e como sua IA vai responder a isso, está no caminho certo para construir uma Inteligência Viva que cria valor para todos.

Checklist Prático – Etapa 1 – Identificação das Partes Interessadas

Preencha a tabela com os principais públicos que estão diretamente ou indiretamente envolvidos com a IA da sua organização.

Grupo ou Pessoa	Tipo de Relação com a IA	Impacto Esperado
Ex: Clientes finais	Usuários dos serviços baseados em IA	Decisões automatizadas, privacidade
Ex: Colaboradores	Operadores ou afetados pela IA interna	Redução de tarefas手工的, requalificação
Ex: Reguladores	Fiscalizam ou criam normas	Cumprimento legal e ético
Ex: Comunidade local	Potencialmente impactada	Sustentabilidade, imagem da marca

Checklist Prático – Etapa 2 – Levantamento de Requisitos e Expectativas

Liste os desejos, medos, exigências legais ou preocupações que cada parte interessada pode ter em relação ao uso da IA.

Parte Interessada	Expectativas / Requisitos	Tipo (Legal, Ético, Operacional, Socioambiental)
Ex: Clientes	Explicações claras sobre decisões automatizadas	Ético / Legal
Ex: Colaboradores	Treinamento para lidar com novas ferramentas	Operacional
Ex: Órgão regulador	Conformidade com LGPD e normas de IA	Legal
Ex: Sociedade civil	Preocupações com impactos ambientais e sociais	Socioambiental



Checklist Prático – Etapa 3 – Avaliação e Priorização

Avalie a criticidade de cada requisito identificado com base em três critérios:

- **Relevância Legal (L):** Obrigação por lei ou regulamento?
- **Impacto Reputacional (R):** Pode afetar imagem pública ou confiança?
- **Viabilidade de Atendimento (V):** Podemos atender isso de forma prática?

Requisito	L (0-3)	R (0-3)	V (0-3)	Prioridade (L+R+V)
Ex: Explicabilidade para o cliente	3	3	2	4 (Alta)
Ex: Zero impacto ambiental	1	2	1	2 (Média)

Checklist Prático – Etapa 4 – Plano de Atendimento e Acompanhamento

Agora registre o que será feito para atender (ou não) os requisitos e expectativas mapeados.

Requisito / Expectativa	Ação ou Justificativa	Responsável	Status / Prazo
Ex: Transparência algorítmica	Criar política de explicabilidade e canal de dúvidas	Jurídico / TI	Em andamento / 30 dias
Ex: Capacitação interna	Oferecer curso introdutório de IA para equipe	RH / TI	Planejado / 60 dias

Checklist Prático – Etapa 5 – Revisão Periódica

↑

- Periodicidade sugerida: a cada 6 ou 12 meses
- Atualize este checklist sempre que:
 - Novas partes interessadas surgirem;
 - Mudanças no projeto ou na IA ocorrerem;
 - Novas legislações forem aprovadas.



Escopo de IA

“Até onde vocês querem ir com a IA?”

Isso pode parecer uma pergunta filosófica, mas, na verdade, é muito prática. Antes de começar a implementar ferramentas, criar políticas ou envolver especialistas, é fundamental saber o que está dentro e o que está fora do sistema de gestão de IA.

Essa definição tem nome: **escopo**.

O que é o escopo, afinal?

É como traçar o “mapa da área” que queremos cuidar.

Definir o escopo é dizer claramente:

- Onde vamos aplicar a inteligência artificial;
- Quais áreas, departamentos ou projetos estão envolvidos;
- Que tipos de decisões serão automatizadas ou auxiliadas;
- E até quais tecnologias ou fornecedores farão parte disso.

Esse limite é importante porque nem toda IA da organização precisa, obrigatoriamente, estar dentro do sistema de governança logo de início.

Às vezes começamos pequeno — por um chatbot, uma ferramenta de análise de dados ou um algoritmo de recomendação — e, aos poucos, vamos expandindo.

Mas atenção: definir escopo não é excluir responsabilidades.

É priorizar, organizar e garantir que o que está sendo gerido esteja sendo gerido com qualidade.

Dica de Paulo Carvalho:

“Não tente abraçar tudo de uma vez. Comece pequeno, com clareza, e vá ampliando à medida que a maturidade da organização cresce.”

“Um escopo bem definido é o primeiro passo para um uso consciente, seguro e eficiente da inteligência artificial.”

— Paulo Carvalho

Exemplos simples de escopo:

- “Nosso sistema de gestão de IA, nesta fase, vai se aplicar apenas ao algoritmo de análise de crédito que usamos na área financeira.”
- “Vamos incluir todos os sistemas de IA que tomam decisões automatizadas sobre clientes.”
- “Nesta primeira etapa, vamos cuidar apenas dos projetos de IA desenvolvidos internamente.”

Por que isso é tão importante?

Porque um escopo bem definido evita confusão, retrabalho e risco desnecessário.

Ajuda a equipe a entender quem é responsável por quê, quais normas precisam ser seguidas e o que precisa ser monitorado.

E mais: isso ajuda até a conversar melhor com autoridades reguladoras, com os clientes e com os próprios colaboradores. Transparência começa por saber exatamente o que estamos fazendo com a IA.

MODELO DE ESCOPO - Sistema de Gestão de IA

Inspirado em práticas de grandes empresas como Google e OpenAI
Por Paulo Carvalho

Título do Documento:

Definição do Escopo do Sistema de Gestão de Inteligência Artificial – Versão 1.0

1. Propósito do Escopo

Este escopo estabelece os limites e a aplicabilidade do Sistema de Gestão de IA da organização, considerando os princípios éticos, legais e técnicos exigidos para o uso responsável de inteligência artificial.

2. Nome da Organização:

Exemplo: OpenAI Brasil Ltda.

3. Escopo Declarado

O Sistema de Gestão de IA (SGIA) da OpenAI Brasil Ltda. se aplica a:

- Desenvolvimento, treinamento, validação e operação de modelos de linguagem generativos (ex: GPT);
- Integração de IA em produtos como assistentes virtuais, motores de busca, e aplicativos de produtividade;
- Processamento de dados para personalização de respostas e interação com o usuário;
- Projetos internos de pesquisa que utilizem IA generativa, aprendizado profundo (Deep Learning) e modelos de transformadores;
- Operações de monitoramento, ajuste e atualização de algoritmos que influenciem decisões automatizadas ou assistidas no relacionamento com usuários;
- Aplicações com impacto direto em segurança, confiabilidade e explicabilidade algorítmica.

4. Exclusões (se houver)

O escopo não cobre, nesta fase:

- Serviços de IA desenvolvidos por terceiros e integrados por meio de APIs externas sem customização algorítmica;
- Projetos experimentais não lançados comercialmente;
- Algoritmos utilizados apenas para pesquisa acadêmica sem impacto direto em produtos finais.

5. Unidades Organizacionais Incluídas

- Laboratório de Pesquisa e Desenvolvimento de Modelos de IA
- Equipe de Engenharia de Produto (para integração de IA)
- Time de Segurança e Governança de Dados
 - Departamento Jurídico (responsável pela adequação legal dos sistemas de IA)
 - Suporte Técnico e Atendimento com Assistência Automatizada

6. Papéis e Responsabilidades no Escopo

Papel na IA	Responsável	Exemplo
Desenvolvedor	Equipe de Engenharia de IA	Treinamento do GPT
Fornecedor	Produto OpenAI	Plataforma ChatGPT
Usuário Interno	Time de atendimento	Uso de IA para respostas rápidas
Sujeito de IA	Usuário final	Seus dados alimentam os modelos
Responsável legal	Departamento jurídico	Adequação à LGPD e PL 2358

7. Integração com Outros Sistemas de Gestão

O SGIA está alinhado com os seguintes sistemas complementares da organização:

- Sistema de Gestão de Segurança da Informação (SGSI – ISO/IEC 27001)
- Programa de Privacidade e Proteção de Dados (conforme LGPD)
- Políticas internas de ética e uso responsável de tecnologia

8. Aprovação e Validação

Nome.	Cargo	Data	Assinatura
Paulo Carvalho. Consultor Estratégico.	Directoria Técnica. OpenAI Brasil	2/03/2025. 22/03/2025.	Assinatura Assinatura Assinatura



02

LIDERANÇA ISO 42.001



Se tem uma coisa que aprendi nesses anos de jornada com tecnologia e transformação digital é que nenhuma iniciativa de inteligência artificial vai para frente sem o apoio genuíno da liderança.

Não basta comprar ferramentas, contratar especialistas ou montar uma equipe de TI. Quando falamos em gestão de IA com responsabilidade, o envolvimento da alta direção precisa ser real, visível e constante.



O papel da liderança na gestão da IA

Nenhuma iniciativa de inteligência artificial vai para frente sem o apoio genuíno da liderança.

Não basta comprar ferramentas, contratar especialistas ou montar uma equipe de TI. Quando falamos em gestão de IA com responsabilidade, o envolvimento da alta direção precisa ser real, visível e constante.

E como isso acontece na prática? Vou te contar como oriento meus clientes e como aplico isso nos projetos que lidero:

1. Começa pelo propósito

A liderança precisa ajudar a definir com clareza por que a organização está usando IA. Quais são os objetivos? O que queremos melhorar? Esses objetivos precisam estar conectados com a estratégia da empresa – não é só seguir uma moda tecnológica.

2. Integração com o dia a dia

Não dá pra tratar IA como um projeto isolado. A liderança deve garantir que as regras, critérios e boas práticas da gestão de IA estejam integradas nos processos do negócio, seja no RH, no atendimento, no marketing, ou onde for.

4. Falar sobre isso (com clareza)

Muitas vezes, as pessoas só levam a sério algo quando a liderança se posiciona claramente. Por isso, quem lidera precisa comunicar a importância da IA responsável, mostrar que isso não é “só TI” – é estratégia, é reputação, é confiança.

5. Apoiar a equipe

Não existe gestão de IA sem envolvimento das pessoas. A liderança deve incentivar todos a contribuírem, seja dando ideias, sinalizando riscos, propondo melhorias. Isso cria um clima de confiança e inovação.

6. Buscar sempre melhorar

Outro ponto-chave é promover a melhoria contínua. Um sistema de gestão de IA nunca está “pronto” – ele precisa ser revisto, ajustado, atualizado com o tempo. A tecnologia evolui, os riscos mudam e as expectativas também.

7. Ser exemplo

Por fim, o mais importante: a liderança precisa dar o exemplo. Criar uma cultura de uso ético, transparente e responsável da IA começa pelos líderes. É isso que inspira e alinha todo o time.

Se você está à frente de uma organização ou liderando um time, saiba que a sua postura em relação à IA será o termômetro da maturidade digital da empresa.

A liderança é o ponto de partida – e muitas vezes, o diferencial entre uma IA que gera valor e uma IA que gera risco.

“A liderança não é apenas sobre decisões técnicas, é sobre valores, exemplo e direção estratégica.

Quando falamos de IA, liderar é humanizar.” –
Paulo Carvalho

Roteiro para Líderes: Implantando a Cultura de Governança de IA na Prática.

Etapa 2 – Posicionamento Estratégico

Objetivo: Tornar claro que a IA é uma prioridade estratégica e não apenas um tema tecnológico.

Ação	Como fazer	Responsável / Prazo
Definir os objetivos da IA alinhados à estratégia da organização	Ex: melhorar atendimento, automatizar análise de dados, reduzir erros operacionais	CEO / Alta Direção Imediato
Inserir “IA responsável” nos discursos e comunicações internas	Reuniões, comunicados, apresentações de resultados	Diretoria Executiva Contínuo
Criar um comitê de governança de IA	Formado por líderes de diferentes áreas (TI, jurídico, RH, negócio)	Alta Direção 30 dias

Etapa 3 – Engajamento e Comunicação

Objetivo: Garantir que todos na organização saibam que IA é importante e entendam seu papel no processo.

Ação	Como fazer	Responsável / Prazo
Criar uma campanha de “IA na prática”	Materiais simples explicando como a IA está sendo usada e com que propósito	RH / Comunicação 30 dias
Promover rodas de conversa ou cafés com IA	Espaços informais para tirar dúvidas, ouvir ideias e falar de ética na IA	Lideranças de área Mensal
Incluir o tema IA nas reuniões de liderança	Atualizações de projetos, riscos e oportunidades	CEO / Gestores Mensal

Etapa 1 – Capacitação e Consciência

Objetivo: Formar líderes e equipes com visão crítica, técnica e ética sobre IA.

Ação	Como fazer	Responsável / Prazo
Treinar lideranças em fundamentos de IA, riscos e legislação	Workshops práticos com linguagem acessível	RH / TI / Consultor 45 dias
Oferecer trilhas de aprendizado contínuo	Cursos curtos, vídeos, leitura guiada com temas como ética algorítmica, LGPD, IA generativa	RH / Parceiros Trimestral



Criando uma Política de IA na Prática

“Antes de implantar tecnologia, é preciso ter clareza de intenção.”



O que é, afinal, uma política de IA?

Na prática, é uma declaração oficial da liderança dizendo:

- Por que estamos usando IA;
- O que esperamos dela;
- Quais são os nossos compromissos éticos, legais e estratégicos;
- E como vamos garantir que a IA esteja sempre sendo bem usada e melhorada com o tempo.

O que eu incluo quando ajudo uma organização a criar essa política?

A política de IA é o ponto de partida da governança inteligente. Ela é o compromisso público da liderança com o uso responsável da tecnologia.

Exemplo prático de trecho de política:

“A [nome da empresa] compromete-se a utilizar sistemas de inteligência artificial de forma ética, transparente, segura e alinhada às legislações vigentes. Nossos projetos de IA visam gerar valor sustentável para a organização e para a sociedade, respeitando a privacidade, os direitos fundamentais e promovendo a melhoria contínua do nosso sistema de gestão.”



Elá precisa fazer sentido para o nosso negócio.

Envolve as atividades relacionadas com o recebimento, armazenamento e distribuição de matérias-primas.



Tem que deixar claro que vamos seguir a lei e agir com responsabilidade.

Ou seja, nos comprometemos a cumprir a LGPD, o Marco Legal da IA no Brasil, regras internacionais, e também a aplicar os princípios da ética digital.



Elá deve servir de base para os objetivos que serão traçados.

Por exemplo: “usar IA para melhorar o atendimento ao cliente sem comprometer a privacidade” pode se transformar em metas e indicadores específicos.



E, claro, precisa prever evolução contínua.

A política não pode ser estática. A IA muda, o mercado muda, a sociedade muda — nossa governança também precisa acompanhar isso.

Como essa política deve ser tratada dentro da empresa?

Elá precisa ser mais do que um arquivo perdido no servidor.

Eu sempre oriento as organizações a:

- Deixar esse documento acessível e documentado (nada de guardar só no jurídico);
- Relacioná-lo com outras políticas existentes, como segurança da informação, ética ou LGPD;
- Comunicar claramente a todos os colaboradores, inclusive com exemplos práticos;
- E quando fizer sentido, compartilhar com parceiros, fornecedores ou o público, especialmente se a IA tiver impacto direto nas pessoas.



Política de Governança de Inteligência Artificial

Inspirada nas práticas da Google, adaptada por Paulo Carvalho para o cenário brasileiro e latino-americano
 Versão 1.1 – Março/2025

POLÍTICA	OBJETIVOS ESTRATÉGICOS	PRINCÍPIOS ÉTICOS E OPERACIONAIS DA IA	ESCOPO DA POLÍTICA	ESTRUTURA DE GOVERNANÇA	CONTROLES E REGRAS	DOCUMENTAÇÃO OBRIGATÓRIA
CAPACIDADE PREDITIVA	CAPACITAÇÃO E CULTURA	COMUNICAÇÃO E ACESSO	REVISÃO E ATUALIZAÇÃO	DECLARAÇÃO DE COMPROMETIMENTO	ANEXOS RECOMENDADOS	



Objetivos Estratégicos da Governança de IA

- Garantir que toda IA usada ou desenvolvida esteja alinhada com os valores organizacionais e objetivos de negócio;
- Promover a transparência, justiça, inclusão e não discriminação nos processos automatizados;
- Assegurar que as soluções de IA respeitem as leis aplicáveis, como a LGPD, o Marco Legal da IA (PL 2.338/2023) e os princípios da ISO/IEC 24001;
- Fortalecer a confiança dos usuários, colaboradores, clientes e sociedade no uso da tecnologia;
- Fomentar uma cultura de inovação ética e melhoria contínua.

3.1. Benefício Social

Toda aplicação de IA deve ter como finalidade melhorar a vida das pessoas, promovendo bem-estar, eficiência, sustentabilidade ou inclusão.

Exemplo prático:

IA usada para priorizar atendimentos médicos emergenciais com base em sintomas relatados — ampliando o acesso à saúde.

3.2. Evitar Vieses e Discriminações Injustas

Modelos devem ser treinados e validados com diversidade de dados e revisões éticas, evitando reforço de preconceitos históricos, sociais ou culturais.

Exemplo prático:

Avaliação prévia para evitar que uma IA de crédito penalize automaticamente moradores de regiões periféricas.

3.3. Segurança e Robustez

Sistemas devem ser testados para resistir a erros, falhas, manipulações e ataques cibernéticos.

Medidas recomendadas:

- Testes de estresse;
- Validação de confiabilidade algorítmica;
- Backups e redundância.

3.4. Transparência e Explicabilidade

Os modelos devem permitir explicação, contestação e rastreabilidade de decisões automatizadas.

Ferramentas sugeridas:

- Dashboards explicativos;
- Log de decisões;
- Canal de dúvidas do usuário.

3.5. Supervisão Humana Significativa

Nenhuma decisão crítica à vida, liberdade ou dignidade humana deve ser totalmente automatizada. Sempre haverá intervenção ou supervisão humana.

Exemplo:

A IA pode sugerir a aprovação de um tratamento médico, mas a decisão final cabe a um profissional humano.

3.6. Privacidade e Proteção de Dados

Todo uso de dados seguirá os princípios da LGPD, incluindo base legal, consentimento, minimização de dados, anonimização e portabilidade.

3.7. Responsabilidade e Accountability

Toda IA usada na organização deve ter um responsável designado, com definição clara de funções e prestação de contas em caso de falhas.



Inspirada nas práticas da Google, adaptada por Paulo Carvalho para o cenário brasileiro e latino-americano
Versão 1.1 – Março/2025

POLÍTICA	OBJETIVOS ESTRATÉGICOS	PRINCÍPIOS ÉTICOS E OPERACIONAIS DA IA	ESCOPO DA POLÍTICA	ESTRUTURA DE GOVERNANÇA	CONTROLES E REGRAS	DOCUMENTAÇÃO OBRIGATÓRIA
	CAPACIDADE PREDITIVA	CAPACITAÇÃO E CULTURA	COMUNICAÇÃO E ACESSO	REVISÃO E ATUALIZAÇÃO	DECLARAÇÃO DE COMPROMETIMENTO	ANEXOS RECOMENDADOS



Escopo da Política

A política se aplica a todos os sistemas de IA que estejam sob o controle direto da organização, incluindo:

- Projetos internos (desenvolvimento próprio);
- Soluções adquiridas de terceiros;
- Produtos integrados com IA (ex: APIs, plataformas em nuvem);
- Algoritmos que influenciem clientes, colaboradores, operações ou decisões automatizadas.

Áreas envolvidas:

TI, Jurídico, RH, Marketing, Atendimento, Produtos, Inovação, Financeiro, Segurança da Informação.



Estrutura de Governança

Papel	Responsabilidade
Alta Direção	Aprovar a política e garantir recursos
Comitê de IA	Avaliar riscos, deliberar diretrizes, monitorar conformidade
TI / Engenharia	Implementar controles técnicos, revisar modelos
Jurídico e Compliance	Verificar aderência à LGPD e legislações aplicáveis
RH / Cultura	Capacitação, alinhamento cultural e comunicação
Auditoria / Riscos	Avaliações periódicas, mitigação de falhas e relatórios



Controles e Regras Operacionais

6.1. Avaliação de Impacto Algorítmico (AIA)

Obrigatoriedade para IA de alto risco, analisando:

- Riscos éticos, sociais e legais;
- Efeitos sobre grupos vulneráveis;
- Transparência, contestabilidade e mitigação de danos.

6.2. Classificação de Sistemas por Nível de Risco

Nível	Tipo de IA	Exemplo	Ação
Alto	Decisões sobre saúde, crédito, justiça, segurança	IA de triagem médica	AIA + Auditoria
Médio	IA com interação direta com usuários	Chatbots com tomada de decisão	Avaliação ética + transparéncia
Baixo	IA interna sem impacto direto	Recomendador de conteúdo interno	Boas práticas mínimas



Documentação Obrigatorária

Todo sistema de IA deve conter:

- Descrição funcional;
- Justificativa de uso;
- Fonte de dados;
- Resultados esperados;
- Riscos identificados;
- Responsável designado;
- Plano de atualização e melhoria.



Inspirada nas práticas da Google, adaptada por Paulo Carvalho para o cenário brasileiro e latino-americano
Versão 1.1 – Março/2025



Capacidade Preditiva

A capacidade preditiva é quando a IA usa dados passados para prever situações futuras. Na governança de IA, isso deve ser feito com transparência, responsabilidade e supervisão humana — principalmente quando afeta pessoas ou decisões críticas.



Capacitação e Cultura

- Todos os colaboradores devem receber capacitação básica em IA responsável;
- Lideranças e áreas técnicas passam por formações específicas sobre ética, privacidade e risco algorítmico.



Comunicação e Acesso

A política será:

- Publicada na intranet;
- Explicada em workshops de onboarding e cultura digital;
- Compartilhada com parceiros estratégicos e stakeholders conforme aplicável.



Revisão e Atualização

- A política será revisada anualmente ou diante de mudanças regulatórias significativas;
- Avaliações serão realizadas por meio de:
 - Indicadores de maturidade de IA;
 - Incidentes reportados;
 - Auditorias internas e externas.



Declaração de Comprometimento da Liderança

A Alta Direção da [Nome da Organização] declara seu comprometimento institucional com esta Política de Governança de IA, promovendo sua aplicação prática, fornecendo os recursos necessários e atuando como exemplo da conduta ética no uso de tecnologias emergentes.



Anexos Recomendados

- Modelo de Avaliação de Impacto Algorítmico (AIA)
- Matriz RACI de Responsabilidade
- Inventário de Sistemas de IA
- Cartilha de Ética Algorítmica
- Plano de Capacitação em IA



Política de Governança de Inteligência Artificial

Empresa: TechNova Digital Solutions Ltda.

Versão: 1.0 – Data de Emissão: Abril/2025

1. Objetivo

Estabelecer diretrizes para o uso responsável, ético e transparente da Inteligência Artificial (IA) dentro da TechNova, promovendo inovação alinhada aos valores organizacionais, à legislação vigente e aos princípios da ISO/IEC 42001.

2. Escopo

Esta política se aplica a todos os sistemas de IA sob controle da organização, incluindo:
Projetos de desenvolvimento interno
Soluções adquiridas de terceiros
APIs e plataformas baseadas em IA
Algoritmos que influenciem decisões internas, clientes ou operações

3. Princípios Orientadores

A IA na TechNova será sempre guiada por:

Benefício Social – Melhorar a vida das pessoas e gerar valor sustentável
Ética e Inclusão – Evitar vieses e discriminações injustas
Segurança e Robustez – Garantir confiabilidade e proteção contra falhas
Transparência e Explicabilidade – Permitir rastreabilidade e contestação de decisões
Supervisão Humana Significativa – Nenhuma decisão crítica será totalmente automatizada
Privacidade e LGPD – Respeito total à proteção de dados
Responsabilidade – Designação clara de responsáveis por cada sistema de IA

4. Instrumentos de Governança

A política será operacionalizada por meio dos seguintes instrumentos:

Modelo de Avaliação de Impacto Algorítmico (AIA)
Matriz RACI de responsabilidades
Inventário de Sistemas de IA
Cartilha de Ética Algorítmica
Plano de Capacitação para colaboradores e lideranças



Política de Governança de Inteligência Artificial

Empresa: TechNova Digital Solutions Ltda.

Versão: 1.0 – Data de Emissão: Abril/2025

5. Capacitação

Todos os colaboradores receberão formação básica sobre IA responsável
Lideranças e áreas técnicas passarão por formações específicas em ética, risco e privacidade

6. Transparéncia e Comunicação

A política será publicada na intranet corporativa

Apresentada em workshops de onboarding e cultura digital

Compartilhada com parceiros e fornecedores estratégicos, conforme aplicável

7. Revisão e Avaliação

A política será revisada anualmente ou sempre que houver alterações legais
ou tecnológicas relevantes

Serão utilizados indicadores de maturidade, incidentes registrados e
auditorias internas e externas como base para avaliação

8. Comprometimento da Alta Direção

A diretoria da TechNova declara seu comprometimento com esta política, promovendo sua
aplicação, disponibilizando recursos necessários e atuando como exemplo de conduta
ética no uso de IA.

Aprovado por:

CEO – TechNova Digital Solutions Ltda.

Diretor de Inovação e Tecnologia

Conselho de Ética Algorítmica



03

PLANEJAMENTO ISO 42.001



Sempre que começo a estruturar um sistema de gestão de inteligência artificial (SGIA) com uma organização, eu explico que o planejamento não começa com tecnologia, mas com uma pergunta muito mais estratégica:

“O que pode dar errado – e o que pode dar muito certo – quando usamos IA?”

Planejar bem não é prever o futuro – é se preparar para agir com inteligência quando ele chegar.

PROLÓGO E
PREFÁCIO

CONTEXTO DE IA

LIDERANÇA

PLANEJAMENTO



Ações para abordar riscos e oportunidades

Como eu encaro o planejamento de IA?



Antes de qualquer coisa, olho para dois elementos-chave:

1. O contexto da organização – tudo aquilo que afeta a empresa internamente e externamente (como falei nas seções anteriores).
2. As necessidades e expectativas das pessoas envolvidas – sejam clientes, parceiros, equipe, ou sociedade.

Com isso em mãos, começo a identificar quais riscos precisamos evitar e quais oportunidades podemos aproveitar ao usar a IA.



O que são “riscos” no mundo da IA?

São coisas que podem dar errado e causar algum impacto negativo – técnico, ético, legal ou reputacional.

Exemplos:

- Um algoritmo que gera viés ou discriminação;
- Uma IA que toma decisões erradas por falhas nos dados (ALUCINAÇÃO);
- O uso de dados pessoais sem o devido cuidado, o que pode violar a LGPD;
- A dependência de um sistema automatizado que pode falhar ou ser invadido.

E o que são “oportunidades”?

São possibilidades de melhorar processos, reduzir custos, aumentar a eficiência, melhorar o atendimento ao cliente e até criar novos modelos de negócio com o apoio da IA.

“Quando tratamos IA com seriedade, não só protegemos a organização, mas também criamos um ambiente mais confiável, seguro e inovador para todos”.



Como defino o que é aceitável ou não?

Eu ajudo a organização a criar critérios claros para diferenciar riscos aceitáveis de riscos inaceitáveis. Para isso, usamos perguntas simples como:

- Esse risco afeta direitos humanos?
- Pode gerar dano à reputação?
- Existe supervisão humana?
- Há impacto legal ou regulatório?



Com base nessas respostas, definimos:

- O que precisa ser monitorado com atenção;
- O que deve ser mitigado ou ajustado;
- E o que não pode ser tolerado de forma alguma.



O que fazemos com esses riscos e oportunidades?

Com tudo mapeado, partimos para a ação:

1. Planejamos como resolver ou minimizar os riscos – com ações técnicas, treinamentos, validações e regras claras.
2. Integraremos essas ações no dia a dia da empresa, nos processos, fluxos, decisões e rotinas.
3. Avaliamos se essas ações estão funcionando, por meio de indicadores, feedbacks e auditorias.



Como eu avalio os riscos de IA de forma prática e contínua

Depois de mapear os riscos e oportunidades (como vimos na etapa anterior), chega o momento de aprofundar a análise. É aqui que começamos a fazer uma avaliação estruturada dos riscos relacionados ao uso da inteligência artificial.

Essa etapa é como montar um radar de navegação: a gente mede a direção, o tamanho e a intensidade das ameaças que podem surgir no caminho da IA.



A avaliação de riscos precisa seguir a estratégia

Sempre reforço que essa avaliação não é feita de forma solta. Ela precisa estar alinhada com a política de IA da empresa e com os objetivos definidos no início do projeto.

Ou seja, se nosso objetivo é usar IA para melhorar a experiência do cliente, os riscos devem ser avaliados considerando o que pode atrapalhar ou comprometer essa meta — como perda de confiança, decisões injustas, vazamentos de dados ou falhas no atendimento automatizado.

O processo tem que ser contínuo e coerente

Um dos maiores erros que vejo nas empresas é fazer avaliação de risco só “para cumprir protocolo”. Avaliação de risco precisa ser um processo vivo, recorrente e confiável, que permita comparar os resultados ao longo do tempo.

Eu ajudo as equipes a criar um modelo de avaliação padronizado, para que os riscos sejam sempre medidos da mesma forma — com critérios claros, objetivos e comparáveis.

Como eu faço essa análise na prática?
Costumo dividir a avaliação de risco em duas grandes perguntas:

O que pode acontecer se esse risco se tornar realidade?

Chamamos isso de consequência. A pergunta aqui é:

Se esse risco ocorrer, quem será afetado e de que forma?

Pode ser:

- A própria organização (financeiramente, legalmente, estrategicamente);
- As pessoas envolvidas (clientes, usuários, colaboradores);
- A sociedade como um todo (ética, reputação, confiança social).

Qual é a chance real desse risco acontecer?

Aqui estamos falando de probabilidade.
A pergunta é:

Esse risco é algo raro, provável ou inevitável?

Com base nessas duas dimensões — impacto e probabilidade — conseguimos calcular o nível de risco (baixo, médio, alto) e criar uma matriz de priorização.

Priorização: onde agir primeiro?

Depois de avaliar, a próxima etapa é comparar os riscos identificados com os critérios que a empresa definiu (lembra da etapa anterior?). Isso nos permite:

- Saber quais riscos precisam de atenção urgente;
- Quais podem ser acompanhados com menor intensidade;
- E quais podem ser aceitos ou postergados com segurança.



Avaliação de Riscos e Oportunidades em IA

1. Identificação do Sistema de IA Avaliado

Campo	Preenchimento
Nome do projeto ou sistema de IA	
Finalidade do uso	
Área responsável	
Nome(s) do(s) responsável(is) técnico(s)	
Data da avaliação	

2. Identificação de Riscos de IA - Liste todos os riscos potenciais associados ao uso do sistema de IA.

Planejar bem não é prever o futuro – é se preparar para agir com inteligência quando ele chegar.

ID	Descrição do Risco	Tipo (Técnico / Ético / Jurídico / Operacional)	Impacto Potencial	Probabilidade	Risco Total (Alto / Médio / Baixo)
R01	Possibilidade de viés discriminatório em decisões automatizadas	Ético	Alto	Média	Alto
R02	Uso indevido de dados pessoais	Jurídico	Alto	Alta	Alto
R03	Falha do sistema em ambiente crítico	Técnico	Médio	Alta	Médio

3. Mapeamento de Oportunidades com IA - Liste todos os riscos potenciais associados ao uso do sistema de IA.

ID	Descrição da Oportunidade	Benefício Esperado	Área Impactada	Nível de Relevância (Alto / Médio / Baixo)
O01	Automatização de respostas a clientes	Redução de tempo e aumento de satisfação	Atendimento	Alto
O02	Análise preditiva de comportamento de compra	Mais vendas e segmentação personalizada	Marketing	Médio

4. Critérios para Aceitação de Risco - Defina o que é aceitável para a organização em termos de risco.

Critério	Nível Aceitável	Observações
Risco jurídico ou de conformidade	Nenhum	Deve ser sempre mitigado
Risco técnico com impacto operacional	Médio ou menor	Pode ser aceito com plano de contingência
Risco ético ou de imagem	Baixo	Monitorado constantemente



Planejamento de Riscos e Oportunidades em IA

5. Ações para Tratamento de Riscos

Risco ID	Ação Planejada	Responsável	Prazo	Status
R01	Revisão do modelo por equipe de diversidade de dados	Equipe de IA	15 dias	Em andamento
R02	Aplicar anonimização e adequar à LGPD	Jurídico / TI	30 dias	Não iniciado

6. Ações para Aproveitamento de Oportunidades

Planejar bem não é prever o futuro – é se preparar para agir com inteligência quando ele chegar.

Oportunidade ID	Ação Planejada	Responsável	Prazo	Status
O01	Integração com sistema de CRM	TI / Atendimento	20 dias	Concluído
O02	Treinamento da equipe de marketing para uso de insights de IA	RH / Marketing	15 dias	Em andamento

7. Indicadores de Monitoramento

Indicador	Meta	Freqüência de Acompanhamento	Responsável
% de riscos com plano de ação implementado	100%	Mensal	Comitê de IA
% de usuários impactados com ganho de eficiência	+25%	Trimestral	Operações
Nº de incidentes relacionados a IA	0	Contínuo	Jurídico / Segurança

8. Registro e Atualização

Última atualização	Próxima revisão prevista	Avaliadores responsáveis
[dd/mm/aaaa]	[dd/mm/aaaa]	[Nomes e áreas]
[dd/mm/aaaa]	[dd/mm/aaaa]	[Nomes e áreas]
[dd/mm/aaaa]	[dd/mm/aaaa]	[Nomes e áreas]

9. Observações Finais

Aqui podem ser adicionadas observações gerais, aprendizados, comentários ou recomendações da equipe avaliadora.



Depois que identificamos, avaliamos e priorizamos os riscos da inteligência artificial — o que fazer com eles?

É exatamente aqui que começa uma das partes mais estratégicas da governança: o tratamento dos riscos.

Porque não basta saber o que pode dar errado. É preciso agir com intenção e estrutura para reduzir os riscos, controlá-los ou, em alguns casos, aceitá-los com responsabilidade.

O que significa “tratar um risco”?

No mundo da IA, tratar um risco significa tomar uma decisão sobre como vamos lidar com aquele possível problema.

A partir da análise anterior, eu ajudo as organizações a escolher a melhor opção de tratamento, que pode ser:

1. Eliminar o risco — desligar ou mudar o sistema que representa ameaça.
2. Mitigar o risco — ajustar, revisar ou criar barreiras para que ele não se concretize.
3. Compartilhar o risco — dividir a responsabilidade com parceiros ou fornecedores.
4. Aceitar o risco — quando ele é considerado baixo e gerenciável.

Como faço isso na prática?

A primeira coisa que faço é revisar todos os controles que já existem na empresa — sejam técnicos, jurídicos, operacionais ou culturais.

Mas não paro por aí.

Sempre consulto uma fonte confiável e robusta de controles de IA: o Anexo A da norma ISO/IEC 42001.

Esse anexo funciona como uma “caixa de ferramentas”: ele traz exemplos de controles prontos para aplicar, como:

- Garantir explicabilidade das decisões algorítmicas;
- Validar o modelo antes do uso em ambiente real;
- Testar a IA com diferentes grupos de usuários para evitar viéses;
- Criar processos de contestação de decisões automatizadas.

E se os controles do Anexo A não forem suficientes?

Isso acontece, principalmente em setores muito específicos. Quando vejo que os riscos levantados exigem mais do que o padrão, oriento a criação de controles complementares, adaptados à realidade da organização — ou a adoção de boas práticas de fontes externas confiáveis (como NIST, UNESCO, OCDE, etc.).

A importância da Declaração de Aplicabilidade

Após escolher os controles certos, eu ajudo a empresa a montar o que chamamos de Declaração de Aplicabilidade.

É como um documento-mestre onde registramos:

- Quais controles vamos aplicar;
- Por que esses controles foram escolhidos;
- E por que não vamos aplicar certos controles (caso não sejam relevantes para aquele contexto).

Esse documento ajuda a manter a transparência e a rastreabilidade — e demonstra que a organização tomou decisões com base em critérios e não por acaso.

O plano de tratamento de riscos

Agora sim, com as opções e os controles escolhidos, montamos um plano de ação claro, que inclui:

- O que será feito para tratar cada risco;
- Quem será responsável;
- Qual o prazo de execução;
- E como será monitorado o sucesso dessas ações.

E quando tudo está pronto?

Antes de colocar em prática, é fundamental que a liderança aprove o plano — tanto as ações quanto os chamados riscos residuais (aqueles que permanecerão mesmo após o tratamento).

Isso mostra maturidade organizacional: não ignoramos o risco, mas sabemos que estamos preparados para lidar com ele se necessário.

Comunicar, documentar e evoluir

Por fim, todo esse processo de tratamento deve ser:

- Formalizado em documentos acessíveis (para consulta futura ou auditoria);
- Comunicado internamente, para que todos saibam o que está sendo feito e por quê;
- E quando necessário, compartilhado com parceiros, reguladores ou stakeholders externos.

Tratar riscos de IA não é apagar incêndios — é construir uma governança sólida, baseada em decisões conscientes e sustentáveis.

E como eu sempre digo:

Governança não é controle excessivo. É liberdade com responsabilidade.



Até aqui, você já percebeu que tratar riscos de IA vai muito além de proteger a tecnologia em si. Trata-se, sobretudo, de proteger pessoas, grupos e sociedades inteiras.

É por isso que, em todo projeto de inteligência artificial que lidero, sempre reservo uma etapa essencial chamada Avaliação de Impacto do Sistema de IA.

Mas o que é essa tal avaliação de impacto?

É uma análise estruturada e consciente que busca responder a uma pergunta simples e poderosa:

“Quem pode ser afetado pelo uso (ou pelo mau uso) dessa IA – e de que forma?”

Não estou falando só de impacto técnico, mas de consequências humanas, sociais e até culturais.

É nesse momento que a organização se olha no espelho e assume sua responsabilidade diante das pessoas.

A IA pode ser brilhante tecnicamente, mas se ela prejudica pessoas ou reforça desigualdades, falhou em seu propósito.

Por isso, essa etapa é o coração humano da governança algorítmica.

Quem pode ser afetado?

- Indivíduos diretamente envolvidos, como clientes, usuários, funcionários;
- Grupos de indivíduos, como comunidades vulneráveis, minorias, ou perfis demográficos;
- A sociedade como um todo, especialmente quando a IA é usada em áreas sensíveis: saúde, educação, segurança, justiça, crédito, entre outras.

E não é só o uso correto que importa...

Na avaliação de impacto, também levo em conta o que chamamos de mau uso previsível. Ou seja, mesmo que a IA seja usada “da forma certa”, é preciso prever como outras pessoas podem usá-la de forma indevida – intencionalmente ou não.

Exemplos:

- Um chatbot que pode ser manipulado para espalhar desinformação;
- Um sistema de vigilância que, se mal configurado, pode invadir a privacidade;
- Um algoritmo de recomendação que favorece conteúdos polarizadores.

A importância do contexto

Essa avaliação nunca é feita no “vácuo técnico”. Sempre levo em conta:

- O contexto técnico (como o sistema foi desenvolvido, testado e implantado);
- O contexto social (quem são os usuários, onde vivem, quais valores prevalecem);
- As leis e normas do país ou região onde a IA será usada (como a LGPD, por exemplo).

E o que fazemos com os resultados?

Os resultados da avaliação de impacto devem ser documentados com clareza, e – quando fizer sentido – compartilhados com as partes interessadas, como clientes, reguladores, órgãos públicos ou até o público em geral.

Essa transparência é um diferencial competitivo e ético.

Integração com a avaliação de riscos

Outro ponto que sempre aplico:

Os impactos identificados aqui devem alimentar diretamente a avaliação de riscos que vimos anteriormente.

Se descobrimos que a IA pode afetar injustamente um grupo específico, isso precisa entrar no radar de riscos com ações corretivas, preventivas e mitigadoras.

Em casos mais críticos...

Em projetos de IA que envolvem segurança, saúde, dados sensíveis ou impactos em grande escala, também é essencial realizar avaliações de impacto específicas, como:

- Avaliação de impacto à privacidade (AIPD – já exigida pela LGPD);
- Avaliação de impacto à segurança pública;
- Avaliação de impacto ético ou ambiental, dependendo do setor.



Template de Avaliação de Impacto Algorítmico (AIA)



Versão 1.0 – Alinhado à ISO 42001 + PL 2.338/2023 + AI Act EU
Autor: IA de Paulo Carvalho – Aplicável a projetos de IA de alto impacto

1. Identificação do Sistema de IA

Campo	Resposta
Nome do sistema	
Objetivo / Finalidade	
Setor de aplicação	
Tipo de IA	() ML () DL () GenAI () Outro: _____
Classificação de risco	() Alto () Médio () Baixo () Inaceitável
Desenvolvimento interno ou terceirizado?	
Nome(s) do(s) responsável(is) técnico(s)	
Versão do algoritmo / modelo	
Data da avaliação	

2. Análise de Riscos Éticos e Sociais

Conclusão da Avaliação

- Classificação final do risco:

Alto | Médio | Baixo

| Inaceitável

- Autorização para operação do sistema:

Aprovado | Aprovado

com ressalvas |

Reprovado

- Próxima revisão:

2.1 Direitos Fundamentais

Questão	Avaliação	Evidência / Observações
Há risco de discriminação (gênero, raça, classe, etc.)?	() Sim () Não	
Pode violar privacidade ou proteção de dados?	() Sim () Não	
Reduz a autonomia humana em decisões críticas?	() Sim () Não	
Pode reforçar desigualdades socioeconômicas?	() Sim () Não	
Afeta grupos vulneráveis? (crianças, idosos, etc.)	() Sim () Não	

3. Transparência e Explicabilidade

Questão	Avaliação	Evidência / Observações
As decisões são compreensíveis para o usuário?	() Sim () Parcialmente () Não	
Existe explicação sobre como a IA chega às decisões?	() Sim () Parcialmente () Não	
O modelo permite contestação e revisão por humanos?	() Sim () Parcialmente () Não	
Existe documentação técnica acessível?	() Sim () Parcialmente () Não	

4. Supervisão e Controle Humano

Questão	Avaliação	Evidência / Observações
O sistema possui checkpoints de validação humana?	() Sim () Parcialmente () Não	
Existe possibilidade de intervenção humana em decisões críticas?	() Sim () Parcialmente () Não	
A supervisão está registrada em políticas formais?	() Sim () Parcialmente () Não	



Template de Avaliação de Impacto Algorítmico (AIA)



Versão 1.0 – Alinhado à ISO 42001 + PL 2.338/2023 + AI Act EU
Autor: IA de Paulo Carvalho – Aplicável a projetos de IA de alto impacto

5. Segurança, Robustez e Proteção de Dados

Questão	Avaliação	Evidência / Observações
O sistema é resiliente a falhas e ataques?	() Sim () Parcialmente () Não	
Há protocolos de proteção de dados (LGPD)?	() Sim () Parcialmente () Não	
Existe controle sobre o uso e reuso de dados sensíveis?	() Sim () Parcialmente () Não	
Algoritmos são auditáveis e testáveis?	() Sim () Parcialmente () Não	

6. Impactos Operacionais e Organizacionais

Questão	Avaliação	Evidência / Observações
Haverá substituição de mão de obra humana?	() Sim () Não	
Existem planos de capacitação e transição?	() Sim () Parcialmente () Não	
O projeto foi validado por comitê ético / multidisciplinar?	() Sim () Parcialmente () Não	

7. Engajamento e Participação dos Stakeholders

Questão	Avaliação	Evidência / Observações
Foram ouvidos usuários, clientes ou sociedade civil?	() Sim () Parcialmente () Não	
Existe canal de feedback e correção contínua?	() Sim () Não	

8. Plano de Mitigação e Ações Corretivas

Risco / Impacto Identificado	Ação Corretiva Proposta	Responsável	Prazo



Objetivos de IA e planejamento para alcançá-los



Como definir objetivos de IA e fazer um bom plano para alcançar esses objetivos

Por que isso é importante?

Para que a inteligência artificial traga benefícios reais, a empresa precisa ter objetivos bem definidos. Não basta só "implantar IA". É preciso saber o que ela deve ajudar a melhorar, como vamos medir isso e quem será responsável.

Esse processo ajuda a manter a IA alinhada com a estratégia, com as leis e com os valores da organização.

O que são os "objetivos de IA"?

São metas que mostram para que serve a IA na empresa.

Exemplos simples:

- Ajudar a prever a demanda por produtos.
- Sugerir metas mais eficazes nos OKRs.
- Automatizar respostas no atendimento ao cliente.
- Reduzir falhas ou retrabalho.

Como devem ser esses objetivos?

"Sem planejamento, a IA é só tecnologia; com planejamento, ela se torna estratégia inteligente e responsável."

Segundo a ISO 42001, os objetivos de IA precisam:

Requisito	Explicação simples
a) Alinhar com a política de IA	Seguir os princípios e regras que a empresa definiu para usar IA.
b) Ser mensuráveis (se possível)	Ter números ou indicadores para ver se estão dando certo.
c) Considerar requisitos legais e internos	Estar de acordo com leis (como AI ACT) e regras da empresa.
d) Ser monitorados	Ser acompanhados com frequência para evitar desvios.
e) Ser comunicados	Todo mundo envolvido deve saber quais são os objetivos.
f) Ser atualizados quando necessário	Ajustar os objetivos se algo mudar (nova lei, nova estratégia, novo risco).
g) Estar documentados	Tudo precisa estar escrito, registrado e acessível em caso de auditoria.

Como planejar para atingir esses objetivos com OKRs?

Usar OKRs (Objectives and Key Results) no planejamento de IA é altamente eficaz porque essa metodologia:

1. Dá direção clara ao uso da IA

Com OKRs, a organização define objetivos estratégicos concretos para a IA — como reduzir erros, melhorar decisões ou aumentar produtividade. Isso evita que a IA seja usada de forma genérica ou apenas "porque é tendência".

2. Mede impacto com resultados-chave

Os KR (Resultados-Chave) tornam o progresso da IA mensurável, como por exemplo:

- % de aumento na precisão das previsões
- Tempo médio de resposta automatizada
- Redução de falhas em processos críticos

Isso facilita auditorias, revisões e a melhoria contínua.

3. Promove alinhamento entre áreas

OKRs ajudam times de TI, jurídico, RH, inovação e negócio a trabalharem em conjunto, pois todos veem claramente como a IA contribui para metas comuns.

4. Facilita a governança e a responsabilidade

Como cada OKR tem responsáveis, prazos e critérios de sucesso, o uso da IA fica documentado, rastreável e auditável — o que é essencial para seguir normas como a ISO/IEC 42001.



Exemplo OKRs para planejamento de IA

Objetivo de IA: Ajudar os gestores a definir metas de desempenho mais realistas com base em dados históricos

KRS	INICIATIVAS	PLANOS DE AÇÃO
<p>“OKRs transformam a IA de experimento técnico em ferramenta estratégica mensurável, ética e colaborativa.”</p> <p>KR 1 – Aumento da assertividade das metas definidas com suporte da IA em 25% no próximo ciclo de OKRs</p>	<p>Integrar modelo preditivo à plataforma XGOAL360 para sugerir metas comparando histórico de desempenho por área.</p>	<p>What (O quê?) Desenvolver e conectar modelo de IA ao XGOAL360 para análise histórica e sugestão de metas</p> <p>Why (Por quê?) Melhorar a qualidade das metas e reduzir erros de superestimação/subestimação</p> <p>Where (Onde?) Plataforma XGOAL360 (ambiente de OKRs)</p> <p>When (Quando?) Início em 01/06 e conclusão até 30/07</p> <p>Who (Quem?) Time de Dados + TI + Líder de Inovação</p> <p>How (Como?) Usando séries temporais, histórico de OKRs e validação com especialistas</p> <p>How much (Quanto?) R\$ 15.000 em horas de desenvolvimento e validação</p>
<p>KR 2 – 90% das metas sugeridas pela IA revisadas e aprovadas por gestores humanos</p>	<p>Criar painel explicativo com justificativa de cada meta sugerida, com base nos dados usados pela IA.</p>	<p>What Criar interface que exiba os dados e lógica usada pela IA para propor cada meta</p> <p>Why Aumentar a confiança dos gestores e garantir supervisão humana significativa</p> <p>Where Tela de metas do sistema XGOAL360</p> <p>When Entre 10/07 e 15/08</p> <p>Who Time de UX + Responsável de IA + Equipe de TI</p> <p>How Usar logs de decisão, dashboards e explicabilidade visual</p> <p>How much R\$ 10.000 (design + desenvolvimento front-end)</p>
<p>KR 3 – Reduzir em 20% a variação entre metas planejadas e resultados reais</p>	<p>Realizar workshop com gestores para avaliar os resultados das metas sugeridas pela IA e ajustar critérios.</p>	<p>What Promover workshop com áreas-piloto para avaliação crítica das metas definidas com IA</p> <p>Why Alinhar expectativas, ajustar parâmetros da IA e fortalecer a tomada de decisão colaborativa</p> <p>Where Auditório / Teams - com participação das áreas-piloto</p> <p>When Entre 01/09 e 10/09</p> <p>Who Comitê de IA + RH + Gestão Estratégica</p> <p>How Apresentação de resultados, discussão em grupos e coleta de sugestões</p> <p>How much R\$ 3.000 (facilitação e apoio operacional)</p>

Planejar o uso da Inteligência Artificial não é apenas uma exigência técnica — é uma prática essencial para garantir que a tecnologia seja usada com propósito, responsabilidade e impacto positivo.

Ao definir objetivos claros, mensuráveis e alinhados com a estratégia da organização, damos à IA um papel útil e seguro dentro do negócio. Utilizar ferramentas como OKRs permite acompanhar resultados reais, ajustar rotas e envolver todos os setores da empresa de forma coordenada.

Mais do que controlar a IA, o planejamento transforma seu uso em vantagem competitiva, ética e sustentável. E tudo começa com uma pergunta simples, mas poderosa: “Por que estamos usando IA, e como saberemos se está funcionando como deveria?” E agora?

Para que esse planejamento saia do papel e se transforme em realidade, é preciso preparar as pessoas, os dados, os sistemas e a cultura organizacional.

No próximo capítulo, vamos explorar o Suporte ao Sistema de Gestão de IA — incluindo capacitação, infraestrutura, documentação e comunicação.

Porque sem estrutura, nenhum plano se sustenta.
Nos vemos lá!



04

SUPORTE ISO 42.001



Um bom planejamento de IA não vale nada se a organização não tiver estrutura para executá-lo. O sucesso de um Sistema de Gestão de IA depende de um alicerce sólido, que envolve

- Pessoas capacitadas e conscientes do que é IA
- Processos bem documentados
- Dados acessíveis, protegidos e de qualidade
- Sistemas preparados para operar com confiabilidade e Comunicação clara e contínua

Este capítulo aborda como a organização deve se preparar para dar suporte real à IA, garantindo que tudo esteja em ordem para auditorias, conformidade e melhoria contínua.

PROLÓGO E
PREFÁCIO

CONTEXTO DE IA

LIDERANÇA

PLANEJAMENTO

SUPORTE



Recursos

Para que a inteligência artificial funcione de forma segura, útil e responsável, não basta só ter boas ideias ou boas intenções. A empresa precisa garantir que existam recursos suficientes para isso acontecer de verdade.

Isso inclui:

- Pessoas capacitadas (com tempo e conhecimento para cuidar da IA)
- Tecnologia adequada (sistemas, servidores, armazenamento, redes)
- Proteção de dados e segurança digital
- Tempo e orçamento para manter e melhorar os sistemas de IA com frequência

IA só dá certo quando tem gente, estrutura e atenção para funcionar do jeito certo.

IA não funciona direto se quem opera, analisa ou decide não souber o que está fazendo. Treinar as pessoas é tão importante quanto programar o sistema.

Conscientização é quando cada pessoa entende o que a IA faz, como ela afeta seu trabalho e por que é importante seguir as regras.

Ou seja, a empresa deve colocar a IA como prioridade real, e não como algo feito “nas horas vagas” ou “só com boa vontade”.

O que isso significa na prática?

Se a empresa quer usar IA para melhorar o atendimento ao cliente, ela precisa, por exemplo:

- Ter alguém responsável por acompanhar os resultados da IA
- Garantir que os dados estejam organizados e protegidos
- Investir em tecnologia e tempo para que tudo funcione bem
- Atualizar os sistemas quando necessário

Competência

Para que a IA funcione bem e com responsabilidade, as pessoas que trabalham com ela precisam estar preparadas. Isso vale tanto para quem desenvolve sistemas, quanto para quem toma decisões usando IA ou cuida da sua governança.

A empresa deve garantir que cada pessoa envolvida:

- 1.Tenha o conhecimento certo para sua função
 - 2.Isto pode vir de cursos, experiências anteriores ou treinamentos internos.
 - 3.Seja treinada, quando necessário
 - 4.Se alguém ainda não tem o conhecimento adequado, a empresa deve oferecer capacitação, mentoria ou até trocar a função da pessoa, se fizer sentido.
 - 5.Tenha sua competência documentada
 - 6.É importante manter registros: certificados, histórico de treinamentos, avaliações, etc.
- Isso serve como evidência em auditórias.

Exemplo prático:

Se uma empresa usa IA para selecionar currículos automaticamente, ela precisa garantir que:

- O time de RH entenda como funciona a IA e seus possíveis viéses;
- Alguém com conhecimento técnico acompanhe o modelo de IA para garantir justiça e precisão;
- Todos os envolvidos passem por treinamento sobre ética, privacidade e uso responsável de IA.

Conscientização

Não adianta só os especialistas entenderem a IA. Todas as pessoas da organização que lidam com a tecnologia, direta ou indiretamente, precisam saber o básico sobre como ela funciona, para que serve e quais são os cuidados envolvidos.

A norma diz que quem trabalha sob o controle da empresa — seja colaborador, parceiro ou terceirizado — deve estar consciente de três coisas principais:

1. A política de IA da empresa

Cada pessoa precisa entender as regras, valores e princípios definidos pela organização para o uso responsável da inteligência artificial.

2. Sua própria contribuição

Cada colaborador deve saber como o seu trabalho impacta no uso da IA. Por exemplo:

- Um operador de atendimento que alimenta o sistema com dados.
- Um analista que valida saídas da IA.
- Um gestor que toma decisões com base em análises automatizadas.

Saber disso aumenta o cuidado e o senso de responsabilidade.

3. O que acontece se as regras não forem seguidas

As pessoas devem entender que usar IA de forma errada ou negligente pode gerar riscos reais, como:

- Falhas de privacidade
- Decisões injustas
- Danos à reputação da empresa

Exemplo prático:

Imagine que a empresa tem uma IA que aprova crédito. Um colaborador do setor de produtos decide alterar um campo de entrada do sistema sem saber que isso afeta a IA. Sem conscientização, ele pode causar rejeições indevidas e até problemas legais com clientes.

Por isso, é importante que todos saibam o papel que desempenham na cadeia de confiança da IA.



Comunicação

Para que o uso da inteligência artificial seja realmente confiável e transparente, a comunicação precisa ser bem feita — tanto dentro da empresa quanto com parceiros, clientes e até com a sociedade, quando necessário.

A norma pede que a organização defina um plano claro de comunicação sobre a IA, que responda a quatro perguntas simples:

Se as pessoas não sabem o que a IA está fazendo, como confiar nela?
Comunicação clara evita ruídos, aumenta a confiança e protege a empresa.

Documentar o que é feito com IA é o que permite aprender com erros, provar que está certo e melhorar com o tempo.

1. O QUE será comunicado?

A empresa deve decidir quais informações precisam ser compartilhadas sobre IA, como:

- A política e as regras de uso da IA;
- Quais sistemas usam IA e com que finalidade;
- Quais são os riscos e benefícios esperados;
- Resultados, mudanças ou incidentes importantes relacionados à IA.

2. QUANDO será comunicado?

Nem tudo precisa ser dito o tempo todo. A empresa deve planejar momentos estratégicos de comunicação, como:

- No lançamento de um novo sistema com IA;
- Em casos de atualização da política de IA;
- Durante campanhas internas de conscientização;
- Após auditorias ou mudanças relevantes.

3. PARA QUEM será comunicado?

É importante definir quem precisa saber do quê:

- Colaboradores de todas as áreas;
- Lideranças e comitês;
- Clientes e usuários finais (em alguns casos);
- Órgãos reguladores ou parceiros estratégicos.

4. COMO será comunicado?

A empresa deve escolher os canais mais adequados para cada público:

- Intranet e e-mails internos;
- Materiais impressos ou vídeos explicativos;
- Reuniões, workshops e treinamentos;
- Relatórios públicos, newsletters ou redes sociais.

Exemplo prático:

Se a empresa lançar uma IA que ajuda no atendimento ao cliente, ela pode:

- Comunicar internamente aos times de marketing e suporte, explicando como funciona e o que muda;
- Avisar os clientes, deixando claro que parte do atendimento é feito por IA;
- Publicar uma nota explicativa sobre como os dados são usados e protegido.

Informação documentada

Para que a gestão da Inteligência Artificial funcione bem e possa ser auditada, tudo o que for importante deve estar registrado. Não basta “achar que está funcionando” — é preciso ter provas, documentos e evidências organizadas.

A ISO pede que o sistema de gestão de IA inclua dois tipos de documentos:

a) Documentos obrigatórios da norma

São os registros que a própria ISO/IEC 42001 exige que a empresa tenha, como:

- Política de IA
- Objetivos de IA
- Inventário dos sistemas com IA
- Avaliações de risco algorítmico
- Plano de melhoria contínua

b) Documentos definidos pela própria empresa

São informações que a organização considera importantes para o bom funcionamento da IA, mesmo que a norma não obrigue. Exemplos:

- Registros de treinamentos internos
- Checklists de validação ética de sistemas
- Minutas de reuniões do comitê de IA
- Logs de decisões automatizadas

Importante:

A quantidade e a complexidade dos documentos podem variar dependendo de:

- Tamanho da empresa
- Tipo de serviço ou produto
- Nível de risco dos sistemas de IA
- Experiência e competência da equipe

Exemplo prático:

Uma startup que usa IA para recomendar produtos pode ter um sistema mais simples, com poucos documentos.

Já um hospital que usa IA para apoiar diagnósticos médicos precisa de registros mais robustos e detalhados, porque os riscos são maiores.



Criação e atualização de informação documentada

Não basta só ter documentos sobre IA — é preciso garantir que eles estejam corretos, organizados e atualizados.

A norma pede que, sempre que um documento novo for criado ou um existente for modificado, a organização siga alguns cuidados básicos:

1. Identificação clara

Cada documento deve ter:

- Um título compreensível
- A data de criação ou revisão
- O nome do autor ou responsável
- Um código de referência, se for o caso

👉 Isso ajuda qualquer pessoa a saber do que se trata o conteúdo e se está usando a versão certa.

2. Formato e meio adequados

A organização deve escolher o formato certo para que os documentos sejam fáceis de acessar e manter, como:

- PDF, Word ou sistema eletrônico interno
- Planilhas, apresentações, gráficos ou dashboards
- Documentos impressos, se necessário

👉 O formato precisa ser compatível com a realidade da empresa e com quem vai usar a informação.

3. Revisão e aprovação

Todo documento deve ser revisado e aprovado por alguém responsável, para garantir que:

- O conteúdo esteja correto
- A linguagem seja adequada
- A informação esteja completa e útil

👉 Isso evita erros que podem causar confusão, retrabalho ou até problemas legais.

Exemplo prático:

A empresa cria um documento com as regras de uso de IA no setor de RH. Para atender à norma, ela:

- Coloca o título “Política de IA no RH”
- Informa que foi criado em 10/09/2025 por Ana Costa, do Jurídico
- Salva em PDF e publica na intranet
- Passa por revisão do Comitê de IA antes de liberar o uso.

Controle de informação documentada

Apenas criar e atualizar documentos sobre IA não é suficiente — a organização precisa controlar esses documentos com cuidado para garantir que:

- a) Eles estejam disponíveis e atualizados

As pessoas certas precisam encontrar o documento certo, no momento certo, em qualquer área da empresa.

- b) Eles estejam seguros e protegidos

Exemplo prático:

A empresa possui um relatório de avaliação de risco algorítmico. Para controlá-lo corretamente, ela:

- Armazena em um drive seguro com acesso restrito
- Marca como “versão 3 – revisada em janeiro de 2025”
- Deixa visível para auditores e gestores, mas só editável pela área técnica
- Define que será guardado por 5 anos e depois arquivado com segurança

É preciso evitar:

- Vazamento de informações sigilosas
- Uso incorreto de documentos desatualizados
- Perda de dados ou alterações sem controle

O que deve ser controlado?

A empresa precisa organizar os seguintes pontos:

Distribuição, acesso e uso

Quem pode ver ou editar cada documento? Onde ele está armazenado? Todos têm acesso fácil e rápido?

Exemplo: Um guia técnico de IA só pode ser editado pelo time de desenvolvimento, mas deve ser visualizado por outras áreas.

Armazenamento e preservação

Os documentos devem estar armazenados com segurança, e sempre legíveis (sem riscos de apagamento ou corrompimento).

Pode ser na nuvem, em servidores internos ou arquivos físicos.

Controle de versões e mudanças

Quando um documento é alterado, deve-se registrar quem mudou, o que foi mudado e quando. Isso evita confusão entre versões antigas e novas.

Retenção e descarte

A organização deve saber por quanto tempo manter certos documentos — e como descartar de forma segura quando não forem mais necessários.

Informação externa também entra na regra

Documentos criados fora da empresa (como manuais de fornecedores ou contratos com soluções de IA) também precisam ser identificados e controlados, se forem importantes para o sistema de gestão de IA.

Exemplo prático:

A empresa possui um relatório de avaliação de risco algorítmico. Para controlá-lo corretamente, ela:

- Armazena em um drive seguro com acesso restrito
- Marca como “versão 3 – revisada em janeiro de 2025”
- Deixa visível para auditores e gestores, mas só editável pela área técnica
- Define que será guardado por 5 anos e depois arquivado com segurança



05

OPERAÇÃO ISO 42.001



Depois que a IA foi planejada, organizada e estruturada, chega a hora de colocar a mão na massa: desenvolver, implementar, usar e acompanhar os sistemas de IA no dia a dia da organização.

A “Operação”, segundo a norma, é o coração do sistema de gestão de IA. É onde tudo acontece de verdade — desde a criação de um algoritmo até seu uso final por colaboradores, clientes ou parceiros.



Planejamento e Controle Operacionais

Depois de definir as regras e objetivos, a empresa precisa garantir que tudo isso seja colocado em prática de forma organizada e controlada. É como sair do “planejar” e partir para o “fazer bem feito”.

A ISO 42001 chama isso de Planejamento e Controle Operacional, e recomenda que a organização:

A fase operacional da IA exige disciplina, controle e vigilância constante. O segredo é transformar os planos em ações – e corrigir rapidamente se algo fugir do esperado.

Avaliar riscos de IA não é opcional – é parte da responsabilidade de quem usa essa tecnologia. E sempre que algo mudar, os riscos mudam junto.

1. Defina os critérios de funcionamento da IA

Antes de começar a usar um sistema de IA, a empresa precisa planejar como ele será desenvolvido, testado, usado e acompanhado, com critérios bem claros.

Exemplo: “Este sistema de IA só será aprovado se acertar pelo menos 90% dos testes de recomendação, sem violar regras de privacidade.”

2. Aplique controles ao longo do ciclo de vida da IA

Esses controles devem ser definidos na fase de planejamento (conforme a seção 6.1.3 da norma) e aplicados durante toda a operação.

Exemplos de controle:

- Revisões técnicas
- Avaliações de impacto
- Acompanhamento de performance
- Auditorias internas

Exemplo: Um sistema de IA usado para triagem de currículos precisa passar por revisões periódicas para checar viés algorítmico e precisão.

3. Monitore os resultados e corrija o que for necessário

A empresa deve acompanhar se os resultados esperados estão sendo atingidos.

Se algo sair fora do planejado, devem ser tomadas ações corretivas, como ajustes no modelo, mudanças no processo ou até suspensão temporária do sistema.

4. Documente as operações

A norma exige que haja informações registradas para mostrar que tudo foi feito corretamente.

Isso dá confiança para a organização, para os usuários e para os auditores.

5. Gerencie mudanças

Mudanças planejadas ou não (como atualizações do sistema ou alterações de dados) devem ser:

- Avaliadas com cuidado
- Ter riscos mapeados
- Ser ajustadas com ações de prevenção, se necessário

Exemplo: Uma mudança nos dados de entrada do sistema deve ser revisada para garantir que não afete a precisão ou gere riscos éticos.

6. Controle fornecedores e terceiros

Se a empresa terceiriza partes do sistema de IA (como desenvolvimento, manutenção, serviços em nuvem ou bases de dados), ela deve garantir que esses parceiros sigam os mesmos critérios de governança e segurança.

Avaliação de riscos de IA

Toda tecnologia traz benefícios – mas também riscos. E com a inteligência artificial, esses riscos precisam ser avaliados com método, cuidado e frequência.

A ISO 42001 exige que a organização avalie os riscos associados aos seus sistemas de IA de forma estruturada e documentada.

Quando fazer a avaliação de riscos?

A avaliação deve ser feita:

1. Regularmente, em intervalos definidos pela própria empresa
2. Sempre que houver mudanças significativas, como:
 3. Atualizações do modelo de IA
 - Mudança nos dados usados
 - Integração com novos sistemas
 - Alteração no público ou na finalidade de uso

Exemplo:

Se um chatbot interno passa a ser usado com clientes, é necessário reavaliar os riscos, pois o contexto e o impacto mudaram.

O que deve ser feito?

- Identificar os possíveis riscos: como vieses, erros, falta de explicabilidade, riscos à privacidade ou reputação.
- Avaliar a gravidade e a probabilidade de ocorrência
- Definir como cada risco será tratado: evitar, reduzir, aceitar ou transferir.
- Revisar ações preventivas ou corretivas já implementadas.

Documentar é obrigatório

A empresa deve guardar os registros de todas as avaliações de risco feitas. Esses documentos servem como:

- Prova de que a empresa cumpre boas práticas
- Base para auditorias
- Histórico para aprender com melhorias ou falhas



Tratamento de risco de IA

Depois de identificar os riscos de um sistema de IA, não basta só saber que eles existem – é preciso agir para lidar com cada um deles de forma responsável.

A norma ISO 42001 chama essa etapa de tratamento de risco. Ela é a resposta prática da organização diante dos perigos que foram identificados nas avaliações anteriores.

Identificar riscos é só o começo. O verdadeiro compromisso com IA responsável é agir, corrigir e acompanhar de perto os resultados.

Avaliar o impacto da IA é entender como ela afeta as pessoas e a sociedade – e não apenas se funciona tecnicamente.

O que é o tratamento de risco?

É o conjunto de ações que a empresa decide tomar para:

- Eliminar o risco (quando possível)
- Reduzir o impacto ou a chance de acontecer
- Aceitar o risco (se for pequeno e controlado)
- Transferir o risco (por exemplo, por meio de seguros ou contratos com fornecedores)

O que a organização precisa fazer?

1. Implementar o plano de ação definido
2. Cada risco mapeado na avaliação deve ter uma resposta prática, já planejada na seção 6.1.3.
3. Verificar se as ações estão funcionando
4. Não basta aplicar uma medida – é preciso acompanhar se ela resolveu ou reduziu o risco como esperado.
5. Ajustar quando necessário
6. Se o risco continuar existindo ou se surgirem novos riscos, o plano deve ser revisto e atualizado com novas estratégias.
7. Documentar tudo
8. Todos os passos – desde a decisão até o resultado – precisam ser registrados. Isso garante:
 9.
 - Transparência
 - Rastreabilidade
 - Base para auditorias e melhorias futuras

Exemplo prático:

A IA de uma seguradora começou a apresentar indícios de viés contra mulheres ao calcular valores de apólice.

Tratamento aplicado:

- Reforço na diversidade do conjunto de dados
- Inclusão de revisões humanas antes da decisão final
- Treinamento da equipe para entender o viés

Resultado:

O sistema melhorou, mas parte do problema continuava. A seguradora então atualizou o plano, trocando o modelo e adicionando métricas de justiça algorítmica.

Avaliação de Impacto do Sistema de IA

Além de avaliar os riscos técnicos, a organização também precisa analisar os impactos sociais, éticos, legais e organizacionais de seus sistemas de Inteligência Artificial.

Essa análise é chamada de Avaliação de Impacto do Sistema de IA e deve ser feita com método e responsabilidade.

Quando a avaliação deve ser feita?

A empresa deve conduzir essa avaliação:

1. Periodicamente, de acordo com a frequência definida internamente
2. Sempre que houver mudanças importantes, como:
 - Novo uso do sistema de IA
 - Mudança de público ou local de aplicação
 - Atualização de algoritmos ou fontes de dados

O que é avaliado?

A organização deve analisar como a IA pode afetar pessoas, processos e direitos fundamentais.

Exemplos de impacto:

- Privacidade de dados
- Possível discriminação ou exclusão de grupos
- Influência em decisões humanas sensíveis
- Consequências reputacionais ou legais

O que deve ser feito?

- Identificar os possíveis impactos positivos e negativos da IA
- Avaliar a gravidade desses impactos (com base em critérios definidos)
- Propor ações para reduzir impactos negativos
- Registrar todas as informações em documentos oficiais

Exemplo prático:

Uma escola decide usar IA para monitorar o comportamento de alunos por câmeras.

Avaliação de impacto identificou:

- Risco à privacidade dos estudantes
- Possível aumento de ansiedade por sensação de vigilância constante
- Sensibilidade por envolver menores de idade

Ações propostas:

- Ajuste nos horários e locais monitorados
- Comunicação com pais e responsáveis
- Supervisão humana obrigatória



06

AVALIAÇÃO DE DESEMPENHO ISO 42.001



Depois de colocar um sistema de IA para funcionar, a organização precisa acompanhar seu desempenho regularmente para garantir que ele está:

- Alinhado com os objetivos definidos
- Atendendo aos critérios de qualidade e ética
- Livre de falhas, desvios ou riscos emergentes

Essa etapa é chamada de avaliação de desempenho do sistema de IA — e é uma peça essencial da gestão responsável



Monitoramento, Medição, Análise e Avaliação (versão simplificada)

Você não pode melhorar o que não consegue medir.

Por isso, a norma ISO 42001 exige que a organização acompanhe de forma sistemática o desempenho de seus sistemas de IA, coletando dados reais sobre como eles estão se comportando.

Medir, monitorar e analisar é a chave para manter a IA funcionando bem e com confiança.

Um sistema de gestão de IA só é eficaz se ele for acompanhado de perto, com dados reais e decisões rápidas.

Auditória interna é o "check-up" do sistema de IA.
Serve para garantir que tudo esteja em conformidade, funcionando bem e sendo melhorado continuamente.

O que deve ser feito?

A empresa deve definir com clareza:

O que será monitorado e medido

Exemplos:

- Precisão do modelo
- Tempo de resposta
- Incidentes de viés ou erro
- Reclamações de usuários
- Aderência aos objetivos de IA

Como os dados serão coletados e analisados

Ou seja, quais métodos, métricas e ferramentas serão utilizados para garantir dados confiáveis.

Com que frequência isso será feito

A organização precisa definir se as medições serão:

- Diárias?
- Semanais?
- Após cada ciclo de uso?
- Sempre que houver mudanças no modelo?

Quando e como os dados serão analisados e avaliados

Isso garante que os números sirvam para tomar decisões concretas — como melhorar, corrigir ou até suspender o uso de determinada IA.

Tudo precisa ser registrado

A empresa deve manter evidências documentadas de todo esse processo. Esses registros ajudam:

- A comprovar conformidade em auditorias
- A identificar padrões de falha ou sucesso
- A melhorar continuamente o sistema

Exemplo prático:

Uma empresa de transporte usa IA para otimizar rotas de entrega.

Ela define que irá:

- Medir o tempo médio de entrega (meta: até 40 minutos)
- Avaliar as rotas geradas pela IA a cada semana
- Registrar se houve reclamações ou atrasos
- Ajustar o modelo se o tempo médio subir acima de 50 minutos por mais de 3 dias consecutivos

Auditoria interna

Não basta só planejar, executar e monitorar o uso da Inteligência Artificial. Para garantir que tudo esteja realmente funcionando conforme o esperado, a organização precisa realizar auditorias internas do seu sistema de gestão de IA.

O que são essas auditorias?

São verificações feitas dentro da própria organização, de forma periódica e planejada, para responder a duas perguntas principais:

O sistema de gestão de IA está em conformidade com:

- As regras e objetivos definidos pela própria empresa?
- Os requisitos da norma ISO/IEC 42001?

O sistema de IA está sendo bem mantido e operado com eficácia?

Como as auditorias devem ser feitas?

A empresa precisa:

- Definir um cronograma regular (ex: semestral, anual ou por projeto)
- Ter auditores com conhecimento técnico e ético
- Avaliar documentos, indicadores, controles e registros
- Emitir relatórios claros com achados e recomendações
- Acompanhar ações corretivas, se algo não estiver conforme

E a documentação?

Os resultados das auditorias devem ser registrados, servindo como evidência de conformidade e aprendizado contínuo. Esses relatórios também ajudam na preparação para auditorias externas ou certificações.

Exemplo prático:

Uma empresa faz auditorias internas trimestrais para verificar:

- Se as atualizações nos modelos de IA foram documentadas
- Se os riscos foram reavaliados após uma mudança nos dados
- Se os indicadores de viés ou erro estão dentro do aceitável
- Se os treinamentos obrigatórios sobre IA responsável foram realizados

Programa de Auditoria Interna

Auditar é importante — mas precisa ser feito com planejamento, método e imparcialidade.

A ISO 42001 exige que as organizações mantenham um programa de auditoria interna estruturado, que verifique se a gestão de IA está realmente funcionando como deveria.



Análise crítica pela direção

Um bom programa de auditoria interna de IA não é feito em cima da hora – ele é planejado, registrado e executado com critério, garantindo a melhoria contínua da governança algorítmica.

A IA muda rápido. Para garantir que tudo continue no caminho certo, a liderança precisa revisar o sistema com regularidade e responsabilidade.

O que é o programa de auditoria?

É um plano que define como, quando e por quem as auditorias internas de IA serão feitas, incluindo:

- Frequência (ex: mensal, semestral, anual)
- Métodos usados (checklists, entrevistas, amostragens, testes)
- Quem audita quem (garantindo independência e isenção)
- Como os resultados são registrados e compartilhados.

O que o programa precisa ter?

1. Objetivos claros
2. O que você quer verificar com essa auditoria?
3. Ex: conformidade legal, desempenho do sistema, risco ético.
4. Critérios definidos
5. Baseados na ISO 42001, nas políticas da organização e nos objetivos de IA.
6. Escopo bem estabelecido
7. O que será auditado – um projeto, uma área, um sistema ou processo específico.
8. Seleção de auditores imparciais
9. Os auditores devem ser capacitados e não podem auditir seu próprio trabalho.
10. Registro e comunicação dos resultados
11. Os achados devem ser reportados à liderança e às áreas responsáveis.

E quanto à documentação?

A organização precisa manter:

- O plano de auditorias
- As evidências de execução (checklists, relatórios, registros)
- As ações corretivas resultantes

Esses documentos são essenciais para mostrar transparência, melhoria contínua e conformidade com a norma.

Exemplo prático:

Uma startup de tecnologia planeja:

- Auditorias internas semestrais para avaliar todos os sistemas de IA em produção
- Auditorias extraordinárias sempre que houver falha ética ou incidente técnico
- Escopo rotativo, priorizando sistemas com maior impacto social ou regulatório
- Auditores externos contratados para projetos sensíveis (como IA aplicada à saúde)

A liderança não pode apenas aprovar um sistema de gestão de IA e esquecer-lo.

De tempos em tempos, a alta direção precisa parar e olhar com atenção para o sistema, fazendo uma análise crítica completa para garantir que ele ainda esteja:

- **Apto:** continua fazendo sentido para a empresa?
- **Adequado:** está alinhado com os objetivos e valores da organização?
- **Eficaz:** está dando os resultados esperados?

O que é essa análise crítica?

É uma reunião estratégica, feita em intervalos planejados (por exemplo, a cada 6 ou 12 meses), em que a alta liderança:

1. Revisa o funcionamento do sistema de IA
2. Analisa indicadores, riscos, melhorias e não conformidades
3. Decide ajustes, investimentos ou mudanças de direção

Por que isso é importante?

Porque as tecnologias, os contextos e os riscos mudam com rapidez.

A análise crítica garante que:

- A empresa esteja atualizada
- A IA continue alinhada com os objetivos do negócio
- A confiança nos sistemas seja mantida
- A conformidade com leis e normas (como a ISO 42001) seja preservada

E a documentação?

Essa reunião de análise crítica deve ser registrada em ata ou relatório, com:

- Data e participantes
- Itens analisados
- Decisões tomadas
- Ações futuras planejadas

Exemplo prático:

Uma empresa de varejo faz reuniões trimestrais com a alta direção para revisar:

- O desempenho do algoritmo de recomendação de produtos
- Os incidentes registrados envolvendo uso indevido de dados
- A atualização das diretrizes éticas de IA
- As sugestões de melhoria dos times técnicos e jurídicos

Com base nisso, a liderança decide:

- Investir em novo treinamento da equipe
- Ajustar o modelo para maior diversidade nas recomendações
- Iniciar um processo de auditoria externa



Entradas da análise crítica pela direção

Antes de revisar o sistema de gestão de IA, a alta direção precisa saber o que olhar.

A norma ISO 42001 define claramente quais informações devem ser levadas para essa reunião estratégica. Esses dados são chamados de entradas da análise crítica — e são fundamentais para decisões bem embasadas.

A alta direção só pode tomar boas decisões se tiver os dados certos na mesa.
As entradas da análise crítica garantem que o sistema de gestão de IA seja avaliado com base em evidências reais, atualizadas e relevantes.

O que deve ser levado para a reunião?

A direção deve receber e considerar:

a) Status das ações anteriores

- O que foi decidido na última análise crítica?
- O que já foi feito? O que ainda está pendente?

b) Mudanças no cenário externo e interno

- Leis ou normas novas (ex: LGPD, PL 2338/2023)
- Novas tecnologias, concorrentes ou demandas do mercado
- Mudanças internas na empresa que impactam a IA (ex: reestruturações, mudanças de equipe)

c) Mudança nas expectativas das partes interessadas

- Clientes, reguladores, sociedade, investidores...
- O que essas partes esperam da IA hoje que não esperavam antes?

d) Informações sobre o desempenho da IA

- Resultados do monitoramento e dos indicadores
- Não conformidades e ações corretivas realizadas
- Conclusões das auditorias internas ou externas
- Incidentes, reclamações, erros, falhas, etc.

e) Oportunidades de melhoria

- O que pode ser ajustado ou otimizado?
- Onde a IA pode ser mais ética, eficiente ou útil?

Exemplo prático:

Antes da reunião de análise crítica, a equipe técnica reúne:

- Um relatório das ações prometidas na última reunião
- Mudanças na regulação de IA aprovadas pelo Senado
- Feedback de clientes sobre uso excessivo de dados pessoais
- Um painel de indicadores que mostra queda na precisão do algoritmo de crédito
- Uma proposta de nova capacitação para os times de TI e jurídico

Essas informações permitem que a alta direção tome decisões com clareza e visão estratégica.

Resultados da análise crítica pela direção

Depois de avaliar todos os dados e informações (as chamadas entradas), a alta direção precisa decidir o que fazer a seguir.

Essas decisões e conclusões são chamadas de resultados da análise crítica — e são o principal produto da reunião.

O que a direção deve decidir?

Com base nas informações discutidas, a liderança precisa definir:

Melhorias a serem feitas

- O que pode ser ajustado para que a IA funcione melhor?
- Como tornar o sistema mais eficiente, ético ou confiável?

Mudanças no sistema de gestão de IA

- É preciso revisar políticas, indicadores ou processos?
- Alguns novos controles devem ser implementados?
- Há necessidade de treinamento, investimento ou correção?

Registro obrigatório

Tudo o que for decidido precisa ser documentado. Esse registro:

- Serve como evidência de conformidade com a ISO 42001
- Garante o acompanhamento de ações corretivas e melhorias
- Dá continuidade e histórico à governança de IA

Exemplo prático:

Após revisar os dados da operação de IA de atendimento automatizado, a alta direção decide:

- Substituir o modelo atual por um mais transparente
- Atualizar os critérios de privacidade da política de IA
- Criar um plano de capacitação em ética algorítmica para todo o time de tecnologia
- Incluir novas métricas de satisfação do cliente na avaliação trimestral

Todas essas decisões são registradas em ata, com prazos, responsáveis e metas.



07

MELHORIA ISO 42.001



A melhoria no sistema de gestão de IA garante que a tecnologia evolua com segurança, corrigindo falhas, prevenindo riscos e promovendo ajustes contínuos. É um processo essencial para manter a IA alinhada aos objetivos da organização, às leis e aos valores éticos.



Não Conformidade e Ação Corretiva

Quando algo sai errado no sistema de IA – como um erro, falha, ou violação de política – isso é chamado de não conformidade.

A organização deve:

1. Corrigir o problema imediatamente, se possível;
2. Analisar por que ele aconteceu e se pode acontecer de novo;
3. Implementar ações para evitar que se repita;
4. Avaliar se a correção funcionou mesmo;
5. Atualizar o sistema de gestão de IA, se necessário.

O Relatório de Não Conformidade e Ação Corretiva documenta falhas no sistema de IA, suas causas, correções e ações preventivas. Ele garante que o problema seja resolvido e não se repita, promovendo melhoria contínua e conformidade com a ISO 42001.

Tudo isso precisa ser registrado – tanto o que foi feito quanto os resultados obtidos.

Exemplo prático:

Um chatbot de atendimento usou termos considerados discriminatórios em uma resposta.

A equipe:

- Corrigiu o erro e suspendeu o uso do modelo;
- Analisou que faltava uma etapa de validação ética nos testes;
- Implementou uma nova checagem antes da publicação de modelos;
- Verificou se o mesmo risco existe em outros canais automatizados.

Relatório de Não Conformidade e Ação Corretiva – ISO/IEC 42001

Este relatório tem como objetivo registrar, analisar e tratar falhas ou desvios identificados no sistema de gestão de inteligência artificial (SGIA) de uma organização. É um instrumento essencial para garantir a melhoria contínua, transparência e conformidade com normas técnicas e éticas.

Estrutura do Relatório:

1. Identificação da Não Conformidade

- Data da ocorrência
- Área ou projeto envolvido
- Descrição detalhada do que ocorreu, onde e como a falha foi detectada

2. Ações Imediatas

- Medidas de contenção e correção aplicadas de forma emergencial
- Quem executou e qual o resultado

3. Análise de Causa

- Investigação das causas da não conformidade
- Identificação de falhas em processos, dados, treinamentos, decisões, etc.

E4. Avaliação de Riscos e Ocorrências Similares

- Análise de possibilidade de ocorrência em outros sistemas
- Avaliação do impacto e da gravidade do desvio identificado

5. Ações Corretivas

- Ações específicas para eliminar a causa da não conformidade
- Indicação de responsáveis e prazos definidos para cada ação

6. Verificação da Eficácia

- Como será medida a eficácia das ações implementadas
- Quais indicadores ou métodos de validação serão utilizados

7. Atualizações no Sistema de Gestão de IA

- Necessidade de ajustar políticas, procedimentos, controles ou treinamentos
- Detalhamento das alterações a serem feitas

8. Registro e Aprovação

- Nome do responsável pela elaboração do relatório
- Assinatura da liderança ou área responsável pela aprovação
- Data de conclusão

Exemplos de Observações na Seção de Melhoria:

- Aprendizado extraído:
- “A situação evidenciou a necessidade de validar dados externos antes de alimentar o modelo de IA.”
- Sugestão para prevenção futura:
- “Recomenda-se revisar trimestralmente os critérios de entrada do algoritmo, mesmo em modelos já aprovados.”
- Mudança estrutural:
- “A partir desta ocorrência, será incluída uma etapa obrigatória de verificação ética nos ciclos de atualização do modelo.”
- Boas práticas identificadas:
- “O tempo de resposta da equipe foi eficiente, o que minimizou o impacto. Essa agilidade será incorporada ao plano de resposta padrão.”
- Reforço cultural:
- “A falha reforçou a importância de manter todos os times informados sobre os riscos do uso de IA sem supervisão.”

Essas observações são especialmente úteis para o auditor ou gestor que deseja ir além do “cumprimento de obrigação” e construir um sistema de IA mais maduro, ético e confiável.



08

CONTROLES A.2

Política



Políticas Relacionadas à IA da ISO/IEC 42001 orienta que a organização crie uma política formal para o desenvolvimento e uso responsável de sistemas de IA, alinhada à sua estratégia, cultura, valores e apetite ao risco. A política deve considerar requisitos legais, impactos nas partes interessadas e fazer referência cruzada com outras políticas, como privacidade, segurança e qualidade. Deve ser analisada criticamente de forma periódica e atualizada sempre que necessário, garantindo sua eficácia contínua. Essa política é essencial para guiar decisões e práticas responsáveis ao longo de todo o ciclo de vida da IA.



As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.2 Políticas relacionadas à IA

Objetivo: Fornecer orientação à gestão e suporte aos sistemas de IA de acordo com os requisitos de negócios.

CÓDIGO	TEMA	CONTROLE	KPIs
A.2.2	Política de IA	A organização deve documentar uma política para o desenvolvimento ou uso de sistemas de IA.	<p>KPI: Cobertura da Política de IA na Organização</p> <p>Descrição: Mede o percentual de áreas, unidades ou projetos que possuem a política de IA formalmente implementada e acessível.</p> <p>Fórmula: $(\text{Número de áreas com política de IA documentada} / \text{Total de áreas relevantes}) \times 100$</p> <p>Meta sugerida: 100%</p> <p>Frequência de medição: Trimestral</p> <p>Fonte: inventário de áreas, registros de distribuição da política, auditorias internas, atas de comitês e sistemas de governança (GRC/LMS).</p> <p>Responsável: Área de Governança de IA ou Compliance Digital</p>
A.2.3	Alinhamento com outras políticas organizacionais	A organização deve determinar a maneira como outras políticas podem ser afetadas ou aplicadas aos objetivos organizacionais relacionados com os sistemas de IA.	<p>KPI: Integração de Políticas Organizacionais com IA</p> <p>Descrição: Mede o grau de análise e integração das políticas internas (ex: segurança da informação, ética, LGPD, compliance) com os objetivos e riscos dos sistemas de IA.</p> <p>Fórmula: $(\text{Número de políticas revisadas com foco em IA} / \text{Total de políticas organizacionais aplicáveis}) \times 100$</p> <p>Meta sugerida: ≥ 90%</p> <p>Frequência de medição: Semestral</p> <p>Fonte: registros de revisão normativa, atas de comitês, matriz de mapeamento de políticas aplicáveis e documentos de integração com diretrizes de IA.</p> <p>Responsável: Governança Corporativa ou Comitê de IA</p>
A.2.4	Análise crítica da política de IA	A política de IA deve ser analisada criticamente em intervalos planejados, ou conforme for necessário, de maneira a garantir aptidão, adequação e eficácia contínuas.	<p>KPI: Frequência de Revisão da Política de IA</p> <p>Descrição: Avalia se a política de IA está sendo revista periodicamente, conforme o cronograma definido, garantindo sua relevância e eficácia contínuas.</p> <p>Fórmula: $(\text{Número de revisões realizadas dentro do prazo} / \text{Número de revisões planejadas no período}) \times 100$</p> <p>Meta sugerida: 100%</p> <p>Frequência de medição: Anual ou conforme definido na política</p> <p>Responsável: Comitê de Governança de IA ou Compliance Digital</p>



A.2 Políticas relacionadas à IA

As orientações para implementação documentadas neste Anexo referem-se aos controles apresentados na Tabela A.1. Este Anexo fornece informações para apoiar a implementação dos controles apresentados na Tabela A.1 e para atender ao objetivo do controle, mas as organizações não precisam documentar ou justificar a inclusão ou exclusão de orientação para implementação na declaração de aplicabilidade (ver 6.1.3).

A orientação para implementação nem sempre é adequada ou suficiente em todas as situações, bem como nem sempre atende aos requisitos de controle específicos da organização. A organização pode estender ou modificar uma orientação ou definir sua própria orientação para implementação de um controle de acordo com seus requisitos específicos e necessidades de tratamento de risco.

Este Anexo deve ser utilizado como orientação para determinar e implementar controles para o tratamento de riscos de IA no sistema de gestão de IA definido neste documento. Os controles organizacionais e técnicos adicionais que não os incluídos neste Anexo podem ser determinados (ver tratamento de riscos no sistema de gestão de IA em 6.1.3). Este Anexo pode ser considerado um ponto de partida para o desenvolvimento de implementação de controles específicos da organização.

A.2 Objetivo

Fornecer direção e suporte da gestão para sistemas de IA de acordo com os requisitos do negócio.

A.2.1 Política de IA

Controle

Convém que a organização documente a política para o desenvolvimento ou uso de sistemas de IA.

A.2.2 Orientações para implementação

Convém que a política de IA seja informada por:

- estratégia de negócio;
- valores e cultura organizacional e quantidade de riscos que a organização está disposta a perseguir ou reter;
- nível de risco representado pelos sistemas de IA;
- requisitos legais, incluindo os por força de contrato;
- ambiente de risco da organização;
- impacto para as partes interessadas relevantes (ver 6.1.4).

Convém que a política de IA inclua (além dos requisitos de 5.2):

- princípios que norteiem todas as atividades da organização relacionadas à IA;
- processos de tratamento de desvios e exceções à política.

Convém que políticas pertinentes orientem o desenvolvimento, a compra, a operação e o uso de sistemas de IA.

A.2.3 Alinhamento com outras políticas organizacionais

Controle

Convém que a organização determine onde outras políticas podem ser afetadas ou aplicadas a objetivos em relação aos sistemas de IA.

Orientações para implementação

Muitos domínios se cruzam com a IA, incluindo qualidade, segurança, segurança física e privacidade. Convém que a organização considere uma análise completa para determinar se e onde as políticas atuais podem necessariamente se cruzar e atualize essas políticas se as atualizações forem necessárias ou inclua provisões na política de IA.

Outras informações

Convém que as políticas que o órgão direutivo define em nome da organização mencionem a política de IA. A ABNT NBR ISO/IEC 38507 fornece orientações para que os membros do órgão direutivo de uma organização habilitem e governem o sistema de IA durante todo o seu ciclo de vida.

A.2.4 Análise crítica da política de IA

Controle

Convém que a política de IA seja analisada criticamente a intervalos planejados ou adicionalmente, conforme necessário, para assegurar sua continua aptidão, adequação e eficácia.

Orientações para implementação

Convém que um papel aprovado pela direção seja responsável pelo desenvolvimento, análise crítica e avaliação da política de IA ou dos componentes nela contidos. Convém que a análise crítica inclua a avaliação de oportunidades de melhoria das políticas e da abordagem da organização para gerenciar sistemas de IA em resposta a mudanças no ambiente organizacional, circunstâncias de negócios, condições legais ou ambiente técnico.

Convém que a análise crítica da política de IA considere os resultados das análises críticas pela direção.

Estudo de Caso: Criação e Implementação da Política de IA na empresa FinData Solutions

Perfil da empresa:

A FinData Solutions é uma empresa de médio porte que oferece soluções de análise de crédito e risco para instituições financeiras. Em 2023, a empresa começou a usar modelos de IA para automatizar a análise de perfil de clientes e prever inadimplência.

Desafio:

Com a introdução da IA, surgiram dúvidas internas sobre responsabilidade, critérios éticos e riscos legais. A liderança percebeu que não havia diretrizes claras sobre como os algoritmos deveriam ser usados ou revisados, o que poderia comprometer a confiança de clientes e reguladores.

Ação: Criação da Política de IA

A empresa decidiu elaborar uma Política de IA conforme as orientações da ISO/IEC 42001. O processo foi conduzido em etapas:

1. Alinhamento estratégico

- A liderança definiu que a IA deveria aumentar a eficiência, mas sem comprometer princípios éticos, como a não discriminação.
- Decidiu-se que o uso de IA não poderia influenciar decisões críticas sem supervisão humana.

2. Conteúdo da Política

- Princípios: transparência, justiça, explicabilidade e privacidade.
- Escopo: todos os sistemas de IA usados para crédito, atendimento e prevenção a fraudes.
- Responsáveis: equipe de governança de TI e jurídico.
- Avaliações de impacto obrigatórias para modelos novos.
- Integração com políticas de LGPD e compliance.

3. Revisão de políticas correlatas

- A política de segurança da informação e de proteção de dados foi atualizada para mencionar o uso de IA.
- O código de ética passou a incluir diretrizes para desenvolvimento de algoritmos justos.

4. Revisão e atualização

- A política foi publicada na intranet, com um cronograma de revisão anual ou sempre que houvesse mudanças regulatórias relevantes.

Resultados:

- A empresa passou a registrar todos os modelos de IA em um inventário centralizado, incluindo seu objetivo, riscos e responsáveis.
- Durante uma auditoria de conformidade com a LGPD, a empresa apresentou a política e seus controles, reduzindo o risco regulatório.
- Foi criado um painel com KPIs, como:
 - “% de modelos com avaliação de impacto concluída”;
 - “% de colaboradores capacitados em IA responsável”.

Lições aprendidas:

- Ter uma política de IA clara reduziu o risco de decisões automatizadas discriminatórias.
- O processo aumentou o alinhamento entre áreas técnicas e jurídicas.
- A política serviu de base para novos projetos com IA generativa, mantendo coerência com os valores da empresa.



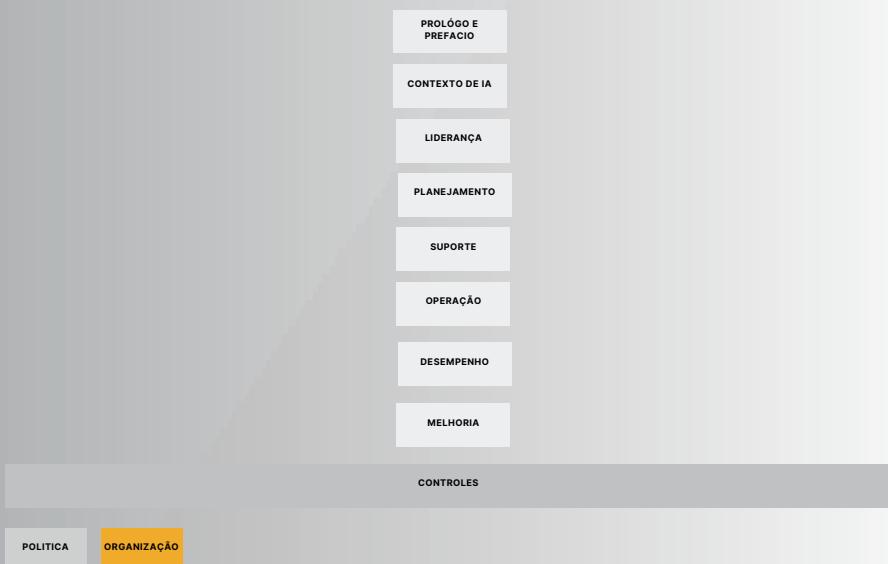
08

CONTROLES A.3

Organização Interna



Organização Interna da ISO/IEC 42001 trata da estrutura interna necessária para garantir o uso responsável da inteligência artificial. A organização deve definir e atribuir claramente papéis e responsabilidades relacionados à IA, cobrindo áreas como risco, privacidade, supervisão humana e qualidade dos dados. Também deve implementar mecanismos de relato de preocupações, assegurando anonimato, proteção contra retaliações e resposta adequada. Essa estrutura fortalece a governança, assegura responsabilização e permite uma atuação coordenada durante todo o ciclo de vida dos sistemas de IA.



As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.3 Organização interna			
Objetivo: Estabelecer responsabilização dentro da organização para manter sua abordagem responsável pela implementação, operação e gestão de sistemas de IA.			
CÓDIGO	TEMA	CONTROLE	KPIs
A.3.2	Papéis e responsabilidades da IA	Os papéis e responsabilidades da IA devem ser definidos e alocados de acordo com as necessidades da organização.	<p>KPI: % de papéis e responsabilidades de IA formalmente definidos e atribuídos</p> <p>Descrição: Mede o percentual de funções diretamente envolvidas com IA que possuem papéis documentados, aprovados e com responsáveis designados.</p> <p>Fórmula: (Número de papéis e responsabilidades definidos para sistemas de IA : Total de papéis necessários identificados) x 100</p> <p>Meta recomendada: ≥ 95%</p> <p>Frequência de medição: Trimestral</p> <p>Fonte de dados: Matriz RACI, organograma de IA, documentos de governança, atas de designação formal.</p> <p>Responsável: Escritório de Governança de IA ou área de Compliance/Projetos Estratégicos</p>
A.3.3	Relato de preocupações	A organização deve definir e alocar um processo para os funcionários da organização relatarem preocupações sobre o papel da organização em relação ao sistema de IA ao longo de seu ciclo de vida.	<p>KPI: Canal de Relato Ativo para Preocupações com IA</p> <p>Descrição: Mede a existência, uso e cobertura de um processo formal para que os funcionários possam relatar preocupações sobre o papel da organização no ciclo de vida dos sistemas de IA.</p> <p>Fórmula: (Número de canais ativos e acessíveis de relato de IA + nº de relatos processados) ÷ (Total de áreas com uso de IA) Obs: Pode ser adaptado para percentual de áreas com canal de relato funcional.</p> <p>Meta sugerida: 100% das áreas com IA devem ter canal funcional e ao menos 1 relatório validado por semestre.</p> <p>Frequência de Medição: Semestral</p> <p>Fonte de Dados: Relatórios do canal de ética, ouvidoria, HelpDesk técnico de IA, sistema de GRC, atas do comitê de IA.</p> <p>Responsável: Comitê de Ética Digital ou Governança Corporativa</p>



A.3 Organização interna

A.3.1 Geral

Objetivo

Estabelecer responsabilização dentro da organização para manter sua abordagem responsável pela implementação, operação e gestão de sistemas de IA.

A.3.2 Papéis e responsabilidades da IA

Controle

Convém que os papéis e responsabilidades da IA sejam definidos e alocados de acordo com as necessidades da organização.

Orientações para implementação

Definir papéis e responsabilidades é fundamental para assegurar a responsabilização de toda organização por seu papel em relação ao sistema de IA ao longo do seu ciclo de vida. Convém que a organização considere as políticas e os objetivos de IA, e identifique riscos ao atribuir papéis e responsabilidades, a fim de assegurar que todas as áreas pertinentes sejam contempladas.

A organização pode priorizar como os papéis e as responsabilidades são atribuídos. Exemplos de áreas que podem requerer papéis e responsabilidades definidos podem incluir:

- gestão de riscos;
- avaliações de impacto do sistema de IA;
- gestão de ativos e recursos;
- segurança;
- segurança física;
- privacidade;
- desenvolvimento;
- desempenho;
- supervisão humana;
- relações com fornecedores;
- demonstração de sua capacidade para cumprir de forma coerente os requisitos legais;
- gestão da qualidade dos dados (durante todo o ciclo de vida).

Convém que as responsabilidades dos vários papéis sejam definidas ao nível adequado para o(s) indivíduo(s) desempenhar(em) as suas funções.

A.3.3 Relato de preocupações

Controle

Convém que a organização defina e coloque em prática um processo para o relato de preocupações sobre o papel da organização em relação a um sistema de IA ao longo de seu ciclo de vida.

Orientações para implementação

Convém que o mecanismo de comunicação de informações desempenhe as seguintes funções:

- a) forneça opções de confidencialidade ou anonimato, ou ambas;
- b) seja disponível e promovido a empregados e contratados;
- c) conte com pessoal qualificado;
- d) estipule poderes adequados de investigação e resolução para as pessoas referidas na alínea c);
- e) forneça mecanismos para reportar e escalar casos à direção em tempo hábil;
- f) forneça uma proteção eficaz contra represálias, tanto para as pessoas envolvidas na denúncia como na investigação (por exemplo, permitindo que as denúncias sejam feitas de forma anônima e confidencial);
- g) forneça relatórios de acordo com 4.4 e, se for o caso, com a alínea e), mantendo a confidencialidade e anonimato da alínea a) e respeitando considerações gerais de confidencialidade de negócios;
- h) forneça mecanismos de resposta dentro de um prazo apropriado.

NOTA A organização pode utilizar os mecanismos de relato existentes como parte desse processo.

Estudo de Caso – Responsabilização e Relato de Preocupações sobre IA na empresa LogiChainTech

Cenário da Empresa:

A LogiChainTech é uma empresa brasileira de médio porte especializada em soluções logísticas com uso intensivo de IA, especialmente para roteirização dinâmica e previsão de demandas. A empresa adotou a ISO/IEC 42001 como referência para implantar um Sistema de Gestão de IA.

Desafio Identificado:

Com a expansão do uso de IA em suas operações, surgiram preocupações internas sobre:

- Falta de clareza nas responsabilidades dos times técnicos e de negócio.
- Ausência de um canal estruturado para relatar riscos éticos ou operacionais com os algoritmos.
- Necessidade de demonstração de conformidade com LGPD e outras normas regulatórias aplicáveis.

Soluções Implementadas:

1. Definição de Papéis de IA

- A LogiChainTech criou um Comitê de Governança de IA, com representantes de TI, Jurídico, RH, Qualidade, Inovação e Dados.
- Papéis foram formalmente definidos:
 - Owner de Algoritmo: responsável técnico e legal por cada modelo em produção.
 - Gestor de Risco de IA: monitora os riscos operacionais e éticos.
 - Auditor de IA Interno: avalia o cumprimento dos controles da ISO 42001 e da LGPD.

2. Criação de um Canal de Relato Seguro

- Implementado um canal de denúncia confidencial, via intranet, para relatar problemas com o uso de IA (ex: viés algorítmico, falhas operacionais ou privacidade).
- O canal:
 - Garante anonimato do denunciante.
 - Tem responsável independente (Compliance Digital).
 - Fornece retorno em até 15 dias úteis.
 - É divulgado em onboarding, cartilhas e workshops de IA responsável.

3. Capacitação e Monitoramento

- Todos os líderes passaram por formação em ética algorítmica e papéis da ISO 42001.
- O canal é monitorado trimestralmente e os relatos são apresentados anonimamente ao comitê de IA e à direção.

Resultados:

- 100% dos sistemas de IA da empresa têm responsáveis alocados.
- 85% dos colaboradores sabem como relatar uma preocupação com IA (medido por pesquisa interna).
- Dois relatos levaram à ajuste no modelo de decisão de crédito para transportadoras, reduzindo vieses e aumentando a transparência.

Lição Aprendida:

Sem papéis claros e sem escuta ativa, os riscos de IA se escondem. A LogiChainTech demonstrou que um sistema robusto de responsabilização e relato é chave para a governança ética e confiável da inteligência artificial.



08

CONTROLES A.4

Recursos para os sistemas de IA



Recursos para os Sistemas de IA da ISO/IEC 42001 orienta que a organização identifique, documente e disponibilize os recursos necessários para o desenvolvimento, operação e gestão contínua de sistemas de IA. Isso inclui dados, ferramentas, infraestrutura computacional e recursos humanos com competências adequadas. A gestão adequada desses recursos deve ser feita ao longo de todo o ciclo de vida do sistema de IA, garantindo robustez, confiabilidade e alinhamento com os objetivos organizacionais e requisitos legais.



CONTROLES

POLÍTICA

ORGANIZAÇÃO

RECURSOS

As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.4 Recursos para os sistemas de IA			
Objetivo: Assegurar que a organização se responsabilize pelos recursos (incluindo os componentes e ativos do sistema de IA), a fim de compreender completamente			
CÓDIGO	TEMA	CONTROLE	KPIs
A.4.2	Documentação de recursos	<p>A organização deve identificar e documentar os recursos pertinentes necessários para as atividades em determinados estágios do ciclo de vida do sistema de IA e outras atividades relacionadas à IA relevantes para a organização.</p>	<p>KPI: Mapeamento de Recursos de IA por Estágio do Ciclo de Vida</p> <p>Nome: Cobertura de Recursos em Projetos de IA</p> <p>Descrição: Mede o percentual de projetos de IA que possuem mapeamento completo de recursos (humanos, tecnológicos, financeiros, dados) documentado por estágio do ciclo de vida (desenvolvimento, validação, operação, monitoramento, etc.).</p> <p>Fórmula: $(\text{Número de projetos de IA com recursos mapeados} / \text{Total de projetos ativos de IA}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Freqüência de medição: Trimestral</p> <p>Responsável: PMO de IA ou Governança de IA</p> <p>Fonte de dados: Planilhas de gestão de projetos, sistema de gerenciamento de portfólio (PPM), repositório de documentação de IA</p>
A.4.3	Recursos de dados	<p>Como parte da identificação de recursos, a organização deve documentar informações sobre os recursos de dados utilizados para o sistema de IA</p>	<p>KPI: Documentação dos Recursos de Dados Utilizados na IA</p> <p>Nome: Percentual de Projetos com Dados de Treinamento Documentados</p> <p>Descrição: Mede quantos projetos de IA possuem documentação completa dos recursos de dados utilizados (origem, tipo, volume, sensibilidade, licença e uso pretendido).</p> <p>Fórmula: $(\text{Número de projetos com documentação de dados validada} / \text{Total de projetos de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Freqüência de medição: Trimestral</p> <p>Responsável: Responsável por Governança de Dados ou CDO (Chief Data Officer)</p> <p>Fonte de dados: Repositório de documentação técnica, sistema de governança de dados, relatórios de conformidade de IA</p>
A.4.4	Recursos de ferramentas	<p>Como parte da identificação de recursos, a organização deve documentar informações sobre os recursos de ferramentas utilizados para o sistema de IA.</p>	<p>KPI: Documentação de Ferramentas Utilizadas na IA</p> <p>Descrição: Mede a proporção de projetos de IA que possuem documentação completa e atualizada das ferramentas utilizadas (como bibliotecas, frameworks, APIs, plataformas de desenvolvimento e execução).</p> <p>Fórmula: $(\text{Número de projetos com documentação completa de ferramentas} / \text{Total de projetos de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Freqüência de medição: Trimestral</p> <p>Responsável: Equipe de Engenharia de IA ou Arquitetura de Soluções</p> <p>Fonte de dados: Inventário técnico de sistemas de IA, repositórios de código, relatórios de conformidade ou governança de IA</p>



Tabela A.1 – Objetivos de controle e controles

A.4 Recursos para os sistemas de IA			
Objetivo: Assegurar que a organização se responsabilize pelos recursos (incluindo os componentes e ativos do sistema de IA), a fim de compreender completamente			
CÓDIGO	TEMA	CONTROLE	KPIs
A.4.5	Sistema e recursos computacionais	Como parte da identificação de recursos, a organização deve documentar as informações sobre o sistema e os recursos computacionais utilizados para o sistema de IA.	<p>KPI: Documentação de Infraestrutura Computacional para IA</p> <p>Descrição: Avalia a proporção de sistemas de IA com documentação técnica completa sobre infraestrutura utilizada (como servidores, GPUs, serviços em nuvem, requisitos de memória e processamento).</p> <p>Fórmula: $(\text{Número de sistemas de IA com infraestrutura documentada} / \text{Total de sistemas de IA em produção}) \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Área de Infraestrutura de TI ou Arquitetura de Sistemas</p> <p>Fonte de dados: Inventário de infraestrutura, relatórios técnicos de sistemas, repositórios de documentação de projeto</p>
A.4.6	Recursos humanos	Como parte da identificação de recursos, a organização deve documentar informações sobre os recursos humanos e suas competências utilizadas no desenvolvimento, implantação, operação, gestão de mudança, manutenção, verificação e integração do sistema de IA. transferência e decomissionamento, bem como na verificação e integração do sistema de IA.	<p>KPI: Documentação de Competências dos Recursos Humanos em IA</p> <p>Descrição: Mede o percentual de sistemas de IA cuja equipe envolvida tem competências e responsabilidades formalmente documentadas em todas as fases do ciclo de vida (desenvolvimento, operação, manutenção etc.).</p> <p>Fórmula: $(\text{Número de projetos de IA com competências da equipe documentadas} / \text{Total de projetos de IA em operação}) \times 100$</p> <p>Meta sugerida: $\geq 85\%$</p> <p>Frequência de medição: Semestral</p> <p>Responsável: Recursos Humanos / Governança de IA / Gestão de Projetos</p> <p>Fonte de dados: Planos de projeto, matriz de competências, RACI, dossiês técnicos de equipe</p>



A.4 Recursos para os sistemas de IA

A.4.1 Geral

A.4.1.1 Objetivo

Assegurar que a organização contabilize os recursos (incluindo componentes e ativos do sistema de IA), a fim de compreender e abordar completamente os riscos e impactos.

A.4.2 Documentação de recursos

Controle

Convém que a organização identifique e documente os recursos relevantes necessários para as atividades em determinados estágios do ciclo de vida do sistema de IA e outras atividades relacionadas à IA relevantes para a organização.

Orientações para implementação

A documentação dos recursos do sistema de IA é fundamental para entender os riscos, bem como os potenciais impactos do sistema de IA (positivos e negativos) para indivíduos ou grupos de indivíduos, ou ambos, e para as sociedades. A documentação de tais recursos (que pode utilizar, por exemplo, diagramas de fluxo de dados ou diagramas de arquitetura de sistema) pode informar as avaliações de impacto do sistema de IA (ver B.5).

Os recursos podem incluir, mas não estão limitados a:

- componentes do sistema de IA;
- recursos de dados, isto é, dados utilizados em qualquer fase do ciclo de vida do sistema de IA;
- recursos de ferramentas (por exemplo, algoritmos, modelos ou ferramentas de IA);
- recursos de sistema e computação (por exemplo, hardware para desenvolver e executar modelos de IA, armazenamento de dados e recursos de ferramentas);
- recursos humanos, ou seja, pessoas com a expertise necessária (por exemplo, para o desenvolvimento, vendas, treinamento, operação e manutenção do sistema de IA) em relação ao papel da organização durante todo o ciclo de vida do sistema de IA.

Os recursos podem ser fornecidos pela própria organização, por seus clientes ou por terceiros.

Outras informações

A documentação de recursos também pode ajudar a determinar se os recursos estão disponíveis e, se não estiverem, convém que a organização revise a especificação do projeto do sistema de IA ou seus requisitos de implantação.

A.4.3 Recursos de dados

Controle

Como parte da identificação de recursos, convém que a organização documente informações sobre os recursos de dados utilizados para o sistema de IA.

Orientações para implementação

Convém que a documentação sobre dados inclua, mas não se limite a, os seguintes tópicos:

- proveniência dos dados;
- data em que os dados foram atualizados ou modificados pela última vez (por exemplo, etiqueta de data nos metadados);
- categorias de dados, para o aprendizado de máquina (por exemplo, dados de treinamento, validação, teste e produção);
- categorias de dados (por exemplo, como definido na ISO/IEC 19944-1);
- processo de rotulagem dos dados;
- utilização prevista dos dados;
- qualidade dos dados (por exemplo, como descrito na série ISO/IEC 52592);
- políticas aplicáveis de retenção e descarte de dados;
- questões de viés conhecidas ou potenciais nos dados;
- preparação de dados

A.4.4 Recursos de ferramentas

Controle

Como parte da identificação de recursos, convém que a organização documente informações sobre os recursos de ferramentas utilizados para o sistema de IA.

Orientações para implementação

Os recursos de ferramentas para um sistema de IA e, particularmente, para o aprendizado de máquina, podem incluir, mas não se limitam a:

- tipos de algoritmos e modelos de aprendizado de máquina;
- ferramentas ou processos de condicionamento de dados;
- métodos de otimização;
- métodos de avaliação;
- ferramentas de provisão de recursos;
- ferramentas de auxílio ao desenvolvimento de modelos;
- software e hardware para projeto, desenvolvimento e implementação de sistemas de IA.

Outras informações

A ISO/IEC 23053 fornece orientação detalhada sobre os tipos, métodos e abordagens para vários recursos de ferramentas para aprendizado de máquina.

B.4.5 Sistemas e recursos computacionais

Controle

Como parte da identificação de recursos, convém que a organização documente informações sobre o sistema e os recursos computacionais utilizados para o sistema de IA.

Orientações para implementação

As informações sobre o sistema e os recursos computacionais para um sistema de IA podem incluir, mas não se limitam a:

- requisitos de recursos do sistema de IA (isto é, para ajudar a assegurar que o sistema possa ser executado em dispositivos de recursos restritos);
- onde o sistema e os recursos computacionais estão localizados (por exemplo, no local, cloud computing ou edge computing);
- recursos de processamento (incluindo rede e armazenamento);
- impacto do hardware usado para executar as cargas de trabalho do sistema de IA (por exemplo, o impacto no ambiente, tanto pelo uso quanto pela fabricação do hardware ou pelo custo da utilização do hardware).

Convém que a organização considere que diferentes recursos podem ser necessários para permitir a melhoria contínua dos sistemas de IA. O desenvolvimento, a implantação e a operação do sistema podem ter diferentes necessidades e requisitos do sistema.



B.4 Recursos para os sistemas de IA

A.4.6 Recursos humanos

Controle

Como parte da identificação de recursos, convém que a organização documente informações sobre os recursos humanos e suas competências utilizados para o desenvolvimento, implantação, operação, gestão de mudanças, manutenção, transferência e descomissionamento, bem como sobre a verificação e integração do sistema de IA.

Orientações para implementação

Convém que a organização considere a necessidade de expertises diversas e inclua os tipos de funções necessárias para o sistema. Por exemplo, a organização pode incluir grupos demográficos específicos relacionados a conjuntos de dados usados para treinar modelos de aprendizado de máquina, se esse for um componente necessário do projeto do sistema. Os recursos humanos necessários podem incluir, mas não se limitam a:

- cientistas de dados;
- papéis relacionados à supervisão humana de sistemas de IA;
- especialistas em tópicos de fidedignidade, como segurança física, segurança e privacidade
- pesquisadores e especialistas em IA e especialistas em domínios relevantes para os sistemas de IA.

Diferentes recursos podem ser necessários em diferentes estágios do ciclo de vida do sistema de IA.

Estudo de Caso – Gestão de Recursos de IA na empresa HealthMind

Contexto:

A HealthMind, empresa de tecnologia em saúde, decidiu implantar um sistema de IA para triagem automatizada de pacientes em unidades de pronto atendimento. Para garantir o uso ético, eficiente e seguro da tecnologia, a organização adotou diretrizes baseadas na ISO/IEC 42001, com foco especial no item B.4 – Recursos para sistemas de IA.

Desafio:

Garantir que todos os recursos — humanos, tecnológicos, computacionais e de dados — estivessem adequadamente identificados, documentados e mantidos ao longo de todo o ciclo de vida do sistema de IA.

Ações Realizadas:

Mapeamento de Recursos Humanos:

A empresa identificou as competências necessárias para desenvolvimento, validação e manutenção da IA.

- Criou uma matriz de competências com perfis como: cientista de dados, auditor de ética, responsável por privacidade e médico validante.

Inventário de Dados:

- Catalogou todas as bases utilizadas, incluindo dados clínicos anonimizados.
- Avaliou qualidade, diversidade e riscos de viés nos dados históricos.

Infraestrutura Computacional:

- Documentou o uso de servidores com GPU, sistema de armazenamento redundante e provedores em nuvem.
- Incluiu requisitos de escalabilidade para suportar picos de acesso em emergências. A HealthMind alcançou um alto nível de transparência e controle sobre seus recursos de IA. Em uma auditoria externa, a empresa foi reconhecida por sua boa prática em governança de IA, inclusive sendo capaz de demonstrar todos os ativos e competências relacionadas ao ciclo de vida do sistema.

Ferramentas de IA:

- Registrhou todas as bibliotecas, frameworks e APIs utilizadas (ex: TensorFlow, scikit-learn).
- Criou um processo de validação de novas ferramentas antes da adoção.

Plano de Atualização e Manutenção:

- Estabeleceu calendário de revisão semestral dos modelos de IA.
- Definiu responsáveis e critérios para descomissionamento ético do sistema, quando necessário.

Resultado:

A HealthMind alcançou um alto nível de transparência e controle sobre seus recursos de IA. Em uma auditoria externa, a empresa foi reconhecida por sua boa prática em governança de IA, inclusive sendo capaz de demonstrar todos os ativos e competências relacionadas ao ciclo de vida do sistema.



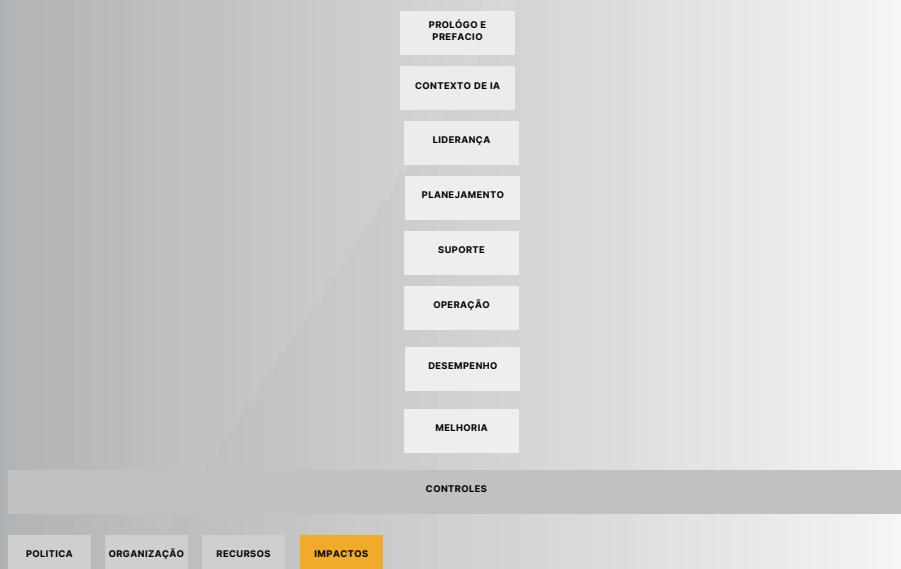
08

CONTROLES A.5

Avaliação dos impactos dos sistemas de IA



Avaliação dos Impactos dos Sistemas de IA da ISO/IEC 42001 orienta que a organização estabeleça um processo para avaliar os possíveis efeitos que seus sistemas de IA podem ter sobre indivíduos, grupos e a sociedade, ao longo de todo o ciclo de vida da tecnologia. Essa avaliação deve considerar fatores como impactos jurídicos, psicológicos, sociais e de direitos humanos, especialmente em contextos críticos ou de alto risco. A organização deve documentar esses impactos e usar os resultados para mitigar riscos, adaptar o projeto da IA e garantir o uso responsável e ético da tecnologia.



As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.5 Avaliação dos impactos dos sistemas de IA			
Objetivo: Avaliar os impactos do sistema de IA em indivíduos ou grupos de indivíduos, ou ambos, e nas sociedades afetadas pelo sistema da IA ao longo de seu ciclo de vida.			
CÓDIGO	TEMA	CONTROLE	KPIs
A.5.2	Processo de avaliação de impacto do sistema de IA	A organização deve avaliar as potenciais consequências para indivíduos ou grupos de indivíduos, ou ambos, e para sociedades, que podem resultar dos sistemas de IA ao longo do seu ciclo de vida.	<p>KPI: Avaliação de Impacto Social e Individual dos Sistemas de IA</p> <p>Descrição: Mede a proporção de sistemas de IA que passaram por avaliação formal das potenciais consequências para indivíduos, grupos ou a sociedade ao longo de seu ciclo de vida.</p> <p>Fórmula: $(\text{Número de sistemas de IA com avaliação de impacto social documentada} / \text{Total de sistemas de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Frequência de medição: Semestral</p> <p>Responsável: Comitê de Ética em IA / Governança Corporativa / Jurídico</p> <p>Fonte de dados: Relatórios de Avaliação de Impacto (AIA), atas de comitês, dossiês de conformidade</p>
A.5.3	Documentação das avaliações de impacto do sistema de IA	A organização deve documentar os resultados das avaliações de impacto do sistema de IA e reter os resultados por um período definido	<p>KPI: Registro de Avaliações de Impacto de IA</p> <p>Descrição: Mede a proporção de avaliações de impacto do sistema de IA que foram formalmente documentadas e armazenadas dentro do período definido pela organização.</p> <p>Fórmula: $(\text{Número de avaliações de impacto documentadas e armazenadas} / \text{Total de avaliações de impacto realizadas}) \times 100$</p> <p>Meta sugerida: 100%</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Área de Governança de IA ou Compliance Digital</p> <p>Fonte de dados: Repositório de documentação de conformidade e banco de dados de avaliações de impacto</p>
A.4.4	Avaliação dos impactos sociais de sistemas de IA	A organização deve avaliar e documentar os potenciais impactos sociais dos seus sistemas de IA ao longo do seu ciclo de vida.	<p>KPI: Avaliação de Impacto Social de Sistemas de IA</p> <p>Nome: Cobertura de Avaliações de Impacto Social de IA</p> <p>Descrição: Mede o percentual de sistemas de IA que passaram por avaliação formal de impacto social, com resultados documentados, ao longo de seu ciclo de vida.</p> <p>Fórmula: $(\text{Número de sistemas de IA com avaliação de impacto social documentada} / \text{Total de sistemas de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Semestral</p> <p>Responsável: Comitê de Ética em IA ou Área de Sustentabilidade e Impacto Social</p> <p>Fonte de dados: Relatórios de avaliação de impacto social, sistema de governança de IA</p>



A.5 Avaliação dos impactos dos sistemas de IA

A.5.1 Geral

A.5.1.1 Objetivo

Avaliar os impactos do sistema de IA para os indivíduos ou grupos de indivíduos, ou ambos, e para as sociedades, afetados pelo sistema de IA ao longo de seu ciclo de vida.

A.5.2 Processo de avaliação de impacto do sistema de IA

Controle

Convém que a organização estabeleça um processo de avaliação das potenciais consequências para os indivíduos ou grupos de indivíduos, ou ambos, e para as sociedades, que resultariam do sistema de IA ao longo de seu ciclo de vida.

orientações para implementação

Como os sistemas de IA potencialmente geram impacto significativo para os indivíduos ou grupos de indivíduos, ou ambos, e para as sociedades, convém que a organização que fornece e utiliza tais sistemas considere o propósito pretendido e o uso desses sistemas, bem como os impactos desses sistemas nesses grupos.

Convém que a organização considere se o sistema de IA afeta:

- a posição jurídica ou as oportunidades de vida dos indivíduos;
- o bem-estar físico ou psicológico dos indivíduos;
- os direitos humanos universais;
- as sociedades.

Convém que os procedimentos da organização incluam, mas não estejam limitados a:

a) circunstâncias nas quais convém que uma avaliação de impacto do sistema de IA seja realizada, que podem incluir, mas não se limitam a:

- 1) criticidade do propósito pretendido e do contexto em que o sistema de IA é usado ou quaisquer mudanças significativas neles;
- 2) complexidade da tecnologia de IA e nível de automação dos sistemas de IA ou quaisquer mudanças significativas neles;
- 3) sensibilidade dos tipos e fontes de dados processados pelo sistema de IA ou quaisquer mudanças significativas nelas;

b) elementos que fazem parte do processo de avaliação de impacto do sistema de IA, que podem incluir:

- 1) identificação (por exemplo, fontes, eventos e resultados);
- 2) análise (por exemplo, consequências e probabilidades);
- 3) avaliação (por exemplo, decisões de aceitação e priorização);
- 4) tratamento (por exemplo, medidas de mitigação);
- 5) documentação, relatórios e comunicação (ver 7.4, 7.5 e B.3.3);

c) quem desempenha a avaliação de impacto do sistema de IA;

d) como a avaliação de impacto do sistema de IA pode ser utilizada (por exemplo, como ela pode informar o projeto ou o uso do sistema (ver B.6 e B.8), se pode desencadear análises críticas e aprovações);

e) indivíduos e sociedades que são potencialmente impactados com base no propósito pretendido do sistema, uso e características (por exemplo, avaliação de indivíduos, grupos de indivíduos ou sociedades).

Convém que a avaliação de impacto considere elementos do sistema de IA, incluindo os dados usados para o desenvolvimento do sistema de IA, das tecnologias de IA usadas e da funcionalidade do sistema geral.

Estudo de Caso – Avaliação de Impacto do Sistema de IA na empresa EduMind

Contexto:

A EduMind, uma edtech brasileira, lançou uma plataforma de tutoria baseada em IA chamada MentorAI, voltada para alunos do ensino médio. O sistema recomenda conteúdos, propõe trilhas de aprendizagem e avalia automaticamente redações. Antes de expandir a plataforma nacionalmente, a empresa decidiu aplicar o processo de avaliação de impacto de IA, conforme diretrizes da ISO/IEC 24001.

Objetivo:

Avaliar possíveis consequências sociais, psicológicas e legais da aplicação da IA no ambiente educacional, garantindo uso responsável e ético da tecnologia.

Etapas Aplicadas:

1. Quando Avalia

A EduMind definiu que avaliações de impacto seriam realizadas:

- Antes da implantação do sistema em novas regiões;
- Ao incluir novas funcionalidades (ex: sugestões de carreira);
- Quando alterasse o tipo de dado utilizado (ex: voz, imagem, sentimentos).

2. O Que Avaliar

O comitê de ética da empresa considerou os seguintes riscos:

- Psicológicos: impacto de recomendações negativas em alunos vulneráveis;
- Sociais: tratamento desigual de alunos de regiões com menor infraestrutura;
- Direitos: uso de dados sem consentimento claro dos responsáveis legais;
- Oportunidades de vida: influência da IA nas escolhas de carreira ou reprovação escolar.

3. Como Avaliar

A equipe multidisciplinar conduziu a avaliação com base em cinco passos:

- Identificação de riscos: coleta de dados históricos e entrevistas com usuários-piloto;
- Análise: simulações com alunos fictícios de perfis variados;
- Avaliação: classificação de riscos por gravidade e probabilidade;
- Tratamento: ajustes no algoritmo, como remover termos que sugerem profissões com base no desempenho apenas;
- Comunicação: relatório enviado ao conselho da empresa, famílias e escolas parceiras.

4. Quem Avaliou

Um comitê de impacto formado por:

- Responsável de IA e segurança de dados;
- Representantes pedagógicos e psicológicos;
- Representante da área jurídica;
- Dois diretores escolares parceiros.

5. Resultado

Após a avaliação, a EduMind:

- Incluiu mensagens motivacionais para alunos com baixo desempenho;
- Reforçou o consentimento dos pais sobre o uso dos dados;
- Ajustou os algoritmos para evitar recomendações enviesadas;
- Criou um canal de escuta de alunos para reportar situações de desconforto com a IA.



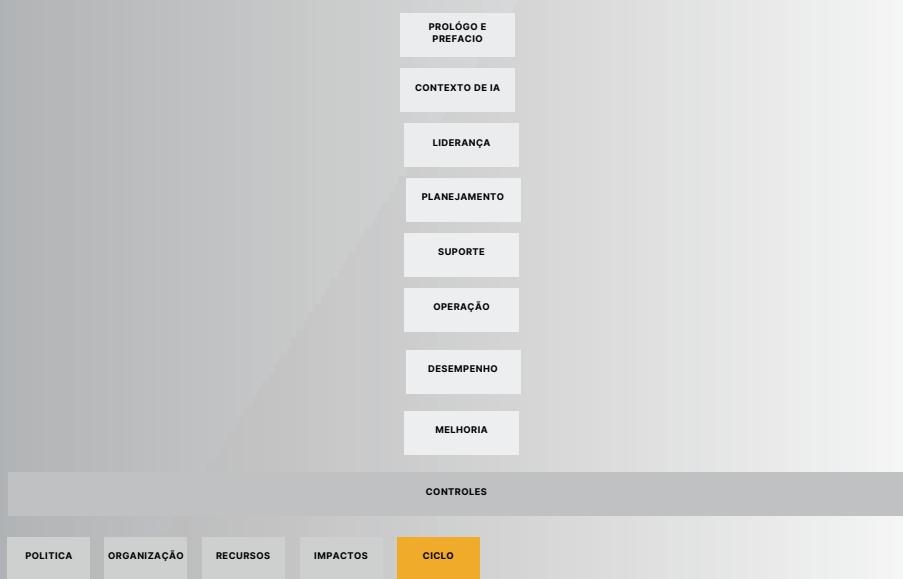
08

CONTROLE A.6

Ciclo de vida do sistema de IA



A seção B.6 – Ciclo de Vida do Sistema de IA da ISO/IEC 42001 trata da necessidade de gerenciar todas as etapas do ciclo de vida dos sistemas de Inteligência Artificial, desde o planejamento, desenvolvimento e implantação até a operação, manutenção, sativação e descarte. A organização deve documentar cada fase e garantir que as decisões e ações sejam alinhadas com seus objetivos éticos, legais e de desempenho. A boa gestão do ciclo de vida permite maior controle sobre riscos, qualidade dos dados, segurança e responsabilidade, promovendo o uso confiável e sustentável da IA.



As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.6.1 Orientações da direção para o desenvolvimento de sistemas de IA			
Objetivo: Assegurar que a organização identifique e documente os objetivos e implemente os processos para o projeto e desenvolvimento responsáveis de sistemas de IA.			
CÓDIGO	TEMA	CONTROLE	KPIs
A.6.1.1	Objetivos para o desenvolvimento responsável de sistemas de IA	<p>A organização deve identificar e documentar os objetivos para orientar o desenvolvimento responsável de sistemas de IA, considerar esses objetivos e integrar as medidas para alcançá-los no ciclo de vida de desenvolvimento.</p>	<p>KPI: Integração de Objetivos de Desenvolvimento Responsável no Ciclo de Vida da IA</p> <p>Descrição: Mede o percentual de projetos de IA que identificaram, documentaram e integraram objetivos de desenvolvimento responsável (ex: ética, inclusão, transparéncia) ao longo de seu ciclo de vida.</p> <p>Fórmula: $(\text{Número de projetos com objetivos de desenvolvimento responsável integrados} / \text{Total de projetos de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Comitê de IA ou Área de Governança de IA</p> <p>Fonte de dados: Inventário de Projetos de IA + Relatórios de Planejamento e Documentação de Projetos</p>
A.6.1.2	Processos para projeto e desenvolvimento responsáveis de sistemas de IA	<p>A organização deve definir e documentar os processos específicos para o projeto e desenvolvimento responsáveis do sistema de IA.</p>	<p>KPI: Documentação de Processos de Desenvolvimento Responsável de IA</p> <p>Descrição: Mede o percentual de projetos de IA que seguem processos formalmente definidos e documentados para desenvolvimento responsável, conforme critérios éticos, legais e técnicos estabelecidos.</p> <p>Fórmula: $(\text{Número de projetos de IA com processos de desenvolvimento responsável documentados} / \text{Total de projetos de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Área de Engenharia de IA ou Governança de IA</p> <p>Fonte de dados: Repositório de documentação técnica e planos de projeto de IA</p>



Tabela A.1 – Objetivos de controle e controles

A.6.2 Ciclo de vida do sistema de IA			
Objetivo: Definir os critérios e requisitos para cada estágio do ciclo de vida do sistema de IA.			
CÓDIGO	TEMA	CONTROLE	KPIs
A.6.2.1	Requisitos e especificações do sistema de IA	A organização deve especificar e documentar os requisitos para novos sistemas de IA ou melhorias materiais para os sistemas existentes.	<p>KPI: Especificação Documentada de Requisitos de IA</p> <p>Descrição: Mede o percentual de novos sistemas de IA ou atualizações significativas que possuem requisitos documentados de forma clara, abrangente e alinhada aos objetivos organizacionais.</p> <p>Fórmula: $(\text{Número de projetos de IA com requisitos documentados} / \text{Total de novos projetos ou melhorias materiais}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Mensal ou por ciclo de projeto</p> <p>Responsável: Escritório de Projetos de IA ou Engenharia de Produto/Desenvolvimento</p> <p>Fonte de dados:</p> <ul style="list-style-type: none"> • Planos de projeto, documentos de requisitos funcionais e técnicos, repositório de controle de versões
A.6.2.2	Documentação de projeto e desenvolvimento de sistemas de IA	A organização deve documentar o projeto e o desenvolvimento do sistema de IA com base em objetivos organizacionais, requisitos documentados e critérios de especificação	<p>KPI: Documentação de Projeto e Desenvolvimento de Sistemas de IA</p> <p>Descrição: Mede o percentual de projetos de IA documentados conforme os objetivos organizacionais, requisitos formais e critérios de especificação técnica.</p> <p>Fórmula: $(\text{Número de projetos de IA com documentação completa} / \text{Total de projetos de IA iniciados}) \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Gerência de Desenvolvimento de IA ou Escritório de Projetos</p> <p>Fonte de dados: Repositório de documentos técnicos, sistema de versionamento, atas de revisão de projeto</p>
A.6.2.3	Verificação e validação do sistema de IA	A organização deve definir e documentar as medidas de verificação e validação para o sistema de IA e especificar os critérios para a sua utilização.	<p>KPI: Implementação de Medidas de Verificação e Validação em Sistemas de IA</p> <p>Descrição: Mede o percentual de sistemas de IA que possuem medidas de verificação e validação documentadas e aplicadas conforme critérios definidos.</p> <p>Fórmula: $(\text{Número de sistemas de IA com verificação e validação documentadas} / \text{Total de sistemas de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Qualidade de IA / Auditoria Técnica / Engenharia de Confiabilidade</p> <p>Fonte de dados: Relatórios técnicos, plano de testes, logs de validação, registros de revisão de conformidade</p>



Tabela A.1 – Objetivos de controle e controles

A.6.2 Ciclo de vida do sistema de IA			
Objetivo: Definir os critérios e requisitos para cada estágio do ciclo de vida do sistema de IA.			
CÓDIGO	TEMA	CONTROLE	KPIs
A.6.2.4	Implantação do sistema de IA	<p>A organização deve documentar um plano de implantação e assegurar que os requisitos apropriados sejam atendidos antes da implantação.</p>	<p>KPI: Documentação e Cumprimento do Plano de Implantação de Sistemas de IA</p> <p>Descrição: Mede o percentual de sistemas de IA que possuem plano de implantação documentado e com verificação de requisitos antes da entrada em operação.</p> <p>Fórmula: $(\text{Nº de sistemas de IA com plano de implantação e checklist de requisitos atendidos} / \text{Total de sistemas de IA implantados}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Gerência de Projetos de IA / Área de Operações Técnicas</p> <p>Fonte de dados: Planos de implantação documentados, checklists de conformidade, relatórios de readiness</p>
A.6.2.5	Operação e monitoramento do sistema de IA	<p>A organização deve definir e documentar os elementos necessários para a operação contínua do sistema de IA. No mínimo, convém que isso inclua monitoramento do sistema e do desempenho, reparos, atualizações e suporte.</p>	<p>KPI: Conformidade com Elementos de Operação Contínua de Sistemas de IA</p> <p>Descrição: Mede o percentual de sistemas de IA com todos os elementos essenciais de operação contínua (monitoramento, desempenho, reparos, atualizações e suporte) definidos e documentados.</p> <p>Fórmula: $(\text{Nº de sistemas de IA com elementos operacionais documentados} / \text{Total de sistemas de IA em operação}) \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Área de Operações de IA / Suporte Técnico</p> <p>Fonte de dados: Documentações técnicas dos sistemas, registros de manutenção, logs de monitoramento, planos de suporte e atualização.</p>
A.6.2.6	Documentação técnica do sistema de IA	<p>A organização deve determinar qual documentação técnica do sistema de IA é necessária para cada categoria relevante de partes interessadas, como usuários, parceiros e autoridades supervisoras, e fornecer a documentação técnica a elas de forma apropriada.</p>	<p>KPI: Cobertura da Documentação Técnica para Partes Interessadas</p> <p>Descrição: Mede o percentual de sistemas de IA que possuem documentação técnica adequada e entregue para cada grupo relevante de partes interessadas (usuários, parceiros e autoridades supervisoras).</p> <p>Fórmula: $(\text{Nº de sistemas com documentação técnica entregue conforme requisitos das partes interessadas} / \text{Total de sistemas em operação}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Semestral</p> <p>Responsável: Governança de IA / Área Técnica / Jurídico Regulatório</p> <p>Fonte de dados: Registros de entrega de documentação, recibos de aceite das partes interessadas, repositórios documentais internos.</p>



Tabela A.1 – Objetivos de controle e controles

A.6.2 Ciclo de vida do sistema de IA			
Objetivo: Definir os critérios e requisitos para cada estágio do ciclo de vida do sistema de IA.			
CÓDIGO	TEMA	CONTROLE	KPIs
A.6.2.7	Registro de logs de eventos do sistema de IA	A organização deve determinar em quais fases do ciclo de vida do sistema de IA convém habilitar a manutenção dos registros de log de eventos, mas no mínimo quando o sistema de IA estiver em uso.	<p>KPI: Registro de Logs nas Fases do Ciclo de Vida do Sistema de IA</p> <p>Descrição: Mede o percentual de sistemas de IA com registros de log implementados nas fases críticas do ciclo de vida, especialmente durante a fase de uso.</p> <p>Fórmula: ($\text{Nº de sistemas de IA com logs ativos nas fases definidas} / \text{Total de sistemas de IA operacionais}$) $\times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Área de Governança de IA / Segurança da Informação / TI</p> <p>Fonte de dados: Relatórios de auditoria de logs, repositórios de monitoramento, documentação de ciclo de vida.</p>



A.6.1 Orientações da direção para o desenvolvimento de sistemas de IA

A.6.1.1 Objetivo

Assegurar que a organização identifique e documente os objetivos e implemente os processos para o projeto e desenvolvimento responsáveis de sistemas de IA.

A.6.1.2 Objetivos para o desenvolvimento responsável de sistemas de IA

Controle

Convém que a organização identifique e documente os objetivos para orientar o desenvolvimento responsável de sistemas de IA, e considere esses objetivos e integre medidas para alcançá-los no ciclo de vida do desenvolvimento.

Orientações para implementação

Convém que a organização identifique objetivos (ver 6.2) que afetem os processos de projeto e desenvolvimento do sistema de IA. Convém que estes objetivos sejam considerados nos processos de projeto e desenvolvimento. Por exemplo, se uma organização determinar “justiça” como um objetivo, convém que isso seja considerado durante a especificação de requisitos, aquisição de dados, condicionamento de dados, treinamento de modelos, verificação e validação etc. Convém que a organização forneça requisitos e diretrizes conforme necessário para assegurar que as medidas integradas nas várias etapas (por exemplo, a exigência de usar uma ferramenta ou método de teste específico para lidar com injustiça ou viés indesejado) para atingir tais objetivos.

Outras informações

Técnicas de IA estão sendo usadas para aumentar as medidas de segurança, como previsão de ameaças, detecção e prevenção de ataques de segurança. Esta é uma aplicação de técnicas de IA que podem ser usadas para reforçar medidas de segurança para proteger sistemas de IA e sistemas de software convencionais não baseados em IA. O Anexo C fornece exemplos de objetivos organizacionais na gestão de riscos, que podem ser úteis na determinação dos objetivos para o desenvolvimento de sistemas de IA.

A.6.1.3 Processos para projeto e desenvolvimento responsáveis de sistemas de IA

Controle

Convém que a organização defina e documente os processos específicos para o projeto e desenvolvimento responsáveis do sistema de IA.

Orientações para implementação

Convém que o processo de desenvolvimento responsável de sistemas de IA considere, sem limitação, o seguinte:

- estágios do ciclo de vida (um modelo genérico de ciclo de vida do sistema de IA é fornecido pela ABNT NBR ISO/IEC 22989, mas a organização pode especificar seus próprios estágios de ciclo de vida);
 - requisitos de testes e meios previstos para os testes;
 - requisitos de supervisão humana, incluindo processos e ferramentas, especialmente quando o sistema de IA pode afetar pessoas naturais;
 - em que fases convém que sejam realizadas avaliações de impacto do sistema de IA; tecnologias de IA que se destinam a serem usadas para o sistema de IA

- expectativas e regras sobre dados de treinamento (por exemplo, que dados podem ser usados, fornecedores de dados aprovados e rotulagem);
- expertise (domínio do assunto ou outro) necessária ou formação para desenvolvedores de sistemas de IA, ou ambos;
- critérios de liberação;
- aprovações e assinaturas necessárias em várias fases;
- controle das alterações;
- usabilidade e controlabilidade;
- envolvimento das partes interessadas.

Os processos específicos de projeto e desenvolvimento dependem da funcionalidade e das tecnologias de IA que se destinam a serem usadas para o sistema de IA.

A.6.2 Ciclo de vida do sistema de IA

A.6.2.1 Objetivo

Definir os critérios e requisitos para cada estágio do ciclo de vida do sistema de IA.

A.6.2.2 Requisitos e especificações do sistema de IA

Controle

Convém que a organização especifique e documente os requisitos para novos sistemas de IA ou aprimoramentos materiais para sistemas existentes.

Orientações para implementação

Convém que a organização documente a justificativa para o desenvolvimento de um sistema de IA e seus objetivos. Alguns dos fatores que convém que sejam considerados, documentados e compreendidos podem incluir:

- a) por que o sistema de IA deve ser desenvolvido, por exemplo, se é impulsionado por um caso de negócios, por solicitação do cliente ou por política governamental; b) como o modelo pode ser treinado e como os requisitos de dados podem ser atingidos.

Convém que os requisitos do sistema de IA sejam especificados e abrangam todo o ciclo de vida do sistema de IA. Convém que tais requisitos sejam revisitados nos casos em que o sistema de IA desenvolvido não puder funcionar como pretendido ou se surgirem novas informações que possam ser usadas para alterar e melhorar os requisitos. Por exemplo, desenvolver o sistema de IA pode tornar-se inviável do ponto de vista financeiro.

Outras informações

Os processos para descrever o ciclo de vida do sistema de IA são fornecidos na ISO/IEC 5338. Para obter mais informações sobre o projeto centrado no ser humano para sistemas interativos, ver ISO 9241-210.



A.6 Ciclo de vida do sistema de IA

A.6.2.3 Documentação de projeto e desenvolvimento de sistemas de IA

Controle

Convém que a organização documente o projeto e o desenvolvimento do sistema de IA com base em objetivos organizacionais, requisitos documentados e critérios de especificação.

Orientações para implementação

Existem muitas opções de projeto necessárias para um sistema de IA, incluindo, mas não limitado a:

- abordagem de aprendizado de máquina (por exemplo, supervisão versus não supervisão);
- algoritmo de aprendizado e tipo de modelo de aprendizado de máquina utilizado;
- forma como o modelo se destina a ser treinado e qualidade dos dados (ver B.7);
- avaliação e aperfeiçoamento dos modelos;
- componentes de hardware e software;
- ameaças à segurança consideradas durante o ciclo de vida do sistema de IA; ameaças de segurança específicas de sistemas de IA incluem envenenamento de dados, roubo de modelos ou ataques de inversão de modelos;
- interface e apresentação das saídas;
- como os seres humanos podem interagir com o sistema;
- considerações de interoperabilidade e portabilidade.

Pode haver várias iterações entre o projeto e o desenvolvimento, mas convém que a documentação no estágio seja mantida e que uma documentação final da arquitetura do sistema esteja disponível

Outras informações

Para mais informações sobre o projeto centrado no ser humano para sistemas interativos, ver ISO 9241-210.

A.6.2.4 Verificação e validação do sistema de IA

Controle

Convém que a organização defina e documente medidas de verificação e validação para o sistema de IA e especifique critérios para o seu uso.

Orientações para implementação

As medidas de verificação e validação podem incluir, mas não estão limitadas a:

- metodologias e ferramentas de teste;
- seleção dos dados de teste e a sua representatividade em relação ao domínio de uso pretendido;
- requisitos para critério de liberação.

Convém que a organização defina e documente critérios de avaliação, como, mas não se limite a:

- um plano para avaliar os componentes do sistema de IA e de todo o sistema de IA para riscos relacionados com impactos nos indivíduos ou grupos de indivíduos, ou ambos, e nas sociedades;
- o plano de avaliação pode se basear, por exemplo em:

A) requisitos de confiabilidade e segurança do sistema de IA, incluindo taxas de erro aceitáveis para o desempenho do sistema de IA;

B) desenvolvimento responsável e objetivos de uso de sistemas de IA, como os referidos em B.6.1.2 e B.9.3;

C) fatores operacionais, como qualidade dos dados e uso pretendido, incluindo intervalos aceitáveis de cada fator operacional;

D) quaisquer usos pretendidos que possam exigir fatores operacionais mais rigorosos a serem definidos, incluindo diferentes intervalos aceitáveis para fatores operacionais ou taxas de erro mais baixas;

– métodos, orientações ou métricas usados para avaliar se as partes interessadas relevantes que tomam decisões ou estão sujeitas às decisões baseadas nos resultados do sistema de IA podem, de forma adequada, interpretar as saídas do sistema de IA. Convém que a frequência da avaliação seja determinada e possa basear-se nos resultados de uma avaliação de impacto do sistema de IA;

- quaisquer fatores aceitáveis que possam explicar a incapacidade de atingir um nível mínimo de desempenho-alvo, especialmente quando o sistema de IA é avaliado quanto aos impactos nos indivíduos ou grupos de indivíduos, ou ambos, e nas sociedades (por exemplo, baixa resolução de imagem para sistemas de visão computacional ou ruído de fundo que afeta sistemas de reconhecimento de fala). Convém documentar também os mecanismos que lidam com o baixo desempenho do sistema de IA como resultado desses fatores.

Convém que o sistema de IA seja avaliado em relação aos critérios documentados para avaliação.

Se o sistema de IA não puder atender aos critérios documentados de avaliação, especialmente em relação aos objetivos de desenvolvimento e uso responsáveis do sistema de IA (ver B.6.1.2 e B.9.3), convém que a organização reconsidera ou gerencie as deficiências do uso pretendido do sistema de IA, seus requisitos de desempenho e como a organização pode efetivamente abordar os impactos para indivíduos ou grupos de indivíduos, ou ambos, e para as sociedades.

NOTA no ISO/IEC TR 24029-1.

Mais informações sobre como lidar com a robustez de redes neurais podem ser encontradas.

A.6.2.5 Implantação do sistema de IA

Controle

Convém que a organização documente um plano de implantação e assegure que os requisitos apropriados sejam atendidos antes da implantação.

Orientações para implementação

Os sistemas de IA podem ser desenvolvidos em vários ambientes e implantados em outros (como os desenvolvidos no local e implantados usando cloud computing) e convém que a organização considere essas diferenças para o plano de implantação. Convém que a organização também considere se os componentes são implantados separadamente (por exemplo, o software e o modelo podem ser implantados de forma independente). Além disso, convém que a organização tenha um conjunto de requisitos a serem atendidos antes da liberação e implantação (às vezes chamados de «critérios de liberação»). Isso pode incluir medidas de verificação e validação a serem aprovadas, métricas de desempenho a serem atendidas, testes de usuários a serem concluídos, bem como aprovações gerenciais e aceites a serem obtidos. Convém que o plano de implantação considere as perspectivas e os impactos para as partes interessadas relevantes.



A.6 Ciclo de vida do sistema de IA

A.6.2.6 Operação e monitoramento do sistema de IA

Controle

Convém que a organização defina e documente os elementos necessários para a operação contínua do sistema de IA. No mínimo, convém que isso inclua o monitoramento do sistema e do desempenho, reparos, atualizações e suporte.

Orientações para implementação

Cada atividade mínima para operação e monitoramento pode considerar vários aspectos. Por exemplo:

- O monitoramento do sistema e do desempenho pode incluir o monitoramento de erros e falhas gerais, bem como se o sistema está funcionando conforme o esperado com os dados de produção. Os critérios de desempenho técnico podem incluir taxas de sucesso na resolução de problemas ou na realização de tarefas, ou taxas de confiança. Outros critérios podem estar relacionados a atingir o compromisso, ou expectativa, e as necessidades das partes interessadas, incluindo, por exemplo, monitoramento contínuo para assegurar o cumprimento dos requisitos do cliente ou dos requisitos legais aplicáveis;

- Alguns sistemas de IA implantados evoluem seu desempenho como resultado do ML, onde os dados de produção e os dados de saída são usados para treinar ainda mais o modelo de ML. Nos casos em que o aprendizado contínuo é utilizado, convém que a organização monitore o desempenho do sistema de IA para assegurar que ele continue atendendo seus objetivos de projeto e opere nos dados de produção como pretendido;

- O desempenho de alguns sistemas de IA pode mudar mesmo que esses sistemas não usem aprendizado contínuo, geralmente por desvios de conceito ou dados de produção. Nesses casos, o monitoramento pode identificar a necessidade de re-treinamento para assegurar que o sistema de IA continue cumprindo seus objetivos de projeto e operando com dados de produção como pretendido.

Mais informações podem ser encontradas na ISO/IEC 23053.

- Os reparos podem incluir respostas a erros e falhas no sistema. Convém que a organização tenha processos para a resposta e reparo desses problemas. Além disso, as atualizações podem ser necessárias à medida que o sistema evolui ou à medida que problemas críticos são identificados, ou como resultado de problemas identificados externamente (por exemplo, não conformidade com as expectativas do cliente ou requisito legal). Convém haver processos em vigor para atualizar o sistema, incluindo componentes afetados, cronograma de atualização e informações aos usuários sobre o que está incluído na atualização;

- As atualizações do sistema também podem incluir alterações nas operações do sistema, usos pretendidos novos ou modificados ou outras alterações na funcionalidade do sistema. Convém que a organização tenha procedimentos para lidar com mudanças operacionais, incluindo a comunicação aos usuários;

- O suporte ao sistema pode ser interno, externo ou ambos, dependendo das necessidades da organização e de como o sistema foi adquirido. Convém que os processos de suporte considerem como os usuários podem entrar em contato com a ajuda apropriada, como os problemas e incidentes são relatados, além de também levar em conta contratos e métricas de nível de serviço de suporte;

- Sempre que os sistemas de IA forem utilizados para finalidades diferentes daquelas para as quais foram concebidos ou de formas não previstas, convém considerar a adequação dessas utilizações;

- Convém que as ameaças à segurança da informação específicas de IA, relacionadas aos sistemas de IA aplicados e aos desenvolvidos pela organização, sejam identificadas. As ameaças à segurança da informação específicas de IA incluem, mas não são limitadas a, envenenamento de dados, roubo de modelos e ataques de inversão de modelos.

Outras informações

Convém que a organização considere o desempenho operacional que pode afetar as partes interessadas e considere isso ao projetar e determinar os critérios de desempenho. Convém que os critérios de desempenho para os sistemas de IA em operação sejam determinados pela tarefa em questão, como classificação, regressão, ranqueamento, agrupamento ou redução de dimensionalidade. Os critérios de desempenho podem incluir aspectos estatísticos, como taxas de erro e duração do processamento. Para cada critério, convém que a organização identifique todas as métricas relevantes, bem como as interdependências entre elas. Para cada métrica, convém que a organização considere valores aceitáveis com base, por exemplo, nas recomendações de especialistas do domínio e na análise das expectativas das partes interessadas, relativas às práticas existentes que não sejam de IA.

Por exemplo, uma organização pode determinar que obter a pontuação F1 é um valor apropriado com base em sua avaliação do impacto de falsos positivos e falsos negativos, conforme descrito na ISO/IEC TS 4213. A organização pode então estabelecer um valor F1 que se espera que o sistema de IA atenda. Convém que seja avaliado se estas questões podem ser tratadas pelas medidas existentes. Se não for esse o caso, convém que sejam consideradas alterações às medidas existentes ou que sejam determinadas medidas adicionais para detectar e tratar estas questões.

Convém que a organização considere o desempenho de sistemas ou de processos em operação que não sejam de IA e o utilize como contexto potencialmente relevante ao estabelecer critérios de desempenho.

Convém que a organização também assegure que os meios e processos utilizados para avaliar o sistema de IA, incluindo, quando aplicável, a seleção e gestão dos dados de avaliação, melhore a completude e a confiabilidade na avaliação do seu desempenho em relação aos critérios definidos.

O desenvolvimento de metodologias de avaliação de desempenho pode ser baseado em critérios, métricas e valores. Convém que estes critérios, métricas e valores informem a quantidade de dados e os tipos de processos utilizados na avaliação, bem como os papéis e a expertise do pessoal encarregado de efetuar a avaliação.



A.6 Ciclo de vida do sistema de IA

Convém que as metodologias de avaliação de desempenho refletem os atributos e as características de uso e operação o mais próximo possível para assegurar que os resultados da avaliação sejam úteis e relevantes. Alguns aspectos da avaliação de desempenho podem exigir a introdução controlada de dados ou processos errôneos ou espúrios para avaliar o impacto no desempenho.

O modelo de qualidade na ISO/IEC 25059 pode ser usado para definir critérios de desempenho.

A.6.2.7 Documentação técnica do sistema de IA Controle

Convém que a organização determine qual documentação técnica do sistema de IA é necessária para cada categoria relevante de partes interessadas, como usuários, parceiros e autoridades de supervisão, e forneça a documentação técnica a elas de forma apropriada.

Orientações para implementação

A documentação técnica do sistema de IA pode incluir, mas não está limitada a, os seguintes elementos:

- uma descrição geral do sistema de IA, incluindo o seu propósito pretendido;
- instruções de uso;
- pressupostos técnicos sobre a sua implantação e funcionamento (ambiente de execução, capacidades de software e hardware relacionadas, pressupostos sobre dados etc.);
- limitações técnicas (por exemplo, taxas de erro aceitáveis, exatidão, confiabilidade, robustez);
- capacidades e funções de monitoramento que permitam que os usuários ou operadores influenciem o funcionamento do sistema.

Os elementos de documentação relacionados a todos os estágios do ciclo de vida do sistema de IA (conforme definido na ABNT NBR ISO/IEC 22989) podem incluir, mas não estão limitados a:

- projeto e especificação da arquitetura do sistema;
- escolhas de projeto efetuadas e medidas de qualidade tomadas durante o processo de desenvolvimento do sistema;
- informações sobre os dados utilizados durante o desenvolvimento do sistema;
- pressupostos assumidos e medidas de qualidade tomadas em matéria de qualidade dos dados (por exemplo, distribuições estatísticas assumidas);
- atividades de gestão (por exemplo, gestão de riscos) realizadas durante o desenvolvimento ou funcionamento do sistema de IA;
- registros de verificação e validação;
- alterações feitas no sistema de IA quando este estiver em operação;
- documentação relativa à avaliação de impacto, como descrito em B.5.

Convém que a organização documente informações técnicas relacionadas à operação responsável do sistema de IA. Isso pode incluir, mas não está limitado a:

- documentar um plano para gerenciar falhas. Isso pode incluir, por exemplo, a necessidade de descrever um plano de reversão para o sistema de IA, desativar recursos do sistema de IA, um processo de atualização ou um plano para notificar clientes, usuários etc. sobre mudanças no sistema de IA, informações atualizadas sobre falhas no sistema e como elas podem ser mitigadas;
- documentar processos para monitorar a saúde do sistema de IA (isto é, o sistema de IA funciona como pretendido e dentro das suas margens normais de funcionamento, também designado por observabilidade) e processos para lidar com falhas no sistema de IA;
- documentar procedimentos operacionais padrão para o sistema de IA, incluindo quais eventos

convém que sejam monitorados e como os logs de eventos são priorizados e analisados criticamente. Também pode ser incluído como investigar falhas e a prevenção de falhas;

- documentar os papéis do pessoal responsável pela operação do sistema de IA, bem como os responsáveis pela responsabilização do uso do sistema, especialmente em relação ao tratamento dos efeitos de falhas do sistema de IA ou gerenciamento de atualizações no sistema de IA;
- documentar as atualizações do sistema como alterações nas suas operações, usos pretendidos novos ou modificados, ou outras alterações na sua funcionalidade.

Convém que a organização tenha procedimentos estabelecidos para lidar com mudanças operacionais, incluindo comunicação com usuários e avaliações internas sobre o tipo de mudança.

Convém que a documentação esteja atualizada e precisa. Convém que a documentação seja aprovada pela direção pertinente dentro da organização.

Quando fornecidos como parte da documentação do usuário, convém que os controles indicados na Tabela A.1 sejam considerados.

A.6.2.8 Registo de logs de eventos do sistema de IA

Controle

Convém que a organização determine em quais fases do ciclo de vida do sistema de IA a manutenção de logs de eventos seja habilitada, mas no mínimo quando o sistema de IA estiver em uso

Orientações para implementação

Convém que a organização assegure o registro em log dos sistemas de IA implantados para coletar e registrar automaticamente logs de eventos relacionados a determinados eventos que ocorrem durante a operação. Esse registro pode incluir, mas não está limitado a:

- rastreabilidade da funcionalidade do sistema de IA para assegurar que o sistema de IA esteja operando como pretendido;
- detecção, por meio do monitoramento da operação do sistema de IA, do desempenho do sistema de IA fora das condições operacionais pretendidas, o que pode resultar em desempenho indesejável nos dados de produção ou em impactos para as partes interessadas relevantes.

Os logs de eventos do sistema de IA podem incluir informações, como a hora e a data de cada vez que o sistema de IA é usado, dados de produção nos quais o sistema de IA opera, saídas que resultem da faixa de operação pretendida do sistema de IA etc.

Convém que os logs de eventos sejam mantidos pelo tempo necessário para o uso pretendido do sistema de IA e dentro das políticas de retenção de dados da organização. Requisitos regulatórios relacionados à retenção de dados podem ser aplicáveis. Outras informações. Alguns sistemas de IA, como sistemas de identificação biométrica, podem ter requisitos de registro adicionais, dependendo da jurisdição. Convém que as organizações estejam cientes desses requisitos.



A.6 Ciclo de vida do sistema de IA

Estudo de Caso:

Ciclo de Vida da IA no Sistema de Atendimento Virtual da HealthCare+

Contexto:

A HealthCare+, uma rede de clínicas médicas, decidiu implantar um sistema de IA para automatizar o atendimento inicial de pacientes via chatbot, ajudando no agendamento e triagem de sintomas. Para garantir segurança, eficácia e conformidade regulatória, a empresa adotou o modelo de ciclo de vida completo conforme a ISO/IEC 42001.

Desafios Enfrentados:

- Garantir que a IA seja confiável e segura ao longo do tempo.
- Planejar e controlar cada etapa do ciclo de vida, do desenvolvimento à desativação.
- Evitar falhas que comprometesssem diagnósticos ou causassem violação de dados pessoais.

Ações Baseadas em A.6 – Ciclo de Vida do Sistema de IA:

1. Planejamento e projeto inicial

- A equipe multidisciplinar (TI, jurídico, saúde, compliance) definiu objetivos, riscos, critérios de sucesso e requisitos éticos.

2. Desenvolvimento

- Utilizou dados anonimizados de atendimentos anteriores.
- Validou o modelo com médicos e pacientes reais em simulações controladas.

3. Verificação e Validação

- Implementou testes automatizados e revisões humanas.
- Incluiu mecanismos de rastreabilidade para auditoria.

4. Implantação

- O sistema foi implantado em fases (piloto > expansão gradual).
- Documentação técnica foi entregue a todas as áreas envolvidas.

5. Operação e Monitoramento

- IA monitorada em tempo real com alertas para erros de resposta.
- Logs de eventos armazenados para análise e correção.

6. Atualização e Manutenção

- Atualizações regulares com base em feedback dos usuários e novos protocolos clínicos.

7. Descomissionamento

- Foi criado um plano claro para quando o sistema fosse substituído, incluindo backup e eliminação segura de dados.

Resultados Alcançados:

- Redução de 40% no tempo médio de atendimento inicial
- Conformidade com LGPD e diretrizes éticas
- Nenhum incidente de segurança ou violação nos primeiros 12 meses
- Alta confiança dos médicos e pacientes no uso do sistema

Aprendizado:

Este caso destaca a importância de tratar o sistema de IA como um processo vivo e contínuo, que precisa de planejamento, gestão e revisão em cada etapa – desde a concepção até a desativação.



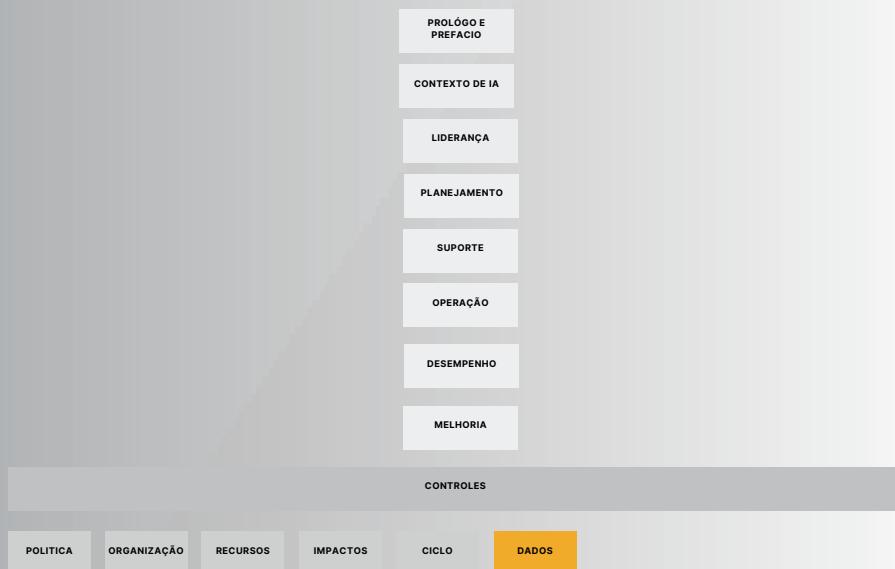
08

CONTROLE A.7

Dados para sistemas de IA



Dados para Sistemas de IA da ISO/IEC 42001 destaca a importância da gestão responsável dos dados usados ao longo do ciclo de vida dos sistemas de Inteligência Artificial. A organização deve identificar, documentar e controlar aspectos como aquisição, qualidade, preparação e proveniência dos dados. Isso inclui garantir que os dados estejam alinhados com os requisitos técnicos e éticos, evitando vieses, protegendo a privacidade e respeitando normas legais como a LGPD. Um bom controle de dados é essencial para garantir que a IA seja justa, precisa, segura e confiável.



As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.7 Dados para sistemas de IA			
CÓDIGO	TEMA	CONTROLE	KPIs
A.7.1	Dados para desenvolvimento e aprimoramento do sistema de IA	A organização deve definir, documentar e implementar processos de gestão de dados relacionados com o desenvolvimento de sistemas de IA.	<p>KPI: Implementação de Processos de Gestão de Dados no Desenvolvimento de IA</p> <p>Descrição: Mede o percentual de projetos de IA que possuem processos formalmente definidos, documentados e implementados para a gestão de dados utilizados em seu desenvolvimento.</p> <p>Fórmula: $(\text{Nº de projetos de IA com gestão de dados documentada} / \text{Total de projetos de IA em desenvolvimento}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Área de Governança de Dados / Equipe de Desenvolvimento de IA</p> <p>Fonte de dados: Registros de projetos, planos de desenvolvimento de IA, relatórios de conformidade de dados.</p>
A.7.2	Aquisição de dados	A organização deve determinar e documentar os detalhes sobre a aquisição e seleção dos dados usados em sistemas de IA.	<p>KPI: Documentação da Aquisição e Seleção de Dados para Sistemas de IA</p> <p>Descrição: Mede o percentual de projetos de IA que possuem documentação completa e atualizada sobre os critérios, fontes e processos de aquisição e seleção dos dados utilizados.</p> <p>Fórmula: $(\text{Nº de projetos com documentação de aquisição e seleção de dados} / \text{Total de projetos de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Governança de Dados / Equipe de Compliance em IA</p> <p>Fonte de dados: Relatórios de projeto, plano de governança de dados, registros de origem e validação dos dados.</p>
A.7.3	Qualidade dos dados para sistemas de IA	A organização deve definir e documentar os requisitos de qualidade dos dados e assegurar que os dados usados para desenvolver e operar o sistema de IA atendam a esses requisitos.	<p>KPI: Conformidade com Requisitos de Qualidade dos Dados em Sistemas de IA</p> <p>Descrição: Mede o percentual de projetos de IA que utilizam dados validados conforme os requisitos de qualidade previamente definidos (ex: precisão, completude, atualidade, consistência).</p> <p>Fórmula: $(\text{Nº de projetos que atendem aos requisitos de qualidade de dados} / \text{Total de projetos de IA ativos}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Trimestral</p> <p>Responsável: Governança de Dados / Líder de Qualidade da Informação</p> <p>Fonte de dados: Relatórios de validação de dados, logs de conformidade, checklist de qualidade de dados documentado.</p>



Tabela A.1 – Objetivos de controle e controles

A.7 Dados para sistemas de IA			
CÓDIGO	TEMA	CONTROLE	KPIs
A.7.4	Proveniência dos dados	<p>A organização deve definir e documentar um processo para verificar e registrar a proveniência dos dados usados em seus sistemas de IA ao longo dos ciclos de vida dos dados e do sistema de IA</p>	<p>KPI: Rastreabilidade da Proveniência dos Dados em Sistemas de IA</p> <p>Descrição: Mede o percentual de conjuntos de dados usados em projetos de IA que possuem proveniência registrada e verificável, desde a origem até o uso final no ciclo de vida do sistema de IA.</p> <p>Fórmula: $(\text{Nº de conjuntos de dados com proveniência verificada} / \text{Total de conjuntos de dados utilizados em IA}) \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Freqüência de medição: Trimestral</p> <p>Responsável: Governança de Dados / DPO / Líder de Conformidade</p> <p>Fonte de dados: Registros de auditoria de dados, sistemas de gerenciamento de metadados, logs de proveniência e checklist de conformidade de dados.</p>
A.7.5	Preparação dos dados	<p>A organização deve definir e documentar seus critérios para seleção de preparação de dados e os métodos de preparação de dados a serem utilizados.</p>	<p>KPI: Conformidade com os Critérios de Preparação de Dados para IA</p> <p>Descrição: Mede o percentual de conjuntos de dados utilizados em sistemas de IA que seguem os critérios documentados de seleção e os métodos definidos de preparação de dados.</p> <p>Fórmula: $(\text{Nº de conjuntos de dados preparados conforme os critérios definidos} / \text{Total de conjuntos de dados utilizados}) \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Freqüência de medição: Trimestral</p> <p>Responsável: Equipe de Governança de Dados / Líder de Engenharia de IA</p> <p>Fonte de dados: Documentos de preparação de dados, planos de qualidade de dados, registros de conformidade e checklist de preparação.</p>



A.7 Dados para sistemas de IA

A.7.0 Objetivo

Assegurar que a organização compreenda o papel e os impactos dos dados em sistemas de IA na aplicação e desenvolvimento, provisionamento ou uso de sistemas de IA ao longo de seus ciclos de vida.

A.7.1 Dados para desenvolvimento e aprimoramento do sistema de IA

Controle

Convém que a organização defina, documente e implemente processos de gestão de dados relacionados ao desenvolvimento de sistemas de IA.

Orientações para implementação

A gestão de dados pode incluir vários tópicos como, mas não limitados a, os seguintes:

- implicações de privacidade e segurança devido à utilização de dados, podendo alguns dos quais ser de natureza sensível;
- ameaças à segurança e à segurança física que podem surgir no desenvolvimento de sistemas de IA dependentes de dados;
- aspectos de transparência e explicabilidade, incluindo a proveniência dos dados e a capacidade de fornecer uma explicação de como os dados são utilizados para determinar as saídas de um sistema de IA, se o sistema exigir transparência e explicabilidade;
- representatividade dos dados de treinamento em comparação com o domínio operacional de uso;
- exatidão e integridade dos dados.

NOTA Informações detalhadas do ciclo de vida do sistema de IA e conceitos de gestão de dados são fornecidas na ABNT NBR ISO/IEC 22989.

A.7.2 Aquisição de dados

Controle

Convém que a organização determine e documente detalhes sobre a aquisição e seleção dos dados usados em sistemas de IA.

Orientações para implementação

A organização pode precisar de diferentes categorias de dados de diferentes fontes, dependendo do escopo e do uso de seus sistemas de IA. Os detalhes para aquisição de dados podem incluir:

- categorias de dados necessários para o sistema de IA;
- quantidade de dados necessários;
- fontes de dados (por exemplo, internos, comprados, partilhados, dados abertos, sintéticos);
- características da fonte de dados (por exemplo, estática, transmitida, coletada, gerada por máquina);
- dados demográficos e características dos sujeitos de dados (por exemplo, vieses potenciais ou conhecidos ou outros erros sistemáticos);
- tratamento prévio dos dados (por exemplo, usos anteriores, conformidade com requisitos de privacidade e segurança);
- direitos dos dados (por exemplo, DP, copyright);
- metadados associados (por exemplo, detalhes de rotulagem e aprimoramento de dados);
- proveniência dos dados.

Outras informações

As categorias de dados e uma estrutura para o uso de dados da ISO/IEC 19944-1 podem ser usadas para documentar detalhes sobre a aquisição e o uso de dados.

A.7.3 Qualidade dos dados para sistemas de IA

Controle

Convém que a organização defina e documente requisitos de qualidade dos dados e assegure que os dados usados para desenvolver e operar o sistema de IA atendam a esses requisitos.

Orientações para implementação

A qualidade dos dados usados para desenvolver e operar sistemas de IA potencialmente tem impactos significativos na validade dos resultados do sistema. A ISO/IEC 25024 define qualidade de dados como o grau em que as características dos dados satisfazem as necessidades declaradas e implícitas, quando usados sob condições especificadas. Para sistemas de IA que usam aprendizado de máquina supervisionado ou semi-supervisionado, é importante que a qualidade dos dados de treinamento, validação, teste e produção seja definida, medida e melhorada na medida do possível, e convém que a organização assegure que os dados sejam adequados ao propósito pretendido. Convém que a organização considere o impacto do viés no desempenho do sistema e na justiça do sistema, e que faça os ajustes necessários no modelo e nos dados usados para melhorar o desempenho e a justiça para níveis aceitáveis para o caso de uso.

Outras informações

Informações adicionais sobre a qualidade dos dados estão disponíveis na série ISO/IEC 52592 sobre qualidade de dados para análise e ML. Informações adicionais sobre diferentes formas de viés em dados usados em sistemas de IA estão disponíveis no ABNT ISO/IEC TR 24027.

A.7.4 Proveniência dos dados

Controle

Convém que a organização defina e documente um processo para verificar e registrar a proveniência dos dados usados em seus sistemas de IA ao longo dos ciclos de vida dos dados e do sistema de IA.

Orientações para implementação

De acordo com a ISO 8000-2, um registro de proveniência dos dados pode incluir informações sobre a criação, atualização, transcrição, abstração, validação e transferência de controle dos dados. Além disso, o compartilhamento de dados (sem transferência de controle) e as transformações de dados podem ser considerados sob a proveniência dos dados. Dependendo de fatores como a fonte dos dados, o seu conteúdo e o contexto da sua utilização, convém que as organizações considerem se são necessárias medidas para verificar a proveniência dos dados.



A.7 Dados para sistemas de IA

A.7.5 Preparação dos dados

Controle

A organização deve definir e documentar seus critérios para selecionar a preparação dos dados e os métodos de preparação dos dados a serem usados.

Orientações para implementação

Os dados usados em um sistema de IA normalmente precisam de preparação para torná-los utilizáveis para uma determinada tarefa de IA. Por exemplo, algoritmos de aprendizado de máquina às vezes são intolerantes a entradas ausentes ou incorretas, distribuição não normal e escalas muito variadas.

Métodos de preparação e transformações podem ser usados para aumentar a qualidade dos dados.

A falha em preparar adequadamente os dados pode, potencialmente, levar a erros do sistema de IA.

Métodos comuns de preparação e transformações para dados usados em sistemas de IA incluem:

- exploração estatística dos dados (por exemplo, distribuição, média, mediana, desvio-padrão, intervalo, estratificação, amostragem) e metadados estatísticos (por exemplo, especificação da iniciativa de documentação de dados (DDI) [28]);
- limpeza (isto é, correção de entradas, lidando com entradas faltantes);
- imputação (isto é, métodos de preenchimento de entradas faltantes);
- normalização;
- dimensionamento;
- rotulagem das variáveis-alvo;
- codificação (por exemplo, conversão de variáveis categóricas em números).

Para uma determinada tarefa de IA, convém que a organização documente seus critérios para selecionar métodos e transformações específicos de preparação de dados, bem como métodos e transformações específicos usados na tarefa de IA.

NOTA Para obter informações adicionais sobre a preparação de dados específicos para aprendizado de máquina, ver a série ISO/IEC 52592 e ISO/IEC 23053.

Estudo de Caso:

Gestão de Dados no Sistema de Recrutamento Inteligente da RHFuture

Contexto:

A RHFuture, uma empresa de tecnologia para gestão de talentos, desenvolveu um sistema de IA para triagem automática de currículos. O objetivo era tornar o processo de recrutamento mais ágil e reduzir vieses humanos.

Desafios Enfrentados:

1. Fontes de dados diversas e desestruturadas (currículos em PDF, perfis de redes sociais, formulários online).
2. Riscos de viés nos dados históricos usados para treinar o modelo (ex: favorecimento de determinadas universidades ou bairros).
3. Falta de rastreabilidade clara sobre a origem e a qualidade dos dados usados no sistema.

Ações Implementadas (alinhadas à Seção B.7 da ISO 42001):

1. Identificação e documentação dos dados

A RHFuture criou um inventário de dados com:

- Origem dos dados (ex: formulários internos, redes públicas autorizadas)
- Base legal para uso de dados pessoais (LGPD)
- Requisitos de qualidade (dados atualizados, completos, não redundantes)

2. Critérios de seleção e preparação dos dados

- Foram definidos padrões mínimos de legibilidade e estrutura.
- Aplicou-se anonimização dos dados para reduzir riscos de identificação sensível.

3. Verificação da proveniência dos dados

- Implantou-se um processo de checagem da origem de cada conjunto de dados, com registros auditáveis.

4. Gestão de ciclo de vida dos dados

- Criado um plano de retenção, arquivamento e descarte dos dados com base em diretrizes legais e éticas.

Resultados Alcançados:

- Redução de 30% no tempo médio de triagem de currículos
- Aumento na diversidade de perfis selecionados
- Conformidade com a LGPD e com os princípios da ISO 42001
- Sistema auditável com rastreabilidade completa dos dados usado.

Aprendizado:

O estudo mostra como a governança de dados é essencial para garantir que os sistemas de IA operem de forma justa, segura e eficaz. Sem dados de qualidade e bem documentados, não há IA confiável.



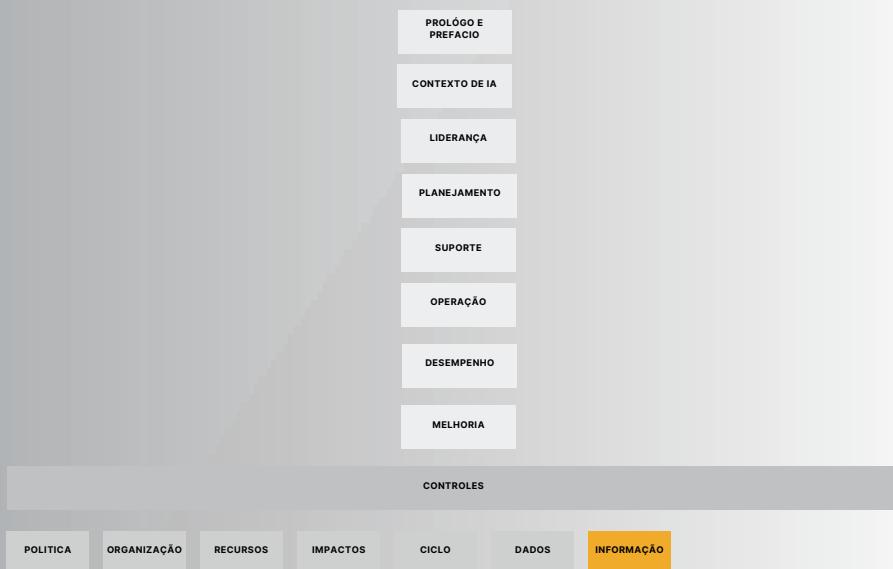
08

CONTROLE A.8

Informação para as partes interessadas



Informação para as Partes Interessadas da ISO/IEC 42001 trata da transparência e comunicação sobre os sistemas de IA com todas as partes envolvidas. A organização deve determinar e fornecer informações apropriadas aos usuários, parceiros, autoridades reguladoras e sociedade, incluindo funcionalidades, riscos, limitações e eventuais incidentes. Também deve oferecer canais seguros para que essas partes possam relatar impactos adversos. Esse processo fortalece a confiança, a responsabilização e o uso ético da IA.



As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.8 Informações para as partes interessadas em sistemas de IA			
Objetivo: Assegurar que as partes interessadas relevantes disponham das informações necessárias para compreender e avaliar os riscos e os seus impactos (positivos e negativos).			
CÓDIGO	TEMA	CONTROLE	KPIs
A.8.1	Documentação do sistema e informação para usuários	A organização deve determinar e fornecer as informações necessárias aos usuários do sistema.	<p>KPI: Fornecimento de Informações aos Usuários de Sistemas de IA</p> <p>Descrição: Mede o percentual de usuários que receberam as informações necessárias para uso adequado, seguro e responsável do sistema de IA.</p> <p>Fórmula: (Número de usuários com acesso à documentação adequada / Total de usuários do sistema de IA) × 100</p> <p>Meta sugerida: ≥ 95%</p> <p>Frequência de Medição: Trimestral</p> <p>Responsável: Área de Produto / UX / Governança de IA</p> <p>Fonte dos Dados: Registro de envio de manuais, treinamentos e logs de acesso à base de conhecimento.</p>
A.8.2	Relatórios externos	A organização deve fornecer recursos para as partes interessadas relatarem impactos adversos do sistema de IA.	<p>KPI: Mecanismo de Relato de Impactos Adversos de IA</p> <p>Nome: Efetividade do Canal de Relato de Impactos Adversos de IA</p> <p>Descrição: Mede a disponibilidade e a utilização do canal fornecido pela organização para que partes interessadas relatem impactos adversos relacionados ao sistema de IA.</p> <p>Fórmula: (Número de relatos processados / Total de relatos recebidos) × 100</p> <p>Meta sugerida: ≥ 90% de relatos respondidos/processados no prazo definido</p> <p>Frequência de Medição: Trimestral</p> <p>Responsável: Governança de IA / Compliance / Ouvidoria Digital</p> <p>Fonte dos Dados: Sistema de atendimento, ouvidoria, registro de incidentes ou plataforma de feedback de IA</p>
A.8.3	Comunicação de incidentes	A organização deve determinar e documentar um plano de comunicação de incidentes aos usuários do sistema de IA.	<p>KPI: Plano de Comunicação de Incidentes de IA aos Usuários</p> <p>Descrição: Mede a existência e a aplicação de um plano documentado para comunicar incidentes relacionados a IA aos usuários afetados, de forma clara e no tempo adequado.</p> <p>Fórmula: (Número de incidentes comunicados conforme plano / Total de incidentes registrados) × 100</p> <p>Meta sugerida: ≥ 95%</p> <p>Frequência de Medição: Trimestral</p> <p>Responsável: Governança de IA / Área de Riscos e Comunicação</p> <p>Fonte dos Dados: Registro de incidentes, logs de comunicação, planos de resposta a incidentes</p>



Tabela A.1 – Objetivos de controle e controles

A.8 Informações para as partes interessadas em sistemas de IA			
Objetivo: Assegurar que as partes interessadas relevantes disponham das informações necessárias para compreender e avaliar os riscos e os seus impactos (positivos e negativos).			
CÓDIGO	TEMA	CONTROLE	KPIs
A.8.4	Informação às partes interessadas	<p>A organização deve determinar e documentar suas obrigações de relatar informações sobre o sistema de IA às partes interessadas.</p>	<p>KPI: Cumprimento das Obrigações de Relato sobre Sistemas de IA</p> <p>Nome: Conformidade com Obrigações de Relato sobre IA</p> <p>Descrição: Mede o grau de cumprimento das obrigações da organização em relatar informações relevantes sobre o sistema de IA às partes interessadas (usuários, reguladores, parceiros).</p> <p>Fórmula: (Número de relatórios entregues conforme exigido / Total de relatórios obrigatórios no período) × 100</p> <p>Meta sugerida: ≥ 100%</p> <p>Frequência de Medição: Semestral</p> <p>Responsável: Área de Governança de IA ou Jurídico/Compliance</p> <p>Fonte dos Dados: Registro de obrigações contratuais, logs de envio, protocolos de comunicação, auditorias regulatórias</p>



A.8 Informação para as partes interessadas

A.8.0 Objetivo

Assegurar que as partes interessadas relevantes disponham das informações necessárias para compreender e avaliar os riscos e os seus impactos (positivos e negativos).

A.8.1 Documentação do sistema e informações para usuários

Controle

Convém que a organização determine e forneça as informações necessárias aos usuários do sistema.

Orientações para implementação

As informações sobre o sistema de IA podem incluir detalhes técnicos e instruções, bem como notificações aos usuários sobre eles estarem interagindo com um sistema de IA, dependendo do contexto. Isso pode também incluir o próprio sistema, bem como saídas potenciais do sistema (por exemplo, notificar os usuários sobre uma imagem que foi criada por IA).

Embora os sistemas de IA possam ser complexos, é fundamental que os usuários sejam capazes de entender, quando eles estiverem interagindo com um sistema de IA, como o sistema funciona.

Os usuários também precisam entender seu propósito e usos pretendidos, seu potencial de causar danos ou beneficiar o usuário. Algumas documentações do sistema podem ser necessariamente direcionadas para usos mais técnicos (por exemplo, administradores de sistema), e convém que a organização compreenda as necessidades das diferentes partes interessadas e o que a compreensibilidade pode significar para elas. Também convém que as informações sejam acessíveis, tanto em termos de facilidade de uso para encontrá-las, quanto para os usuários que podem precisar de recursos de acessibilidade adicionais.

As informações que podem ser fornecidas aos usuários incluem, mas não estão limitadas a:

- propósito do sistema;
- que o usuário está interagindo com um sistema de IA;
- como interagir com o sistema;
- como e quando se sobrepor ao sistema;
- requisitos técnicos para o funcionamento do sistema, incluindo os recursos computacionais necessários e as limitações do sistema, bem como a sua vida útil prevista;
- necessidade de supervisão humana;
- informações sobre a exatidão e o desempenho;
- informações relevantes sobre a avaliação de impacto, incluindo potenciais benefícios e danos, em especial se forem aplicáveis em contextos específicos ou em determinados grupos demográficos (ver B.5.2 e B.5.4);
- revisões dos pedidos sobre os benefícios do sistema;
- atualizações e mudanças no funcionamento do sistema, bem como quaisquer medidas de manutenção necessárias, incluindo a frequência que devem ocorrer;
- informações de contato;
- materiais educativos para utilização do sistema.

Convém que os critérios utilizados pela organização para determinar se e quais informações devem ser fornecidas sejam documentados. Os critérios relevantes incluem, mas não estão limitados ao uso pretendido e utilização indevida razoavelmente previsível do sistema de IA, à expertise do usuário e ao impacto específico do sistema de IA.

As informações podem ser fornecidas aos usuários de várias maneiras, incluindo instruções documentadas de uso, alertas e outras notificações incorporadas no próprio sistema, informações em uma página da web etc. Dependendo de quais métodos a organização usa para fornecer informações, convém que ela valide que os usuários têm acesso a essas informações, e que as informações fornecidas são completas, atualizadas e precisas.

Convém que os critérios utilizados pela organização para determinar se e quais informações devem ser fornecidas sejam documentados. Os critérios relevantes incluem, mas não estão limitados ao uso pretendido e utilização indevida razoavelmente previsível do sistema de IA, à expertise do usuário e ao impacto específico do sistema de IA.

As informações podem ser fornecidas aos usuários de várias maneiras, incluindo instruções documentadas de uso, alertas e outras notificações incorporadas no próprio sistema, informações em uma página da web etc. Dependendo de quais métodos a organização usa para fornecer informações, convém que ela valide que os usuários têm acesso a essas informações, e que as informações fornecidas são completas, atualizadas e precisas.

A.8.2 Relatórios externos

Controle

Convém que a organização forneça recursos às partes interessadas para relatar os impactos adversos do sistema.

Orientações para implementação

Enquanto convém que a operação do sistema seja monitorada para problemas e falhas relatados, também convém que a organização forneça recursos para usuários ou outras partes externas relatarem impactos adversos (por exemplo, injustiça).

A.8.3 Comunicação de incidentes

Controle

Convém que a organização determine e documente um plano para comunicar incidentes aos usuários do sistema.

Orientações para implementação

Os incidentes relacionados ao sistema de IA podem ser específicos do próprio sistema de IA ou relacionados à segurança da informação ou privacidade (por exemplo, uma violação de dados).

Convém que a organização entenda suas obrigações de notificar usuários e outras partes interessadas sobre incidentes, dependendo do contexto em que o opera. Por exemplo, um incidente com um componente de IA que faz parte de um produto que afeta a segurança física pode ter requisitos de notificação diferentes de outros tipos de sistemas. Requisitos legais (como os contratos) e a atividade regulatória podem ser aplicáveis, e podem especificar requisitos para:

- tipos de incidentes que devem ser comunicados;
- prazo para notificação;
- se e quais autoridades devem ser notificadas;
- detalhes necessários a serem comunicados.



A.8 Informação para as partes interessadas

A organização pode integrar atividades de resposta a incidentes e relatórios de IA em seu escopo mais amplo nas atividades de gestão de incidentes organizacionais, mas convém que esteja ciente dos requisitos únicos relacionados aos sistemas de IA ou aos componentes individuais dos sistemas de IA (por exemplo, uma violação de dados pessoais em dados de treinamento, para o sistema, pode ter exigências de comunicação diferentes, relativas à privacidade).

Outras informações

As ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27701 fornecem detalhes adicionais sobre gestão de incidentes para segurança e privacidade, respectivamente.

A.8.4 Informação para partes interessadas

Controle

Convém a organização determinar e documentar suas obrigações de relatar os incidentes sobre o sistema IA para as partes interessadas.

Orientações para implementação

Em alguns casos, uma jurisdição pode exigir que informações sobre o sistema sejam compartilhadas com as autoridades, como reguladores. Informações podem ser relatadas a partes interessadas, como clientes ou reguladores, dentro do prazo adequado. As informações compartilhadas podem incluir, por exemplo:

- documentação técnica do sistema, incluindo, mas não limitado a, conjuntos de dados para treinamento, validação e testes, bem como justificativas de escolhas algorítmicas e registros de verificação e validação;
- riscos relacionados ao sistema;
- resultados das avaliações de impacto;
- logs e outros registros do sistema.

Convém que a organização compreenda as suas obrigações em relação a esta questão e assegure que as informações apropriadas sejam compartilhadas com as autoridades corretas. Adicionalmente pressupõe-se que a organização esteja ciente dos requisitos jurídicos relacionados a informações compartilhadas com a autoridade de aplicação da lei.

Estudo de Caso – Transparência no Uso de IA no Atendimento ao Cliente da FinTech AlfaPay

Contexto:

A AlfaPay, uma fintech que oferece serviços de pagamentos e microcrédito, implantou um sistema de IA para automatizar decisões de concessão de crédito e atendimento ao cliente via chatbot. Com a nova solução, a empresa percebeu a necessidade de fortalecer a comunicação com seus stakeholders — clientes, reguladores e parceiros — sobre como o sistema funcionava, quais dados eram utilizados e como eventuais impactos seriam tratados.

Desafio:

Clientes não entendiam como as decisões de crédito eram tomadas. Além disso, não havia um canal estruturado para relatar dúvidas, impactos adversos ou receber alertas sobre falhas ou incidentes do sistema de IA.

Ações da Empresa (Baseadas no item A.8):

1. Determinação da informação necessária: A AlfaPay mapeou as informações que precisavam ser comunicadas: funcionamento da IA, critérios básicos de decisão, dados utilizados, direitos do cliente e canais de contato.
2. Criação de um portal de transparência de IA: Incluindo explicações acessíveis, vídeos curtos, perguntas frequentes e uma seção de relatórios de impacto.
3. Implantação de um canal exclusivo para feedbacks e incidentes: Integrado ao aplicativo, permitindo relatos anônimos sobre impactos adversos (ex: recusa de crédito indevida).
4. Plano de comunicação de incidentes: Desenvolvido com regras claras sobre prazos e conteúdos mínimos, ativado quando falhas ou alterações importantes ocorrem no sistema.
5. Relatórios periódicos às partes interessadas: Informações como atualizações de modelo, desempenho de IA e impactos sociais passaram a ser enviadas aos órgãos reguladores e parceiros.

Resultados:

- A confiança dos clientes aumentou em 28% (pesquisa de satisfação).
- Redução de reclamações por “falta de explicação” sobre decisões da IA em 45%.
- Cumprimento total das obrigações regulatórias em relatórios de IA.

Lição aprendida:

Comunicar proativamente e com clareza as funcionalidades, impactos e canais de diálogo em torno da IA fortalece a reputação, evita conflitos e contribui para a governança responsável da tecnologia.

Deseja que eu transforme este estudo em slides ou em uma ficha modelo para apresentações?



08

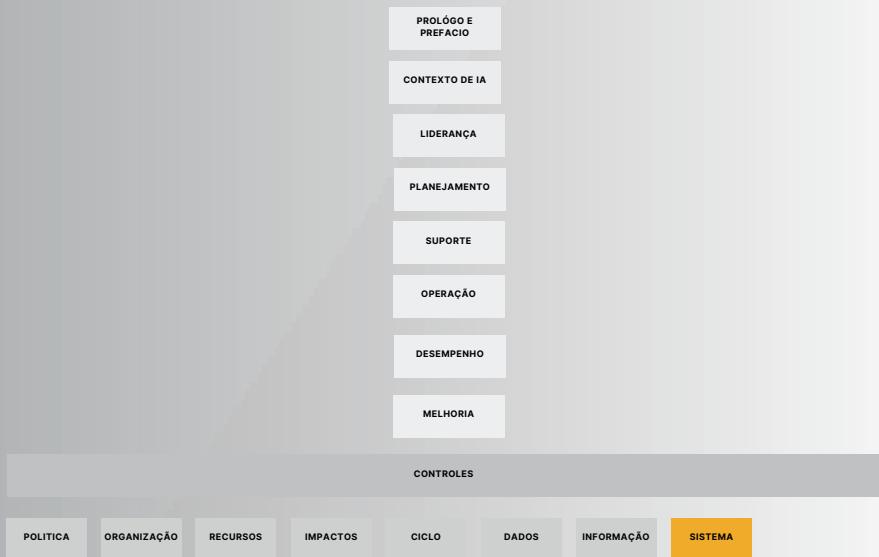
CONTROLE A.9

Uso de sistemas de IA



Uso de Sistemas de IA da ISO/IEC 42001 aborda práticas responsáveis para garantir que os sistemas de inteligência artificial sejam utilizados conforme seus objetivos planejados e de maneira ética e segura. A

organização deve definir processos claros para o uso adequado dos sistemas, estabelecer responsabilidades em todas as etapas do ciclo de vida e garantir que parceiros, fornecedores, clientes e terceiros estejam alinhados com essa abordagem. O foco está em assegurar que os sistemas sejam operados com transparência, segurança, respeito aos direitos dos usuários e aderência à legislação vigente.



As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.9 Uso de sistemas de IA			
Objetivo: Assegurar que a organização use sistemas de IA de forma responsável e de acordo com as políticas organizacionais.			
CÓDIGO	TEMA	CONTROLE	KPIs
A.9.1	Processos para uso responsável de sistemas de IA	A organização deve definir e documentar os processos para o uso responsável dos sistemas de IA.	<p>KPI: Adoção de Processos de Uso Responsável da IA</p> <p>Descrição: Mede o percentual de processos documentados e implementados que garantem o uso ético, seguro e responsável dos sistemas de IA dentro da organização.</p> <p>Fórmula: (Número de processos de uso responsável documentados e implementados / Total de processos previstos) × 100</p> <p>Meta sugerida: ≥ 95%</p> <p>Frequência de Medição: Trimestral</p> <p>Responsável: Comitê de Ética em IA ou Área de Governança de IA</p> <p>Fonte de Dados: Relatórios de conformidade, registros de processos documentados, auditorias internas.</p>
A.9.2	Objetivos para o uso responsável de sistemas de IA	A organização deve identificar e documentar os objetivos para orientar o uso responsável de sistemas de IA.	<p>KPI: Estabelecimento de Objetivos para o Uso Responsável da IA</p> <p>Descrição: Avalia se a organização identificou, documentou e integrou objetivos específicos que orientem o uso responsável de seus sistemas de IA.</p> <p>Fórmula: (Número de objetivos documentados e alinhados às diretrizes éticas / Total de objetivos de IA estabelecidos) × 100</p> <p>Meta sugerida: ≥ 90%</p> <p>Frequência de Medição: Semestral</p> <p>Responsável: Governança de IA ou Comitê de Responsabilidade Algorítmica</p> <p>Fonte de Dados: Plano estratégico de IA, atas de reuniões, documentos de política organizacional.</p>
A.9.3	Uso pretendido do sistema de IA	A organização deve assegurar que o sistema de IA seja usado de acordo com os usos pretendidos do sistema de IA e com a documentação que o acompanha.	<p>KPI: Conformidade de Uso com Finalidade Pretendida do Sistema de IA</p> <p>Descrição: Mede o percentual de sistemas de IA utilizados conforme os propósitos definidos e a documentação oficial associada.</p> <p>Fórmula: (Número de sistemas de IA operando conforme o uso pretendido / Total de sistemas de IA em operação) × 100</p> <p>Meta sugerida: ≥ 95%</p> <p>Frequência de Medição: Trimestral</p> <p>Responsável: Área de Governança de IA ou Auditoria Interna</p> <p>Fonte de Dados: Registros de conformidade, auditorias técnicas, documentação de uso e especificações dos sistemas.</p>



A.9 Uso de sistemas de IA

Objetivo

Assegurar que a organização use sistemas de IA de forma responsável e de acordo com as políticas organizacionais.

A.9.1 Processos para o uso responsável de sistemas de IA

Controle

Convém que a organização defina e documente os processos para o uso responsável de sistemas de IA.

Orientações para implementação

Dependendo do seu contexto, a organização pode ter muitas considerações para determinar se deve usar um sistema de IA em particular. Se o sistema de IA for desenvolvido pela própria organização ou adquirido de terceiros, convém que a organização seja clara sobre quais são essas considerações e desenvolva políticas para abordá-las. Alguns exemplos são:

- aprovações necessárias;
- custos (incluindo o acompanhamento e a manutenção contínuos);
- requisitos de aquisição aprovados;
- requisitos legais aplicáveis à organização.

Caso a organização tenha aceitado políticas para o uso de outros sistemas, ativos etc., essas políticas podem ser incorporadas, se desejado.

A.9.2 Objetivos para o uso responsável de sistemas de IA

Controle

Convém que a organização identifique e documente objetivos para orientar o uso responsável de sistemas de IA.

Orientações para implementação

A organização que opera em diferentes contextos pode ter diferentes expectativas e objetivos sobre o que constitui o desenvolvimento responsável de sistemas de IA. Dependendo de seu contexto, convém que a organização identifique seus objetivos relacionados ao uso responsável. Alguns objetivos incluem:

- justiça;
- responsabilização;
- transparência;
- explicabilidade;
- confiabilidade;
- segurança física;
- robustez e redundância;
- privacidade e segurança;
- acessibilidade.

Uma vez definidos, convém que a organização implemente mecanismos para atingir seus objetivos dentro da organização. Isso pode incluir determinar se uma solução de terceiros atende aos objetivos da organização ou se uma solução desenvolvida internamente é aplicável para o uso pretendido. Convém que a organização determine em quais estágios do ciclo de vida do sistema de IA, objetivos de supervisão humana podem ser incorporados. Isso pode incluir:

- envolver revisores humanos para verificar os resultados do sistema de IA, incluindo ter autoridade para sobrepor decisões tomadas por sistemas de IA;
- assegurar que a supervisão humana seja incluída, se necessário, para a utilização aceitável do sistema de IA de acordo com as instruções ou outra documentação associada à implantação pretendida do sistema de IA;

- monitorar o desempenho do sistema de IA, incluindo a exatidão das saídas do sistema de IA;
- comunicar às partes interessadas relevantes as preocupações relacionadas com as saídas do sistema de IA e o seu impacto;
- relatar preocupações com mudanças no desempenho ou na capacidade do sistema de IA de produzir saídas corretas sobre os dados de produção;
- considerar se a tomada de decisão automatizada é apropriada para uma abordagem responsável ao uso de um sistema de IA e ao uso pretendido do sistema de IA.

A necessidade de supervisão humana pode ser informada pelas avaliações de impacto dos sistemas de IA (ver A.5). Convém que o pessoal envolvido em atividades de supervisão humana relacionadas ao sistema de IA seja informado e treinado sobre o sistema de IA, bem como tenha compreensão das instruções e outras documentações relacionadas ao sistema de IA, de modo que cumpram efetivamente seus deveres para satisfazer os objetivos de supervisão humana. Ao relatar problemas de desempenho, a supervisão humana pode aperfeiçoar os resultados do monitoramento automatizado.

Outras informações

O Anexo C fornece exemplos de objetivos organizacionais para a gestão de riscos, que podem ser úteis para determinar os objetivos para o uso do sistema de IA.

A.9.3 Uso pretendido do sistema de IA

Controle

Convém que a organização assegure que o sistema de IA seja utilizado de acordo com seu uso pretendido e sua documentação associada.

Orientações para implementação

Convém que o sistema de IA seja implantado de acordo com as instruções e demais documentações associadas ao sistema de IA (ver A.8.2). A implantação pode requerer recursos específicos para dar suporte à implantação, incluindo a necessidade de assegurar que a supervisão humana seja aplicada conforme necessário (ver A.9.3). Pode ser necessário que, para o uso aceitável do sistema de IA, os dados em que o sistema de IA é utilizado estejam alinhados com a documentação associada ao sistema de IA para assegurar que o desempenho do sistema de IA seja exato.

Convém que o funcionamento do sistema de IA seja monitorado (ver A.6.2). Onde a implantação correta do sistema de IA, de acordo com as suas instruções associadas, causar preocupações relacionadas ao impacto para as partes interessadas relevantes ou aos requisitos legais da organização, convém que a organização comunique suas preocupações ao pessoal pertinente dentro da organização, bem como a quaisquer fornecedores terceirizados do sistema de IA.



A.9 Uso de sistemas de IA



Convém que a organização mantenha logs de eventos ou outras documentações relacionadas à implantação e operação do sistema de IA, que possam ser usados para demonstrar que o sistema de IA está sendo usado como pretendido ou para ajudar na comunicação de preocupações relacionadas ao uso pretendido do sistema de IA. O período de tempo durante o qual logs de eventos e outras documentações são mantidos depende do uso pretendido do sistema de IA, das políticas da organização e das obrigações legais pertinentes para a retenção de dados.

Estudo de Caso – Uso Responsável de Sistemas de IA na Empresa Verdata Solutions

Contexto:

A Verdata Solutions é uma empresa de tecnologia especializada em serviços de análise preditiva para o setor financeiro. Ela desenvolveu uma solução de IA para prever o risco de inadimplência em pedidos de crédito.

Desafio:

Apesar da eficácia técnica da ferramenta, a empresa começou a receber reclamações de clientes e parceiros sobre possíveis decisões injustas, com base em critérios pouco transparentes.

Ação com base na Seção A.9 da ISO/IEC 42001:

A Verdata decidiu implementar um programa formal de uso responsável do sistema de IA, adotando os seguintes passos:

Definição de Objetivos de Uso Responsável (A.9.2):

1. A empresa estabeleceu que a IA deveria:
 - Apoiar decisões humanas, sem substituí-las.
 - Explicar os fatores que influenciaram a previsão de inadimplência.
 - Minimizar viés contra perfis socioeconômicos.

Processo Documentado de Uso (A.9.1):

1. Criou-se uma política de uso do sistema de IA, incluindo:
 - Escopo de uso permitido.
 - Limites éticos e legais.
 - Responsabilidades dos operadores.

Verificação de Aderência ao Uso Pretendido (A.9.3):

Auditórias internas verificaram se os usuários estavam aplicando a IA apenas nos contextos permitidos. Casos fora do escopo foram bloqueados automaticamente.

1. Treinamento dos Usuários (A.9.4):
2. Todos os analistas passaram por capacitação obrigatória sobre o uso ético, seguro e responsável do sistema.

Resultados:

- Redução em 40% das reclamações relacionadas ao uso da IA.
- Melhora da confiança de parceiros regulatórios.
- Conformidade com a ISO 42001 e aumento da reputação organizacional.



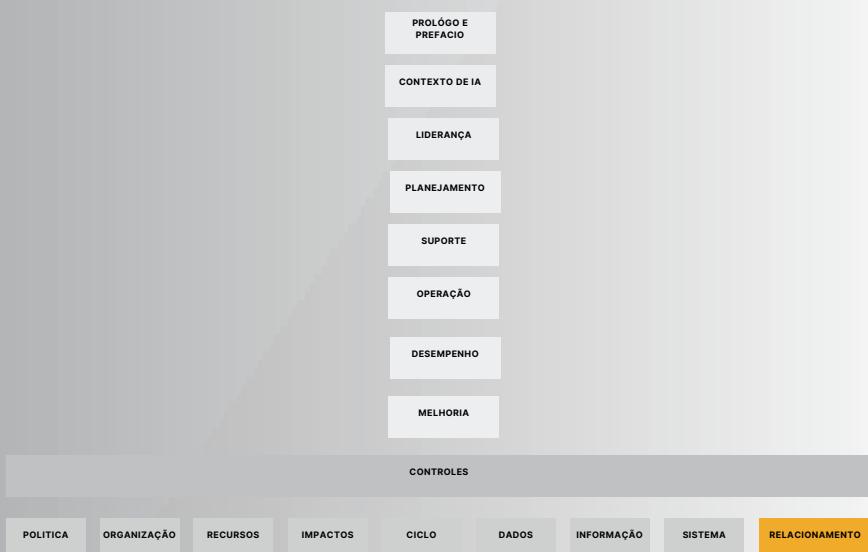
08

CONTROLE A.10

Relacionamento com clientes e terceiros



Relacionamento com clientes e terceiros da ISO/IEC 42001 destaca a importância de garantir que o uso e desenvolvimento de sistemas de IA por fornecedores, parceiros e clientes esteja alinhado com os princípios da organização para uma IA responsável. Isso inclui definir responsabilidades no ciclo de vida da IA entre as partes envolvidas, estabelecer critérios de conformidade em contratos e garantir que expectativas e necessidades dos clientes sejam consideradas. O objetivo é assegurar confiança, transparência e integridade nas interações com terceiros.



As Tabelas da ISO/IEC 42001 apresenta controles sugeridos para apoiar a organização na gestão de riscos e no cumprimento dos objetivos de IA. Esses controles ajudam a garantir segurança, ética e eficácia no uso da inteligência artificial. No entanto, sua aplicação não é obrigatória para todos os casos. A organização pode adaptar ou desenvolver controles próprios, desde que sejam eficazes. O importante é que os riscos sejam tratados e os objetivos do sistema de gestão de IA sejam alcançados.



Tabela A.1 – Objetivos de controle e controles

A.10 Relacionamento com clientes e terceiros			
Objetivo: Assegurar que a organização comprehenda suas responsabilidades e permaneça responsabilizada por elas, e que riscos sejam repartidos de forma adequada quando terceiros estiverem envolvidos em qualquer fase do ciclo de vida do sistema de IA.			
CÓDIGO	TEMA	CONTROLE	KPIs
A.10.1	Atribuição de responsabilidades	<p>A organização deve assegurar que as responsabilidades dentro de seu ciclo de vida do sistema de IA sejam atribuídas entre a organização, seus parceiros, fornecedores, clientes e terceiros.</p>	<p>KPI: Cobertura de Responsabilidades no Ciclo de Vida do Sistema de IA</p> <p>Descrição: Mede o percentual de etapas do ciclo de vida dos sistemas de IA com responsabilidades formalmente atribuídas entre a organização, parceiros, fornecedores, clientes e terceiros.</p> <p>Fórmula: $\{Nº\text{ de etapas do ciclo de vida com responsabilidades formalizadas}\} \backslash \{Total\text{ de etapas do ciclo de vida do sistema de IA}\} \times 100$</p> <p>Meta sugerida: $\geq 95\%$</p> <p>Frequência de medição: Semestral</p> <p>Responsável: Área de Governança de IA ou Gestão de Riscos</p> <p>Fonte de Dados: Documentos contratuais, matriz RACI, registros de governança de IA</p>
A.10.2	Fornecedores	<p>A organização deve estabelecer um processo para assegurar que o uso de serviços, produtos ou materiais providos por fornecedores esteja alinhado com a abordagem da organização para o desenvolvimento e uso responsáveis de sistemas de IA.</p>	<p>KPI: Alinhamento de Fornecedores com a Política de IA Responsável</p> <p>Descrição: Mede o percentual de fornecedores avaliados e formalmente alinhados à política e princípios de uso responsável de IA da organização.</p> <p>Fórmula: $\{Número\text{ de fornecedores com avaliação e cláusulas de IA responsável}\} \backslash \{Total\text{ de fornecedores críticos para IA}\} \times 100$</p> <p>Meta sugerida: $\geq 90\%$</p> <p>Frequência de medição: Anual</p> <p>Responsável: Governança de IA / Suprimentos / Jurídico</p> <p>Fonte de Dados: Contratos de fornecimento, políticas de compliance, registros de due diligence de IA</p>
A.10.3	Clientes	<p>A organização deve assegurar que sua abordagem responsável para o desenvolvimento e uso de sistemas de IA considere as expectativas e necessidades dos clientes</p>	<p>KPI: Consideração das Expectativas dos Clientes na Governança de IA</p> <p>Descrição: Avalia se as expectativas e necessidades dos clientes foram consideradas na concepção, desenvolvimento e uso de sistemas de IA.</p> <p>Fórmula: $\{Número\text{ de projetos de IA com requisitos validados por clientes}\} \backslash \{Total\text{ de projetos de IA entregues}\} \times 100$</p> <p>Meta sugerida: $\geq 85\%$</p> <p>Frequência de medição: Semestral</p> <p>Responsável: Gestão de Produtos / Governança de IA / Atendimento ao Cliente</p> <p>Fonte de Dados: Registros de validação com stakeholders, atas de reuniões com clientes, relatórios de testes de usabilidade e feedbacks documentados</p>



A.10 Relacionamento com clientes e terceiros

Objetivo

Assegurar que a organização entenda suas responsabilidades e permaneça responsabilizada, e que os riscos sejam adequadamente rateados quando terceiros estiverem envolvidos em qualquer fase do ciclo de vida do sistema de IA.

A.10.1 Atribuição de responsabilidades

Controle

Convém que a organização assegure que as responsabilidades dentro de seu ciclo de vida do sistema de IA sejam alocadas entre a organização, seus parceiros, fornecedores, clientes e terceiros.

Orientações para implementação

Em um ciclo de vida de um sistema de IA, as responsabilidades podem ser divididas entre partes que fornecem dados, partes que fornecem algoritmos e modelos, e partes que desenvolvem ou usam o sistema de IA e são responsáveis em relação a algumas ou a todas as partes interessadas. Convém que a organização documente todas as partes que intervêm no ciclo de vida do sistema de IA e seus papéis, e determine suas responsabilidades.

Quando a organização fornece sistemas de IA a terceiros, convém que assegure que adota uma abordagem responsável para desenvolver sistemas de IA. Ver os controles e orientações na Seção A.6. Convém que a organização seja capaz de fornecer a documentação necessária (ver A.6.2 e A.8.2) do sistema de IA para as partes interessadas relevantes e para o terceiro o qual a organização está fornecendo o sistema de IA.

Quando os dados tratados incluem DP(dados pessoais), as responsabilidades geralmente são divididas entre os operadores e os controladores de DP. A ABNT NBR ISO/IEC 29100 fornece mais informações sobre controladores de DP e operadores de DP. Nos casos em que a privacidade dos DP deva ser preservada, convém que sejam considerados controles como os descritos na ABNT NBR ISO/IEC 27701.

Com base nas atividades de tratamento de dados da organização e do sistema de IA em DP e no papel da organização na aplicação e desenvolvimento de sistemas de IA ao longo de seu ciclo de vida, a organização pode ter o papel de um controlador de DP (ou controlador conjunto de DP), operador de DP ou ambos.

A.10.2 Fornecedores

Controle

Convém que a organização estabeleça um processo que assegure que o uso de serviços, produtos ou materiais providos por fornecedores se alinhe com a abordagem da organização no desenvolvimento e uso responsáveis de sistemas de IA.

Orientações para implementação

As organizações que desenvolvem ou usam um sistema de IA podem utilizar os fornecedores de várias formas, desde a aquisição de conjuntos de dados, algoritmos ou modelos de aprendizado de máquina, ou outros componentes de um sistema, como bibliotecas de software, até um sistema de IA completo para sua própria utilização ou como parte de outro produto (por exemplo, um veículo).

Convém que as organizações considerem os diferentes tipos de fornecedores, o que eles fornecem o nível variável de risco que isso pode representar para o sistema e para a organização comum todo ao determinar a seleção de fornecedores, os requisitos estabelecidos para esses fornecedores e os níveis de monitoramento e avaliação contínuos necessários para esses fornecedores.

Convém que as organizações documentem como o sistema de IA e os componentes do sistema de IA são integrados nos sistemas de IA desenvolvidos ou utilizados pela organização.

Quando a organização considera que o sistema de IA ou os componentes do sistema de IA de um fornecedor não têm o desempenho pretendido ou podem resultar em impactos para indivíduos ou grupos de indivíduos, ou ambos, e sociedades, e que não estão alinhados com a abordagem responsável dos sistemas de IA adotada pela organização, convém que a organização exija que o fornecedor tome ações corretivas. A organização pode decidir trabalhar com o fornecedor para atingir esse objetivo.

Convém que a organização assegure que o fornecedor de um sistema de IA forneça documentação apropriada e adequada relacionada ao sistema de IA (ver A.6.2 e A.8.2).

A.10.4 Clientes

Controle

Convém que a organização assegure que sua abordagem responsável para o desenvolvimento e uso de sistemas de IA considere as expectativas e necessidades dos clientes.

Orientações para implementação

Convém que a organização compreenda as expectativas e necessidades dos clientes quando fornecer um produto ou serviço relacionado com um sistema de IA (isto é, quando ela própria for um fornecedor).

Estas expectativas podem surgir sob a forma de requisitos para o próprio produto ou serviço, durante uma fase de projeto ou engenharia, ou sob a forma de requisitos contratuais ou acordos de utilização geral.

Uma organização pode ter muitos tipos diferentes de relações com os clientes, e todos eles podem ter necessidades e expectativas diferentes. Convém que a organização compreenda, em particular, a natureza complexa das relações entre fornecedores e clientes e compreenda onde a responsabilidade recai sobre o fornecedor do sistema de IA e onde recai sobre o cliente, sem deixar de satisfazer as necessidades e expectativas deste.

Por exemplo, a organização pode identificar riscos relacionados ao uso de seus produtos e serviços de IA pelo cliente e pode decidir tratar os riscos identificados, fornecendo informações apropriadas ao seu cliente, para que ele possa tratar os riscos correspondentes.

Como exemplo de informação apropriada, quando um sistema de IA é válido para um determinado domínio de uso, convém que os limites do domínio sejam comunicados ao cliente. Ver A.6.2 e A.8.2.



Estudo de Caso: Aliança Digital e a Governança Responsável com Terceiros

Cenário

A Aliança Digital, uma empresa de tecnologia educacional, desenvolveu uma plataforma de tutoria online baseada em IA para personalizar o aprendizado de estudantes. A solução utiliza modelos preditivos e algoritmos de recomendação desenvolvidos em parceria com um fornecedor de IA e integrados por uma consultoria externa.

Desafio

Durante uma auditoria de conformidade, foram detectadas lacunas no alinhamento entre os fornecedores de tecnologia e os princípios éticos definidos pela Aliança Digital. Entre os riscos encontrados estavam o uso de dados de treinamento não verificados, ausência de documentação técnica compartilhada com os clientes e ausência de canal de relato para impactos adversos.

Ações Adotadas

Baseada na ISO/IEC 42001, a Aliança Digital implementou as seguintes medidas:

1. Contrato com cláusulas específicas sobre IA responsável: Todos os fornecedores passaram a assinar contratos que exigem transparência no uso de dados, explicabilidade dos modelos e alinhamento com os princípios de ética da organização.
2. Processo de homologação técnica e ética de terceiros: Foi criado um comitê de avaliação que valida as práticas dos fornecedores quanto à proteção de dados, segurança e mitigação de vieses.
3. Cocriação com clientes: As escolas clientes foram convidadas para participar de oficinas de validação dos objetivos da IA, garantindo alinhamento com suas expectativas e realidades educacionais.
4. Canal de comunicação para impactos adversos: Um canal anônimo foi ativado para que usuários e clientes possam reportar falhas, impactos ou uso indevido da IA.
5. Monitoramento contínuo do ciclo de vida dos serviços de terceiros: Indicadores passaram a acompanhar o cumprimento de obrigações contratuais e a performance dos algoritmos terceirizados.

Resultados

- 95% dos parceiros adequaram seus serviços aos requisitos éticos e técnicos.
- Redução de 60% nos relatos de inconsistências nos algoritmos.
- A confiança dos clientes aumentou, refletida em uma taxa de renovação de 92% no último ano.



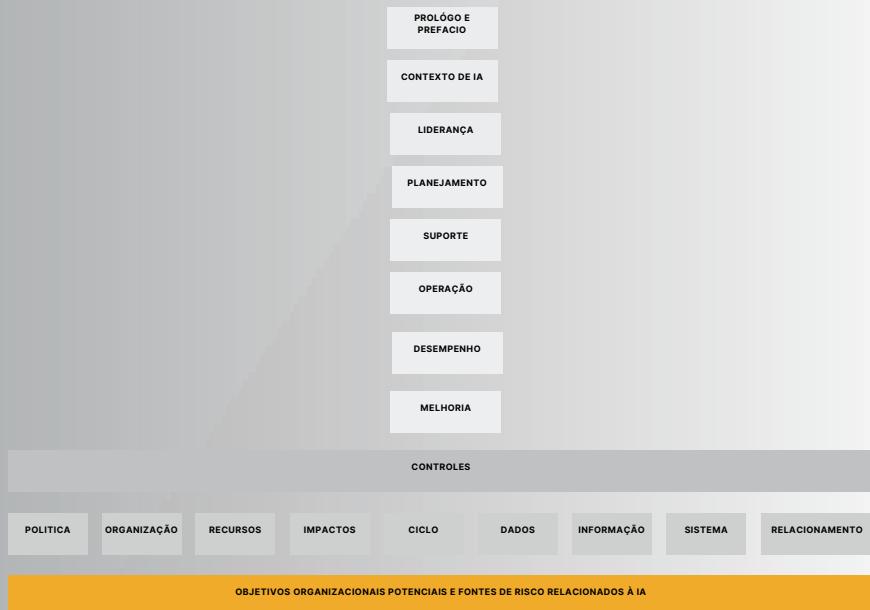
09

INFORMATIVO

Objetivos organizacionais potenciais e fontes de risco relacionados à IA



Na ISO/IEC 42001, os objetivos organizacionais potenciais e as fontes de risco relacionados à IA são elementos fundamentais para garantir uma implementação ética, segura e eficaz de sistemas de inteligência artificial.



GERAL

Este Anexo descreve objetivos organizacionais potenciais, fontes de risco e descrições que podem ser considerados pela organização ao gerenciar riscos. Este Anexo não pretende ser exaustivo nem aplicável a todas as organizações. Convém que a organização determine os objetivos e as fontes de risco considerados relevantes para ela. A ABNT NBR ISO/IEC 23894 fornece informações mais detalhadas sobre esses objetivos e fontes de risco, e sua relação com a gestão de riscos. A avaliação de sistemas de IA, inicialmente, regularmente e quando necessário, fornece evidências para avaliar quando um sistema de IA está sendo utilizado contra os objetivos da organização.

B.2 Objetivos

B.2.1 Responsabilização

O uso de IA pode mudar as estruturas de responsabilização existentes. Onde, antes, as pessoas seriam responsabilizadas por suas ações, suas ações agora podem ser apoiadas por ou baseadas no uso de um sistema de IA.

B.2.2 Expertise em IA

É necessária a seleção de especialistas dedicados com conjuntos de habilidades interdisciplinares e expertise na avaliação, desenvolvimento e implantação de sistemas de IA.

B.2.3 Disponibilidade e qualidade dos dados de treinamento e de teste

Os sistemas de IA baseados em ML precisam de dados de treinamento, validação e teste para treinar e verificar os sistemas para o comportamento pretendido.

B.2.4 Impacto ambiental

O uso de IA pode ter impactos positivos e negativos no ambiente.

B.2.5 Justiça

A aplicação inadequada de sistemas de IA para a tomada de decisões automatizadas pode ser injusta para pessoas ou grupos de pessoas.

B.2.6 Manutenibilidade

A manutenibilidade está relacionada à capacidade da organização de lidar com modificações do sistema de IA para corrigir defeitos ou se ajustar a novos requisitos.

B.2.7 Privacidade

O mau uso ou a divulgação de dados pessoais e sensíveis (por exemplo, registos de saúde) podem trazer efeitos prejudiciais para os sujeitos de dados.

B.2.8 Robustez

Em IA, as propriedades de robustez demonstram a capacidade (ou incapacidade) de o sistema ter desempenho comparável com dados novos, como nos dados nos quais foi treinado ou nos dados de operações típicas.

B.2.9 Segurança física

A segurança física refere-se à expectativa de que um sistema de IA não conduza, em condições especificadas, a um estado em que a vida humana, a saúde, a propriedade ou o ambiente estejam ameaçadas.

B.2.10 Segurança

No contexto de IA e, em particular, no que diz respeito aos sistemas de IA baseados em abordagens de ML, convém que novas questões de segurança sejam consideradas, além das preocupações clássicas de segurança da informação e de sistema.

B.2.11 Transparência e explicabilidade

A transparência está relacionada tanto às características de uma organização que opera sistemas de IA quanto a esses próprios sistemas. A explicabilidade refere-se a explicações de fatores importantes que influenciam os resultados do sistema de IA que são fornecidos às partes interessadas de uma forma compreensível para os seres humanos.

B.3 Fontes de risco

B.3.1 Complexidade do ambiente

Quando os sistemas de IA operam em ambientes complexos, onde a gama de situações é ampla, pode haver incerteza sobre o desempenho e, portanto, uma fonte de risco (por exemplo, ambiente complexo de direção autônoma).

B.3.2 Falta de transparência e explicabilidade

A incapacidade de fornecer informações adequadas às partes interessadas pode ser uma fonte de risco (isto é, em termos de fidedignidade e responsabilização da organização).

B.3.3 Nível de automação

O nível de automação pode ter um impacto em várias áreas de preocupação, como segurança física, justiça ou segurança.

B.3.4 Fontes de risco relacionadas ao aprendizado de máquina

A qualidade dos dados usados para ML e o processo usado para coletar dados podem ser fontes de risco, pois podem impactar objetivos como segurança e robustez (por exemplo, devido a problemas na qualidade ou envenenamento de dados).

B.3.5 Questões de hardware do sistema

As fontes de risco relacionadas ao hardware incluem erros de hardware baseados em componentes defeituosos ou transferência de modelos de ML treinados entre sistemas diferentes.

B.3.6 Questões de ciclo de vida do sistema

As fontes de risco podem aparecer ao longo de todo o ciclo de vida do sistema de IA (por exemplo, falhas no projeto, implantação inadequada, falta de manutenção, questões relacionadas ao descomissionamento).

B.3.7 Prontidão tecnológica

As fontes de risco podem estar relacionadas à tecnologia menos madura devido a fatores desconhecidos (por exemplo, limitações de sistema e condições limitrofes, desvio de desempenho), mas também devido à tecnologia mais madura devido à complacência tecnológica.

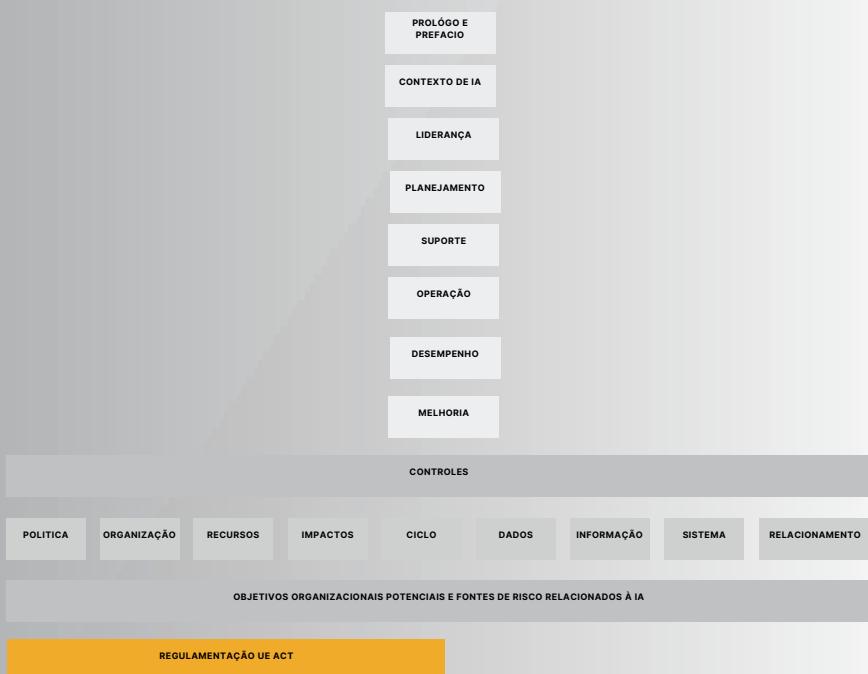


10

REGULAMENTAÇÃO UE ACT x ISO 42.001



O EU AI Act e a ISO/IEC 42001 representam duas abordagens complementares para garantir o uso responsável da inteligência artificial. Enquanto o AI Act é uma lei obrigatória da União Europeia que regula sistemas com base em níveis de risco, a ISO 42001 é uma norma internacional voluntária focada na criação de um sistema de gestão organizacional da IA. Ambos enfatizam a importância da transparência, gestão de riscos, responsabilidade e direitos humanos. A principal diferença está na obrigatoriedade legal do AI Act, com sanções aplicáveis, e no caráter orientador da ISO. Juntos, oferecem uma base robusta para empresas que buscam conformidade e governança de IA. A adoção integrada fortalece a confiança, segurança e inovação ética.



UE AI ACT

REGULAMENTO (UE) 2024/1689 DO PARLAMENTO EUROPEU E DO CONSELHO
 de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.o 300/2008, (UE) n.o 167/2013, (UE) n.o 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial)

Capítulo 1: Como a União Europeia Está Cuidando do Uso Responsável da IA

Imagine que cada país da Europa resolvesse criar suas próprias regras para uso da inteligência artificial. Seria uma confusão. Uma empresa poderia vender um sistema em um país e ser proibida no outro. Para evitar isso, a União Europeia criou uma regra única — um regulamento — que vale para todos os seus países. O objetivo é garantir que os sistemas de IA funcionem bem e com segurança em qualquer lugar da União Europeia.

A União Europeia quer que a IA avance, mas com cuidado e responsabilidade. Ao classificar os sistemas de IA por risco, o regulamento mostra que a confiança vem antes da tecnologia. E isso só será possível se cada empresa souber onde está pisando — e seguir o caminho certo, com ética e transparência.

Mas essa regra não veio para bagunçar o que já existe. Ela respeita leis importantes como a proteção de dados pessoais, os direitos dos trabalhadores e os direitos do consumidor. Se um trabalhador se sentir prejudicado por uma decisão tomada por uma IA, por exemplo, ele continua tendo direito à indenização, como já previsto em outras leis.

O regulamento também não tira o direito das pessoas de fazer greve ou negociar melhorias nas condições de trabalho — esses direitos continuam intactos. Além disso, ele não muda leis específicas que protegem menores de idade ou regulam relações de trabalho, desde que essas leis sigam os princípios da União Europeia.

Então, se você trabalha numa empresa de tecnologia, esse regulamento não vai te impedir de inovar. Ele só quer ter certeza de que a IA será usada de forma ética, transparente e responsável. E mais: o regulamento pede que as empresas mantenham registros técnicos e sejam claras sobre como seus sistemas de IA funcionam — para que todo mundo possa confiar no que está sendo usado.

Esse é um passo importante para garantir que, ao mesmo tempo em que a Europa lidera no uso de tecnologias modernas, os direitos das pessoas estejam sempre em primeiro lugar.

Capítulo 2 — Nem Toda IA É Igual: Como a Europa Classifica os Riscos

Você já pensou que um sistema de IA usado para recomendar filmes é bem diferente de outro que decide se uma pessoa pode conseguir crédito num banco? Pois é exatamente essa diferença que a União Europeia quer deixar bem clara com o novo regulamento: nem toda IA oferece o mesmo tipo de risco.

Para lidar com isso, o regulamento europeu criou uma classificação por níveis de risco. Funciona como um semáforo:

Risco Inaceitável — IA Proibida

Esse é o tipo de IA que vai contra valores básicos da União Europeia. São sistemas que colocam em risco a dignidade ou a liberdade das pessoas. Exemplos incluem:

- Sistemas que fazem manipulação psicológica subliminar para influenciar decisões;
- Classificação social automatizada, como dar ou tirar pontos com base no comportamento de uma pessoa (como visto em filmes distópicos);
- Reconhecimento facial em tempo real em locais públicos para controle de pessoas, exceto em casos muito específicos e sob supervisão.

Esses sistemas não podem ser usados na Europa. Ponto.

Alto Risco — Controle Rigoroso

Aqui estão os sistemas de IA que podem afetar a vida das pessoas de maneira significativa. Eles não são proibidos, mas exigem regras rigorosas para serem usados. Exemplos:

- Sistemas que tomam decisões em processos seletivos de emprego;
- IA em infraestruturas críticas, como eletricidade ou transporte;
- Sistemas que ajudam decisões em áreas como educação, justiça ou saúde.

Essas IAs precisam passar por testes, ter documentação técnica clara, supervisão humana e garantir que os dados usados não tenham viés.

Conexão com a ISO 42001: Esse nível de risco exige que as empresas tenham um sistema de gestão robusto, como o definido na ISO 42001. Isso inclui identificar riscos, documentar decisões, monitorar impactos e garantir transparência e responsabilidade.

Risco Limitado — Informação e Transparência

Algumas IAs não afetam tanto a vida das pessoas, mas ainda podem influenciar decisões. Nesses casos, o regulamento exige que as pessoas saibam que estão interagindo com uma IA. Por exemplo:

- Chatbots;
- IA que gera imagens ou textos

Esses sistemas devem informar claramente ao usuário que não são humanos e devem seguir regras de ética e respeito aos direitos.

Risco Mínimo ou Nenhum — Livre Uso

Esses são os sistemas usados para entretenimento, produtividade ou apoio, como:

- Filtros de fotos;
- Ferramentas de tradução;
- Sistemas de recomendação de produtos.

A boa notícia é que mais de 90% das aplicações de IA hoje entram nessa categoria. Elas continuam livres para circular sem necessidade de aprovação prévia.

Capítulo 3 — Quem Cuida da IA? A Importância da Responsabilidade e da Governança

Quando uma empresa decide usar inteligência artificial, uma pergunta se torna inevitável: quem é responsável se algo der errado?

Assim como em um avião temos piloto, copiloto e torre de controle, nos sistemas de IA também precisamos de papéis bem definidos. O regulamento europeu deixa isso claro: não basta usar IA — é preciso governar esse uso com responsabilidade.



UE AI ACT

O que é “governança da IA”?

Governança é um conjunto de regras, processos e pessoas que cuidam da IA desde o nascimento (desenvolvimento) até o fim (desativação). É ela quem garante que a IA:

- Seja segura;
- Siga as leis;
- Respeite os direitos humanos;
- Esteja alinhada com os valores da empresa.

Segundo a ISO 42001, isso significa definir funções, treinar pessoas, revisar políticas e acompanhar continuamente o desempenho e os riscos dos sistemas de IA.

Quem são os responsáveis?

O AI Act e a ISO 42001 indicam que diferentes atores devem estar envolvidos na governança. Veja alguns papéis típicos:

Papel: Alta liderança (CEO, Diretores)

Função: Principal: Apoiar a IA de forma ética e estratégica.

Papel: Líder de IA ou Comitê de IA

Função: Coordenar políticas, treinamentos e decisões técnicas.

Papel: TI e Dados

Função: Garantir segurança, qualidade e funcionamento dos sistemas.

Papel: Jurídico e Compliance

Função: Monitorar se a IA respeita leis como LGPD e regulamentos setoriais.

Papel: RH, Marketing, Atendimento

Função: Usar a IA com ética no dia a dia e identificar riscos.

Dica prática (ISO 42001 - A.3): Todas essas responsabilidades devem estar documentadas e alinhadas com as políticas de IA da empresa.

E se alguém tiver uma preocupação?

O AI Act exige que a empresa ofereça canais seguros para denúncias. Qualquer pessoa deve poder alertar sobre:

- Discriminação causada por IA;
- Uso indevido de dados pessoais;
- Falhas graves de decisão automatizada.

Esses canais devem ser anônimos, com garantia de que ninguém será punido por falar. Isso também está na ISO (A.3.3), reforçando a ideia de transparência e confiança.

Por que tudo isso importa?

Imagine um sistema de IA que nega um financiamento bancário com base em dados enviesados. Ou um algoritmo de triagem médica que ignora sintomas por falta de representatividade dos dados. Nesses casos, a responsabilidade precisa estar clara: quem criou, quem usou, quem deveria ter revisado?

Sem governança, a IA vira um “navio sem leme” – e isso pode causar danos graves, multas e perda de confiança.

Capítulo 4 – O Que a IA Precisa Para Funcionar? Recursos Humanos, Dados e Tecnologia

Você já parou para pensar no que é necessário para que um sistema de IA funcione bem?

Assim como um carro precisa de combustível, manutenção e um motorista treinado, a IA também exige uma base sólida de recursos para operar com eficiência, segurança e responsabilidade.

Quais são os “recursos” de um sistema de IA?

A ISO 42001 e o AI Act concordam: usar IA não é apenas “ligar o sistema”. É preciso garantir uma série de recursos organizacionais, como:

Recursos humanos: Pessoas com conhecimento técnico, jurídico, ético e de negócio sobre IA.

Dados: Informações de qualidade, sem vieses, e com origem conhecida e segura.

Ferramentas e software: Plataformas, frameworks, APIs e outras soluções técnicas.

Infraestrutura de TI: Servidores, cloud, processamento e segurança digital adequada.

Processos organizacionais: Treinamentos, procedimentos, avaliações e planos de ação.

Pessoas competentes = IA de confiança

Não adianta ter um sistema de IA incrível se ninguém sabe usá-lo ou analisá-lo corretamente. Por isso, a ISO 42001 exige que:

- A empresa identifique quem precisa saber o quê;
- Dê treinamento adequado a cada pessoa envolvida com IA;
- Avalie se as ações foram eficazes;
- Documente tudo isso.

💡 Exemplo prático: Um time de atendimento precisa entender os limites do chatbot de IA, para saber quando transferir para um humano.

Dados bons, decisões melhores

A IA só aprende com os dados que recebe. Se os dados forem ruins, incompletos ou preconceituosos, a IA pode:

- Discriminar pessoas sem perceber;
- Reproduzir erros do passado;
- Oferecer resultados errados.

Bons dados = IA justa, segura e útil.

Por isso, a empresa deve:

- Garantir qualidade, origem e atualidade dos dados;
- Documentar como os dados são obtidos, preparados e validados;
- Proteger os dados com boas práticas de segurança e privacidade.

Tecnologia que sustenta tudo

A infraestrutura da IA precisa ser robusta e confiável. Isso inclui:

- Sistemas seguros contra ataques;
- Capacidade de processamento adequada;
- Backups e continuidade de serviço;
- Ferramentas de monitoramento.



UE AI ACT

Pense como um hospital usando IA para triagem de emergências — a falha de energia ou de rede pode custar vidas.

Capítulo 5 – Classificação e Gerenciamento de Riscos da IA na União Europeia

Introdução ao Capítulo:

Neste capítulo, vamos explorar como a União Europeia organiza os riscos associados à Inteligência Artificial e quais obrigações cada tipo de sistema deve seguir. A classificação por risco é o coração do EU AI Act, pois é a partir dela que se definem as regras. Essa abordagem está totalmente alinhada com o que a ISO/IEC 42001 propõe em seus controles relacionados à avaliação de risco e impacto.

Seção 1 – A Pirâmide de Risco da IA

O modelo de classificação de risco da União Europeia traz clareza e proteção.
Junto com a ISO/IEC 42001, forma uma dupla poderosa para que empresas usem IA de forma responsável, segura e com foco no bem-estar humano.

O regulamento europeu classifica os sistemas de IA em quatro níveis de risco:

Risco Inaceitável

São sistemas proibidos, pois representam ameaça clara aos direitos fundamentais.
 Exemplo: IA usada para manipulação subconsciente ou pontuação social (tipo Black Mirror).

Risco Elevado

São permitidos, mas com regras rígidas. Usam IA para decisões que afetam a vida das pessoas.
 Exemplo: IA em recrutamento, justiça, crédito, saúde ou educação.

Risco Limitado

Devem seguir obrigações de transparência, como avisar o usuário de que está interagindo com uma IA.
 Exemplo: Chatbots, deepfakes, assistentes virtuais.

Risco Mínimo ou Nulo

São livres de exigências adicionais, como sistemas de recomendação de músicas.
 Exemplo: Spotify ou filtros de redes sociais.

Seção 2 – Como Isso Se Conecta com a ISO/IEC 42001

A norma ISO exige que organizações realizem avaliações de risco e impacto (ver seções 6.1.2, B.5 e A.6 da ISO 42001). Isso inclui:

- Avaliar os impactos sociais, psicológicos e jurídicos da IA;
- Criar planos para mitigar riscos;
- Documentar todas as análises realizadas;
- Definir responsáveis por decisões sensíveis.

Na prática, a ISO oferece um sistema de gestão que ajuda a empresa a cumprir o que o EU AI Act exige — principalmente em IA de risco elevado.

Seção 3 – Estudo de Caso (Fictício)

Empresa: TalentAI – Plataforma de Recrutamento com IA

A TalentAI usava algoritmos para analisar currículos e prever o desempenho de candidatos. Após a entrada em vigor do EU AI Act, a empresa foi classificada como sistema de risco elevado, por afetar a empregabilidade de pessoas.

Para se adequar:

- Realizou uma avaliação de impacto algorítmico (AIA) conforme ISO/IEC 42001.
- Garantiu a explicabilidade das decisões da IA (dashboard explicativo).
- Criou um canal de relato de preocupações por candidatos e clientes.
- Nomeou um responsável pela governança de IA na empresa.

Resultado: além de evitar sanções, a empresa ganhou vantagem competitiva ao mostrar que respeita a ética e os direitos dos usuários.

Capítulo 6 – Requisitos Obrigatórios para Sistemas de IA de Risco Elevado

Introdução ao Capítulo

Sistemas de IA considerados de risco elevado são aqueles que impactam diretamente os direitos, a segurança ou o bem-estar das pessoas. Por isso, o EU AI Act impõe uma série de obrigações legais para seu desenvolvimento e uso. Aqui, explicamos essas exigências de forma simples e mostramos como elas se alinham com os controles da ISO/IEC 42001.

Seção 1 – O que são Sistemas de Risco Elevado?

Um sistema de IA é considerado de alto risco quando:

- É usado em áreas críticas como saúde, transporte, educação, justiça, crédito ou emprego;
- Pode influenciar decisões que afetam diretamente a vida das pessoas;
- Está incluído na lista oficial da UE como setor sensível.

Exemplo: Uma IA que analisa exames médicos, ou que decide quem passa para uma entrevista de emprego.

Seção 2 – Quais são os Requisitos Obrigatórios?

O EU AI Act define 8 requisitos principais para que uma IA de alto risco seja autorizada:

Sistema de gestão da qualidade
 Deve haver um processo claro, bem documentado e auditável.

ISO 42001: A.4 – Gestão da qualidade da IA

Documentação técnica detalhada
 Explicando como o sistema foi projetado, treinado e testado.

ISO 42001: A.7 – Dados para sistemas de IA

Registros automáticos (logs)
 A IA deve manter rastros das decisões, entradas e saídas relevantes.

ISO 42001: A.6.3 – Registros do ciclo de vida

Transparéncia e explicabilidade
 O usuário deve ser informado de forma clara sobre o funcionamento da IA.

ISO 42001: A.8 – Informação para partes interessadas



UE AI ACT

Supervisão humana
 A IA não pode decidir sozinha em situações críticas.
 Sempre deve haver supervisão.

ISO 42001: B.6 – Supervisão e uso responsável
Robustez e segurança

A IA deve resistir a falhas, ataques e manipulações.

ISO 42001: A.9.1 – Segurança da IA

Precisão e desempenho
 A performance deve ser monitorada regularmente, com padrões definidos.

ISO 42001: 9.1 – Avaliação de desempenho

Gestão de dados e governança
 Os dados usados no treinamento e operação devem ser de qualidade e protegidos.

ISO 42001: A.7 – Governança de dados

Seção 3 – Estudo de Caso (Fictício)

Os requisitos para sistemas de IA de risco elevado garantem que a tecnologia seja usada com responsabilidade e supervisão. A ISO/IEC 42001 funciona como um manual prático para implementar todos esses cuidados. Cumprir essas obrigações não é apenas uma exigência legal – é também uma demonstração de compromisso com os valores humanos.

Empresa: EduSmart – IA para Avaliação Escolar Automatizada

A EduSmart desenvolveu um sistema de IA que analisa redações e atribui notas automaticamente. Como isso impacta diretamente a vida acadêmica dos estudantes, o sistema foi classificado como de risco elevado.

Para atender à legislação, a empresa:

- Implementou um sistema de gestão da IA com base na ISO/IEC 42001;
- Criou relatórios explicativos para cada nota atribuída;
- Adotou critérios objetivos e auditáveis para garantir não discriminação;
- Designou um professor responsável para revisar os resultados em casos duvidosos;
- Estabeleceu um canal para alunos contestarem avaliações automatizadas.

Resultado: o sistema foi aprovado pelas autoridades e tornou-se referência para escolas que desejam usar IA de forma ética e segura.

Capítulo 7 – O Que Está Proibido pela Lei Europeia de IA?

Introdução ao Capítulo

Nem toda aplicação de inteligência artificial é permitida na União Europeia. O AI Act proíbe usos que ameaçam diretamente os direitos fundamentais, a dignidade humana ou criam riscos inaceitáveis para a sociedade. Neste capítulo, vamos entender o que é proibido, por que é proibido e como garantir conformidade, conectando com os controles da ISO 42001.

Seção 1 – Quais sistemas de IA são proibidos?

O Regulamento Europeu proíbe categoricamente os seguintes usos de IA:

Manipulação subliminar

Sistemas que influenciam o comportamento de uma pessoa de forma inconsciente e perigosa.
 Exemplo: Uma IA que altera a cor de uma propaganda digital para induzir compras compulsivas sem o conhecimento do usuário.

Exploração de vulnerabilidades

Sistemas que exploram fragilidades de grupos específicos (crianças, idosos, pessoas com deficiência).

Exemplo: Um brinquedo com IA que induz crianças a fornecer dados pessoais em conversas.

Pontuação social pública

Avaliações de comportamento das pessoas por governos para restringir acesso a serviços.

Exemplo: Um governo que impede um cidadão de viajar por ter baixo “índice de obediência” calculado por IA.

Reconhecimento biométrico em tempo real em locais públicos para fins policiais

Exceto em situações muito específicas, como busca por criminosos perigosos.

Exemplo: Câmeras que identificam todos os rostos em uma praça 24h por dia e cruzam com bancos de dados da polícia.

Reconhecimento emocional por IA para manipulação ou controle

Aplicações que tentam detectar emoções e tomar decisões sem consentimento ou clareza.

Exemplo: Câmeras que identificam todos os rostos em uma praça 24h por dia e cruzam com bancos de dados da polícia.

Seção 2 – Conexão com a ISO/IEC 42001

A ISO 42001 não lista proibições, mas traz controles e diretrizes para evitar abusos e riscos éticos, como:

- A.5 – Avaliação de impacto dos sistemas de IA;
- Avaliar consequências sociais e psicológicas antes de lançar o sistema;
- A.6.2 – Uso responsável da IA;
- Garantir que a IA seja usada de acordo com sua finalidade e sem ferir direitos humanos.
- A.3.3 – Relato de preocupações;
- Criar canais para que abusos sejam reportados com segurança.
- A.8 – Comunicação transparente com partes interessadas;
- Informar usuários sobre o funcionamento da IA e permitir contestação.

Seção 3 – Como se proteger de riscos legais

Empresas e governos devem tomar medidas para não desenvolver nem utilizar sistemas proibidos:

Verificar a lista de usos proibidos antes de criar uma solução de IA;
 Documentar claramente o propósito e limites da aplicação;
 Realizar avaliações de impacto ético e social (como descrito na ISO);
 Garantir a transparência, supervisão humana e o direito de contestação;
 Estabelecer canais de denúncia anônima para uso indevido de IA.



UE AI ACT

Estudo de Caso (Fictício)

Empresa: HealthAware – Assistente Digital para Clínicas

A HealthAware desenvolveu uma IA para detectar o humor de pacientes com base em expressões faciais. A intenção era ajudar psicólogos a identificar sinais de depressão. Porém, o sistema começou a ser testado em clínicas sem o conhecimento dos pacientes.

Resultado:

- O projeto foi suspenso após denúncia por falta de consentimento e violação da privacidade emocional.
- A empresa foi multada por utilizar IA de reconhecimento emocional sem avisar os usuários.
- Após implementar os controles da ISO 42001, como canais de reporte, documentação técnica e revisões de impacto, o projeto foi reformulado com foco em ética, transparência e supervisão humana.

Capítulo 8 – Como a União Europeia Classifica os Riscos da IA?

Introdução ao Capítulo

Nem toda IA é igual diante da lei. O AI Act classifica os sistemas de inteligência artificial conforme o nível de risco que apresentam para as pessoas e a sociedade. Quanto maior o risco, mais rigorosas são as exigências legais. Neste capítulo, você vai entender essa classificação e como ela impacta diretamente os projetos de IA nas organizações – sempre em sintonia com os controles da ISO 42001.

Compreender o nível de risco da sua IA é o primeiro passo para garantir conformidade legal, ética e estratégica. A integração entre AI Act e ISO 42001 proporciona às organizações uma base sólida para usar a IA de forma segura, humana e alinhada com as melhores práticas globais.

Seção 1 – Os 4 níveis de risco da IA

O regulamento europeu divide os sistemas de IA em quatro categorias de risco:

1. Risco inaceitável (Proibido)

São sistemas banidos pela lei, como vimos no capítulo anterior. Exemplos:

- Pontuação social pública;
- Manipulação psicológica inconsciente;
- Reconhecimento biométrico em tempo real sem autorização legal.

Esses sistemas são totalmente proibidos de serem comercializados ou utilizados na UE.

2. Risco elevado

São os sistemas que afetam significativamente direitos fundamentais, saúde, segurança ou justiça. Exigem conformidade rigorosa. Exemplos:

- IA para decisões em recrutamento;
- Scanners para segurança pública;
- Diagnósticos médicos automatizados.

Requisitos obrigatórios incluem: avaliação de impacto, registro de logs, supervisão humana, explicabilidade e documentação técnica.

3. Risco limitado

Sistemas que envolvem interação com o usuário, mas com impacto controlado. Exigem transparência.

Exemplos:

- Chatbots;
- IA que gera imagens com conteúdo publicitário;
- Assistentes virtuais de atendimento.

É necessário informar ao usuário que está interagindo com uma IA.

4. Risco mínimo ou nulo

Sistemas com uso neutro ou genérico, com impacto desprezível sobre os direitos das pessoas. Exemplos:

- Filtros de spam;
- Recomendações de música;
- Corretores ortográficos com IA.

São livres para uso e inovação, sem exigência específica no regulamento.

Seção 2 – Conexão com a ISO/IEC 42001

A ISO 42001 oferece controles alinhados para lidar com todos os níveis de risco. Veja a relação com os principais pontos:

Classificação AI Act: Risco Inaceitável

Controles da ISO 42001 relacionados: A.5 – Avaliação de Impacto; B.3 – Governança Interna

Classificação AI Act: Risco Elevado

Controles da ISO 42001 relacionados: A.6 – Ciclo de Vida; A.7 – Dados e Verificação; A.9 – Uso Responsável

Classificação AI Act: Risco Limitado

Controles da ISO 42001 relacionados: A.8 – Comunicação Transparente; A.10 – Relacionamento com Terceiros.

Classificação AI Act: Risco Mínimo

Controles da ISO 42001 relacionados: A.4 – Recursos; A.2 – Políticas de IA

Seção 3 – Como saber o nível de risco do meu sistema?

Verifique a finalidade da IA (ex: decidir crédito, identificar rostos, prever comportamento);

Analice quem será impactado e como (ex: grupos vulneráveis, decisões críticas);

Consulte os anexos do AI Act, que listam categorias de risco;

Faça uma Avaliação do Impacto do Sistema de IA (recomendada também na ISO 42001 – A.5.2);

Documente os resultados e atualize periodicamente.

Estudo de Caso – FinTech AvaliaRápido

A AvaliaRápido desenvolveu uma IA para avaliar currículos automaticamente e indicar os candidatos mais promissores. Ao lançar o produto no mercado europeu, percebeu que se tratava de um sistema de IA de alto risco, por afetar diretamente os direitos fundamentais relacionados ao trabalho e à não discriminação.

Ações tomadas:

- Realizou uma avaliação de impacto ética e legal;
- Garantiu supervisão humana nas decisões finais;
- Implementou mecanismos de contestação e explicabilidade;
- Documentou todo o processo técnico e jurídico.

Resultado: o sistema foi certificado como conforme com o AI Act e as diretrizes da ISO 42001.



UE AI ACT

Sistemas de IA de alto risco devem ser tratados com seriedade e responsabilidade. O AI Act oferece um marco jurídico robusto, a ISO/IEC 42001 permite transformar exigências legais em processos práticos e auditáveis. Para as empresas, isso representa não apenas compliance, mas vantagem competitiva baseada em confiança.

Capítulo 9 – Sistemas de IA de Alto Risco: O que sua organização precisa atender

Introdução ao Capítulo

Se a sua empresa desenvolve, fornece ou utiliza uma IA que impacta decisões importantes sobre pessoas, como emprego, educação, crédito, saúde, policiamento ou justiça, ela provavelmente entra na categoria de alto risco. Isso significa que a IA está sujeita a regras específicas e obrigatórias – e o não cumprimento pode gerar penalidades severas. Neste capítulo, explicamos o que é exigido e como aplicar na prática.

Seção 1 – O que caracteriza um sistema de IA de alto risco?

Segundo o Anexo III do AI Act, um sistema é considerado de alto risco quando afeta:

- Educação e acesso à formação profissional (ex: IA que corrige provas ou dá notas);
- Emprego e gestão de trabalhadores (ex: IA que filtra currículos);
- Acesso a serviços essenciais (ex: crédito bancário, saúde);
- Serviços públicos e aplicação da lei (ex: IA usada por polícias);
- Justiça e decisões legais automatizadas;
- Controle de fronteiras, migração e asilo.

Se sua IA se enquadra nessas situações, atenção redobrada: há obrigações legais obrigatórias.

Seção 2 – Requisitos obrigatórios para sistemas de alto risco

Abaixo, listamos os principais requisitos do AI Act e sua conexão com os controles da ISO/IEC 42001:

Requisitos do AI Act e sua conexão com os controles da ISO/IEC 42001		
Requisito do AI Act	Resumo	Conexão ISO 42001
Governança de Riscos	Avaliação e mitigação contínua de riscos	A.5 – Avaliação de Impacto
Qualidade dos dados	Dados de treinamento devem ser corretos, diversos e representativos	A.7 – Gestão de Dados
Documentação técnica	Criar e manter registros técnicos detalhados do sistema	A.6 – Ciclo de Vida da IA
Registro de logs	O sistema deve guardar registros de funcionamento	A.6.7 – Logs e Auditoria
Transparência	O usuário precisa entender que está lidando com uma IA e como ela funciona	A.8 – Informação para as Partes Interessadas
Supervisão Humana	Um humano deve ter poder de rever, contestar ou interromper a IA	A.3.2 – Papéis e Responsabilidades
Robustez e segurança	IA deve resistir a falhas, erros e manipulações	A.4 – Recursos e Continuidade

Seção 3 – Como se preparar para esses requisitos

1. Mapeie todos os sistemas de IA utilizados na organização;
2. Classifique o nível de risco com base no uso e impacto;
3. Realize uma Avaliação de Impacto Algorítmico (AIA) conforme ISO 42001;
4. Crie registros técnicos e rotinas de atualização de dados;
5. Defina responsáveis e políticas de supervisão humana;
6. Implemente testes contínuos de segurança e performance.

Estudo de Caso – HealthCheck AI (Startup de Diagnóstico Médico)

A HealthCheck AI criou um sistema de IA para auxiliar médicos na triagem de pacientes em pronto-socorro com base em sintomas descritos.

Classificação de risco: alto risco (impacto direto em saúde e bem-estar).

Ações tomadas para conformidade:

- Criaram uma política de IA transparente (ISO B.2);
- Garantiram que dados de treinamento incluíssem diversos perfis raciais e faixas etárias (ISO B.7);
- Definiram um plano de supervisão humana: o médico sempre tem a palavra final (ISO B.9);
- Implementaram auditoria de logs e documentação técnica automatizada;
- Fizeram testes mensais de robustez e segurança algorítmica.

Resultado: o sistema foi autorizado a operar na UE, com certificação técnica e respaldo ético.



Capítulo 10 – Modelos de IA de Uso Geral: Como a Europa pretende regular os grandes modelos

Os GPAIs representam o futuro da inteligência artificial – flexível, potente e de múltiplos usos. Mas com grande poder, vem grande responsabilidade. A UE busca criar um ambiente onde a inovação ande junto com a segurança e a ética, especialmente quando os modelos atingem larga escala.

Introdução ao Capítulo

Com a ascensão dos modelos de linguagem e IA generativa, surgiram novos riscos, especialmente ligados à desinformação, viés algorítmico e uso indevido em larga escala. O AI Act da União Europeia criou uma nova categoria chamada Modelos de Uso Geral de IA (General Purpose AI Models – GPAI), com regras específicas para garantir segurança, transparéncia e controle.

Neste capítulo, você vai entender:

- O que é um modelo de uso geral
- Quais modelos se enquadram na categoria “sistêmicos”
- O que a lei exige desses fornecedores
- Como conectar com os controles da ISO 42001

Seção 1 – O que são modelos de IA de uso geral?

São modelos treinados para realizar várias tarefas diferentes, como:

- Responder perguntas (ex: ChatGPT)
- Criar textos, imagens, códigos ou músicas
- Traduzir conteúdos
- Resumir documentos
- Raciocinar ou classificar informações

Esses modelos não são criados para uma tarefa específica, mas sim como plataformas amplas, utilizadas por desenvolvedores, empresas e usuários finais.

Exemplo: Um único modelo pode ser usado para redigir contratos, criar campanhas de marketing ou dar suporte em diagnósticos médicos.

Seção 2 – Quando um modelo é considerado “sistêmico”?

Segundo o AI Act, um GPAI se torna sistêmico quando atinge:

- Altíssima escala de uso;
- Riscos potenciais à saúde, segurança, democracia ou meio ambiente;
- Capacidade de influenciar amplamente o comportamento humano ou automatizar decisões críticas.

Modelos como GPT-4, Claude ou Gemini Ultra podem ser considerados sistêmicos.

Seção 3 - Requisitos do AI Act para Modelos de Uso Geral		
Obrigação	Descrição Simples	Conexão ISO 42001
Documentação técnica	Detalhar como o modelo foi treinado, que dados foram usados e seus limites	A.6.4 – Documentação técnica
Resumo dos dados de treinamento	Explicar as fontes principais, especialmente se houver uso de dados protegidos por direitos autorais	A.7.5 – Proveniência e qualidade de dados
Avaliação de desempenho e risco	Testar o modelo em situações práticas e avaliar possíveis impactos adversos	A.5 – Avaliação de Impacto
Comunicação responsável	Informar claramente que o conteúdo foi gerado por IA	A.8 – Informação às Partes Interessadas
Registro público	Modelos sistêmicos devem ser registrados em base europeia pública	A.3.3 – Transparéncia e relato público
Mitigação de riscos sistêmicos	Criar planos de segurança, contingência e governança específica	A.3 – Organização Interna



Capítulo 11 – Governança, Transparência e o Papel dos Estados na Regulação da IA

Governança eficaz é a base da confiança em sistemas complexos. Com o AI Act, a União Europeia constrói uma arquitetura regulatória que fortalece a segurança, protege os direitos e incentiva a inovação responsável. Não basta criar sistemas inteligentes – é preciso garantir que sejam transparentes, auditáveis e supervisionáveis.

Introdução ao Capítulo

O AI Act da União Europeia não é apenas uma lista de obrigações para empresas – ele cria uma estrutura completa de governança pública, com regras claras sobre quem regula, quem fiscaliza e como garantir a transparéncia nos sistemas de IA.

Neste capítulo, vamos explorar:

- Como os países da UE devem implementar o AI Act
- Quem fiscaliza o cumprimento das normas
- Como as empresas devem garantir transparéncia
- Conexões diretas com os controles da ISO/IEC 42001

Seção 1 – Quem são os responsáveis pela aplicação da lei?

Cada Estado-Membro da UE precisa:

- Designar uma autoridade nacional competente para supervisionar o cumprimento do AI Act.
- Nomear um organismo notificante (para certificações e avaliações de conformidade).
- Criar canais de relato de irregularidades e incidentes de IA.

Esses órgãos terão o poder de:

- Aplicar multas, suspensões ou restrições;
- Exigir documentação técnica e auditorias;
- Suspender sistemas de IA de alto risco ou GPAIs não conformes.

Conexão ISO 42001: A.3.3 – Relato de preocupações / A.2 – Políticas de IA / A.5 – Gestão de riscos

Seção 2 – Transparéncia para todos

O regulamento exige que os desenvolvedores e operadores de sistemas de IA fornecam informações claras sobre:

- Quando e como a IA está sendo usada;
- Quais dados foram utilizados no treinamento (de forma resumida);
- Qual é o objetivo pretendido do sistema;
- Quais são os limites e riscos conhecidos.

Para sistemas de IA que interagem com humanos, deve ser informado quando o usuário está lidando com uma IA.

Conexão ISO 42001:

- A.8 – Informação para partes interessadas
- A.5 – Avaliação de impacto
- A.6.3 – Comunicação com usuários

Seção 3 – O novo Conselho Europeu de Inteligência Artificial

O AI Act cria um órgão de governança europeu, o European AI Board, com funções como:

- Coordenar a aplicação das regras entre os países;
- Emitir recomendações técnicas e éticas;
- Manter registros de modelos sistêmicos GPAI;
- Ayudar a padronizar avaliações de risco e impacto.

Esse conselho também pode:

- Publicar listas de boas práticas;
- Apoiar startups e pequenas empresas com orientações;
- Criar critérios comuns para auditorias de IA.

Conexão ISO 42001:

- B.3 – Governança interna
- B.4.5 – Recursos institucionais para conformidade

Seção 4 – Estudo de Caso: A Autoridade Digital da Estônia

A Estônia foi um dos primeiros países a implementar o AI Act. Criou uma Agência Nacional de Supervisão de IA, com funções específicas:

- Um portal para registro de modelos de alto risco;
- Canal anônimo para denúncias de IA indevida em empresas públicas;
- Equipe multidisciplinar com especialistas em IA, direito e proteção de dados;
- Realização de auditorias aleatórias em sistemas de IA que usam dados sensíveis (ex: saúde, educação).

Impacto: aumento de 42% na conformidade dos modelos de IA do governo com normas de explicabilidade e direitos fundamentais.



Capítulo 12 – Conformidade, Penalidades e Caminhos para Adaptação

A conformidade com o AI Act não é apenas uma obrigação legal – é uma oportunidade para construir credibilidade, confiança e vantagem competitiva no uso da IA. Com ferramentas como a ISO/IEC 42001, é possível transformar o desafio regulatório em uma jornada estratégica de melhoria contínua.

Introdução ao Capítulo

Com a entrada em vigor do AI Act, empresas e governos passam a ter responsabilidades claras sobre o uso ético, seguro e transparente da IA. Mas o que acontece se essas obrigações não forem cumpridas? Neste capítulo, você vai entender:

- Quais são as multas e penalidades previstas pelo regulamento;
- Como as organizações podem provar conformidade;
- Qual o papel da ISO/IEC 42001 nesse processo;
- Estratégias práticas para se adaptar rapidamente às novas regras.

Seção 1 – O que é considerado descumprimento?

As infrações podem ocorrer em diversas situações, como:

- Usar sistemas proibidos (ex: IA que manipula o comportamento humano de forma abusiva);
- Não cumprir com obrigações de transparência e explicação;
- Falhar na avaliação de riscos de sistemas de alto risco;
- Negligenciar o consentimento informado do usuário;
- Não manter registros, logs ou documentação técnica exigidos.

Conexão com ISO 42001:

- A.9 – Uso responsável
- A.5.2 – Avaliação de impacto
- A.6.4 – Registro de logs de eventos

Seção 2 – Quais são as multas e penalidades?

As penalidades variam conforme a gravidade da infração:

Infração	Multa Máxima
Uso de sistemas proibidos	35 milhões de euros ou 7% do faturamento global anual
Não conformidade com obrigações de GPs ou sistemas de alto risco	15 milhões de euros ou 3% do faturamento
Informação falsa à autoridade	7,5 milhões de euros ou 1% do faturamento

 Para pequenas empresas ou startups, os valores podem ser ajustados proporcionalmente.

Seção 3 – Como demonstrar conformidade?

As organizações devem estar preparadas para comprovar:

- Que realizam auditorias internas regulares (ISO 42001 – seção 9.2);
- Que mantêm documentação técnica atualizada (ISO 42001 – seção 7.5);
- Que treinam colaboradores em IA responsável e ética (ISO 42001 – seção 7.2);
- Que seguem políticas claras de uso e avaliação de IA (ISO 42001 – seção A.2).

Uma certificação baseada na ISO/IEC 42001 pode ser um diferencial estratégico.

Seção 4 – Estratégias práticas de adaptação

As organizações podem seguir este roteiro:

1. Mapear todos os sistemas de IA em uso;
2. Classificar o nível de risco de cada sistema segundo o AI Act;
3. Criar um plano de avaliação de impacto (PIA);
4. Atualizar suas políticas internas de tecnologia e dados;
5. Implantar um sistema de governança baseado na ISO 42001;
6. Designar um comitê de ética e risco de IA.

Checklist de alinhamento com ISO 42001:

- A.2.4 – Análise crítica da política
- A.5 – Gestão de riscos
- A.9 – Tratamento de incidentes
- B.3.2 – Papéis e responsabilidades

Estudo de Caso – Adaptação de uma Instituição Financeira Europeia

O Banco EuroData, sediado na Alemanha, usa IA para análises de crédito. Com o AI Act, classificou seu sistema como de alto risco. Para se adaptar:

- Contratou uma equipe de compliance em IA;
- Aplicou a ISO 42001 para estruturar seu sistema de gestão de IA;
- Realizou uma avaliação de impacto ético e técnico;
- Criou um portal de explicabilidade de decisões automatizadas para clientes;
- Submeteu o sistema a uma auditoria externa de conformidade.

Resultado: redução de 36% em reclamações sobre decisões automatizadas e aprovação pela autoridade reguladora alemã.



Capítulo 13 – Inovação Responsável e o Papel das Pequenas e Médias Empresas (PMEs)

As PMEs são o motor da inovação europeia. Com apoio regulatório, ferramentas práticas como a ISO 42001 e atitudes responsáveis, elas podem liderar uma IA ética, confiável e competitiva no cenário global.

Introdução ao Capítulo

A inteligência artificial não é exclusividade das grandes empresas. Cada vez mais, startups e PMEs desenvolvem ou utilizam sistemas baseados em IA para atender nichos de mercado, aumentar a produtividade e oferecer soluções inovadoras.

Neste capítulo, vamos entender:

- O impacto do AI Act para as PMEs;
- Como inovar com segurança e responsabilidade;
- Como o regulamento europeu e a ISO/IEC 42001 apoiam o crescimento sustentável da IA nas pequenas empresas;
- E como superar os desafios de recursos e conformidade com agilidade.

Seção 1 – Oportunidades e Desafios das PMEs com IA

As PMEs europeias representam mais de 90% das empresas da União. Muitas estão criando soluções com IA em áreas como:

- Saúde personalizada,
- Agricultura de precisão,
- Logística urbana,
- Marketing digital automatizado.

Desafios enfrentados pelas PMEs:

- Falta de pessoal especializado em IA;
- Recursos limitados para auditorias e conformidade;
- Insegurança jurídica quanto ao uso ético e legal da tecnologia.

Conexão com ISO 42001:

- A.4.1 – Planejamento de recursos adequados
- A.2.2 – Política de IA documentada
- A.5.2 – Avaliação de impactos sociais e legais

Seção 2 – Como o AI Act apoia as PMEs

O regulamento europeu inclui medidas de apoio específicas às PMEs, como:

- Redução de taxas administrativas para certificação;
- Sandboxes regulatórios para testes controlados;
- Acesso facilitado a laboratórios de inovação e centros de competência em IA;
- Ferramentas de avaliação prévias simplificadas.

Isso estimula um ambiente de inovação segura, sem frear o crescimento tecnológico.

Seção 3 – Como implantar Governança de IA com baixo custo

Mesmo com poucos recursos, as PMEs podem adotar governança eficaz com ações práticas:

Ação	Descrição
Nomear um “guardião da IA”	Alguém responsável por supervisionar o uso ético da tecnologia, mesmo que acumule outras funções.
Criar uma política simples de IA	Um documento curto explicando: objetivos, riscos, limites de uso e boas práticas.
Usar modelos prontos da ISO 42001	A norma oferece controles modulares, aplicáveis à realidade das PMEs.
Fazer autoavaliações trimestrais	Com checklists simples, é possível medir conformidade e evoluir continuamente.
Relevância ISO:	
<ul style="list-style-type: none"> • A.3.2 – Definir papéis e responsabilidades • A.9.2 – Garantir uso conforme propósito 	

Seção 4 – Estudo de Caso: Startup de Agrotech em Portugal

A AgroNova, uma startup com 12 funcionários no interior de Portugal, criou um sistema de IA para monitorar o solo e prever pragas. Com o AI Act, ela se enquadrou como fornecedora de sistema de risco alto.

Ações tomadas:

- Adaptou o ciclo de vida do sistema com base na ISO/IEC 42001;
- Criou um plano de tratamento de riscos éticos e técnicos;
- Treinou os três desenvolvedores com um curso básico de IA responsável;
- Publicou um termo de transparência aos agricultores, explicando o sistema.

Resultado: passou na avaliação de conformidade e atraiu novos investidores europeus por estar alinhada com a legislação.



Capítulo 14 – Direitos dos Usuários e Transparência no Uso de IA

Em um mundo orientado por dados e algoritmos, respeitar os direitos das pessoas e garantir transparéncia é mais do que uma exigência legal – é uma condição para construir confiança e valor a longo prazo. A ISO 42001 e o AI Act oferecem caminhos concretos para transformar boas intenções em práticas reais.

Introdução ao Capítulo

À medida que os sistemas de inteligência artificial passam a fazer parte do dia a dia, os direitos das pessoas impactadas por essas tecnologias ganham centralidade. O AI Act da União Europeia estabelece regras claras sobre transparéncia, explicabilidade e proteção dos usuários. Neste capítulo, vamos explorar:

- Quais são os principais direitos dos usuários de IA;
- O que significa “transparéncia algorítmica” na prática;
- Como a ISO/IEC 42001 auxilia organizações a respeitarem esses direitos;
- Um estudo de caso real sobre comunicação de incidentes com IA.

Seção 1 – Direitos Fundamentais no Contexto da IA

Segundo o regulamento europeu, as pessoas têm o direito de:

- Saber quando estão interagindo com sistemas de IA;
- Entender como decisões automatizadas são tomadas;
- Contestar decisões que afetem significativamente seus direitos;
- Proteger seus dados pessoais e sensíveis usados por sistemas inteligentes;
- Reportar impactos adversos ou falhas no funcionamento dos sistemas de IA.

Conexão com ISO 42001:

- A.8.1 – Comunicação com partes interessadas
- A.5.2 – Avaliação de impactos sociais
- A.2.4 – Análise crítica da política de IA

Seção 2 – O que é Transparéncia em IA?

Transparéncia significa permitir que qualquer pessoa entenda:

- O propósito de um sistema de IA;
- Quais dados ele utiliza;
- Como ele chega às conclusões (explicabilidade);
- Quem é o responsável técnico e ético;
- Como o sistema é monitorado e ajustado.

A ISO 42001 orienta a criação de documentação técnica clara, painéis explicativos e processos de suporte ao usuário.

💡 Exemplo prático: Um banco europeu usa IA para aprovar crédito. O cliente pode acessar um relatório simples que explica os fatores que influenciaram a decisão, além de ter um canal direto para contestação e reavaliação humana.

Seção 3 – Como informar e proteger os usuários

Ação recomendada	Benefício para o usuário
Etiquetar sistemas de IA com aviso visível	Usuário sabe que está interagindo com uma IA
Oferecer canal de contato direto	Permite tirar dúvidas e relatar problemas
Criar manuais em linguagem acessível	Melhora a compreensão e o uso adequado
Manter logs de uso e incidentes	Garante rastreabilidade e responsabilização
Relevância ISO:	
• A.8.2 - Comunicação de incidentes	
• A.9.3 - Garantir uso conforme propósito	
• A.3.5 - Processo de relato de preocupações	

Seção 4 – Estudo de Caso: Plataforma de Reclamações com IA

A JustTech, uma startup de mediação de conflitos, utilizava um chatbot com IA para orientar consumidores sobre seus direitos. Após uma atualização, a IA começou a fornecer informações incompletas, levando usuários a ações erradas.

A empresa:

- Acionou o plano de comunicação de incidentes conforme a ISO 42001;
- Em 48h, notificou os usuários afetados;
- Publicou uma nota explicativa e reforçou o canal de suporte humano;
- Realizou uma nova avaliação de impacto social e corrigiu a lógica da IA.

Resultado: preservou a reputação, evitou penalidades legais e reforçou a confiança dos usuários.



UE AI ACT

Capítulo 15 – Classificação de Riscos e Avaliação de Conformidade em Sistemas de IA

Introdução ao Capítulo

A União Europeia, com o AI Act, adota uma abordagem baseada no risco para regular o uso da inteligência artificial. O objetivo é garantir que quanto maior o risco para as pessoas ou para a sociedade, mais rígidas devem ser as regras. Este capítulo aborda:

- Como os sistemas de IA são classificados por risco;
- O que é a avaliação de conformidade;
- A conexão com a ISO/IEC 42001;
- Um estudo de caso prático sobre conformidade.

Nota ao Leitor: Alguns conceitos — como avaliação de risco, responsabilização e uso ético — aparecerão em mais de um capítulo. Isso ocorre porque o Regulamento Europeu de IA (AI Act) e a norma ISO 42001 tratam desses temas em diferentes fases do ciclo de vida da IA: da criação à operação, incluindo fornecedores e usuários finais. Sempre que um princípio se repetir, ele será explicado no novo contexto, com linguagem simples e exemplos práticos.

Entender o risco de um sistema de IA e aplicar corretamente as exigências de conformidade é essencial para evitar penalidades, garantir a confiança do público e fomentar inovação responsável. A combinação do AI Act com a ISO/IEC 42001 oferece uma trilha clara e estruturada para organizações que querem desenvolver IA de forma segura, ética e sustentável.

Seção 3 – Elementos obrigatórios para sistemas de IA de alto risco

Se sua organização desenvolve ou utiliza IA classificada como “alto risco”, deverá implementar controles como:

- Avaliação de impacto algorítmico (AIA);
- Processo de gestão de riscos contínuo;
- Garantia de supervisão humana significativa;
- Registro de logs e rastreabilidade;
- Governança clara e canais para denúncia de falhas;
- Plano de resposta a incidentes.

Seção 4 – Estudo de Caso: IA para Triagem de Currículos

A empresa TalentMatch, especializada em recrutamento, desenvolveu um sistema de IA para triagem automática de currículos.

Classificação: Alto risco (impacta acesso ao emprego).
 Exigência: Avaliação de conformidade antes da entrada no mercado.

A TalentMatch adotou as seguintes práticas:

- Realizou uma avaliação de impacto do sistema com apoio jurídico;
- Criou uma política clara de supervisão humana;
- Documentou o projeto, fontes de dados e critérios de decisão;
- Submeteu o sistema a auditoria externa;
- Consegiu certificação de conformidade, conforme exigido pelo AI Act.

Resultado: confiança dos clientes aumentou, o produto foi aceito em diversos países da UE, e riscos éticos foram mitigados desde o início.

Seção 1 – Classificação de Riscos no AI Act

O regulamento europeu classifica os sistemas de IA em quatro categorias:

Categoría de Risco	Exemplo	Exigencia Legal
Proibido	IA que manipula comportamento infantil ou faz “score social” por governos	Proibido na UE
Alto risco	Reconhecimento facial, decisões de crédito, IA em saúde, educação ou justiça	Avaliação obrigatória
Risco limitado	Chatbots, sistemas de recomendação	Transparéncia obrigatória
Risco mínimo ou nulo	Jogos com IA, filtros de e-mail	Uso livre, sem exigências específicas
Conexão com ISO 42001: A.5.2 – Avaliação de impacto do sistema de IA A.9.1 – Processo de projeto com análise de riscos A.9.3 – Avaliação contínua de riscos		

Seção 2 – O que é Avaliação de Conformidade?

A avaliação de conformidade é um processo para verificar se o sistema de IA atende às normas e obrigações legais, especialmente para sistemas de alto risco.

Esse processo envolve:

- Avaliação técnica do sistema e sua documentação;
- Verificação de segurança, ética, privacidade e desempenho;
- Auditoria interna ou externa, dependendo do caso;
- Emissão de declaração de conformidade ou certificação.

Conexão com ISO:

- Seções 7.5, 9.2 e 10.1 da ISO/IEC 42001 orientam como documentar, auditar e melhorar continuamente os sistemas de IA.



Capítulo 16 – Obrigações dos Fornecedores, Importadores e Distribuidores.

Introdução ao Capítulo

O ecossistema de inteligência artificial vai muito além do desenvolvedor do sistema. O AI Act define obrigações específicas para fornecedores, importadores, distribuidores e terceiros autorizados, reconhecendo que todos esses agentes têm papel crítico na responsabilidade e conformidade dos sistemas de IA.

Neste capítulo, você vai entender:

- Quem são os atores envolvidos na cadeia de fornecimento da IA;
- Quais são as suas obrigações segundo o AI Act;
- Como essas funções se conectam com os controles da ISO/IEC 42001;
- Exemplos práticos de responsabilidades compartilhadas.

Seção 1 – Quem são os atores e o que fazem?

No contexto do AI Act, os seguintes agentes possuem responsabilidades legais específicas:

Atores	Descrição
Fornecedores	Desenvolvem, treinam e colocam no mercado o sistema de IA.
Importadores	Introduzem no mercado da UE sistemas de IA fabricados em países terceiros.
Distribuidores	Comercializam ou tornam o sistema disponível em nome de terceiros.
Representantes autorizados	Designados por fornecedores não europeus para cumprir com o AI Act na UE.

Esses papéis não são apenas formais: cada um tem obrigações legais distintas para garantir a segurança, conformidade e transparência do sistema de IA ao longo de sua vida útil.

Seção 2 – Obrigações dos fornecedores

Os fornecedores, responsáveis pelo desenvolvimento ou integração de IA, devem:

- Garantir que o sistema atenda aos requisitos do AI Act, especialmente se for classificado como alto risco;
- Elaborar e manter a documentação técnica, incluindo logs e descrição do sistema;
- Executar avaliações de conformidade, incluindo testes de segurança e explicabilidade;
- Registrar o sistema no banco de dados europeu de IA de alto risco;
- Adotar práticas de governança e supervisão humana contínua;
- Cooperar com autoridades reguladoras e fornecer acesso à documentação sob solicitação.

Conexão com a ISO/IEC 42001	
Controle ISO 42001	Alinhamento
A.6 – Ciclo de vida do sistema de IA	Abrange desde o design até o descomissionamento
A.6.3 – Verificação e validação	Garante que o sistema cumpre os requisitos de qualidade e segurança
A.9.1 – Uso responsável	Fornecedores devem garantir uso previsto e supervisão apropriada

Seção 3 – Obrigações dos importadores e distribuidores

Importadores devem:

- Verificar se o fornecedor cumpre com as obrigações legais;
- Garantir que a documentação técnica esteja disponível;
- Registrar-se no sistema europeu como responsável pela entrada do sistema de IA no mercado da UE;
- Interromper a colocação no mercado se houver não conformidade identificada.

Distribuidores devem:

- Manter a integridade da documentação, manuais e etiquetas do sistema de IA;
- Agir imediatamente caso identifiquem sistemas não conformes;
- Informar às autoridades em caso de riscos sérios ou violações.

Conexão com a ISO/IEC 42001	
Controle	Relevância
A.10 – Relacionamento com terceiros	Define obrigações para fornecedores, clientes e parceiros
A.10.2 – Cadeia de responsabilidade	Atribuição de papéis entre todas as partes envolvidas

Seção 4 – Compartilhamento de responsabilidades e rastreabilidade

O AI Act incentiva uma abordagem colaborativa de compliance. Isso significa:

- Fornecedores podem delegar certas funções, mas continuam sendo responsáveis;
- Importadores e distribuidores devem manter registros claros de seus parceiros;
- Todos os atores devem contribuir com a rastreabilidade e segurança do sistema.

💡 Um sistema de IA com risco elevado só pode operar na União Europeia se toda a cadeia de fornecimento estiver em conformidade.

Exemplo prático

Imagine uma empresa brasileira que desenvolve um sistema de IA para triagem de curriculhos e decide comercializá-lo na Europa por meio de um distribuidor espanhol.

Neste caso:

- O desenvolvedor brasileiro precisa nomear um representante legal na UE;
- Deve entregar documentação técnica, avaliação de impacto e registrar o sistema;
- O distribuidor espanhol deve verificar se o produto é seguro e está documentado;
- Ambos são responsáveis em caso de falhas que afetem direitos dos candidatos.



Capítulo 17 – Governança e Supervisão: Quem Fiscaliza e Como?

Introdução ao Capítulo

Com a entrada em vigor do AI Act, surge uma nova estrutura institucional para garantir o cumprimento das regras. Governos nacionais e entidades europeias terão um papel central em supervisionar o desenvolvimento e uso responsável da inteligência artificial.

Neste capítulo, você vai entender:

- Quem são as autoridades responsáveis pela fiscalização do AI Act;
- Como funcionam os mecanismos de supervisão e aplicação da lei;
- O que muda na governança interna das empresas;
- Como a ISO/IEC 42001 ajuda a garantir governança contínua.

A supervisão da IA na União Europeia será um trabalho conjunto entre governos, empresas e sociedade civil. O AI Act inaugura uma nova era de governança algorítmica, onde conformidade, responsabilidade e supervisão ativa são inesparáveis.

A ISO/IEC 42001 fornece as ferramentas para estruturar essa governança dentro das organizações – com políticas claras, definição de papéis, mecanismos de controle e canais de denúncia confiáveis.

Empresas que operam sistemas de alto risco devem também estar preparadas para auditorias externas e inspeções in loco.

Conexão com a ISO/IEC 42001

Controle	Aplicação prática
A.2 - Política de IA	Define diretrizes claras de governança e supervisão
A.6.4 - Registro de logs	Exige controle e rastreabilidade de decisões automatizadas
A.3.3 - Relato de preocupações	Estabelece canais seguros para denúncias internas

Seção 3 – Cooperação, transparência e confiança

Para garantir uma IA ética e segura, o AI Act prevê:

- Compartilhamento de dados com autoridades mediante solicitação;
- Mecanismos de transparéncia ativa (por exemplo: avisar que o usuário está interagindo com uma IA);
- Adoção de padrões europeus harmonizados para assegurar interoperabilidade e confiança.

Empresas que demonstram cooperação proativa com as autoridades podem se beneficiar de redução de penalidades em caso de falhas, desde que haja boa-fé e transparéncia.

Conexão com a ISO/IEC 42001

Controle	Relevância
A.3 – Organização interna	Define papéis e responsabilidades para a governança da IA
A.10 – Relacionamento com clientes e terceiros	Enfatiza a transparéncia e cooperação com partes reguladoras

Seção 2 – Como as empresas devem se organizar internamente?

Além da fiscalização externa, o AI Act exige que as empresas:

- Criem sistemas internos de controle e auditoria para IA;
- Mantenham registros e logs detalhados das decisões automatizadas;
- Tenham um responsável designado pela conformidade do sistema de IA (semelhante ao DPO da LGPD);
- Sejam capazes de demonstrar, sob solicitação, a conformidade técnica e ética dos seus sistemas.



Capítulo 18 – Transparência e Explicabilidade na Prática

Introdução ao Capítulo

A confiança em sistemas de inteligência artificial depende diretamente da sua transparência e da capacidade de explicação das decisões automatizadas. Este é um dos pilares centrais do AI Act.

Neste capítulo, você vai entender:

- O que significa tornar um sistema de IA transparente;
- Quais são as exigências do AI Act nesse tema;
- Como garantir que os usuários compreendam o funcionamento da IA;
- Como aplicar os controles da ISO/IEC 42001 para atender a essas exigências.

Seção 1 – O que é transparência em IA?

A transparéncia e a explicabilidade são pontes de confiança entre humanos e máquinas. Não basta que a IA funcione — é necessário que o usuário entenda como e por que ela funciona daquela forma.

O AI Act reforça a obrigação de informar e explicar. Já a ISO/IEC 42001 fornece o suporte técnico e processual para colocar essas diretrizes em prática de forma consistente e auditável.

Transparéncia em IA significa informar, de forma clara e acessível, que o usuário está interagindo com um sistema automatizado, e fornecer informações essenciais sobre:

- A natureza da IA (ex: se é um chatbot, sistema de recomendação, reconhecimento facial);
- As finalidades do sistema;
- A lógica geral que determina o funcionamento;
- Os direitos dos usuários, incluindo o direito à intervenção humana e à contestação.

O AI Act exige etiquetagem clara para sistemas de IA que:

- Interajam diretamente com humanos (ex: assistentes virtuais);
- Detectem emoções ou manipulem comportamentos;
- Produzam conteúdo sintético (deepfakes, por exemplo).

Conexão com a ISO/IEC 42001	
Controle	Aplicação prática
A.8.2 – Informação ao usuário	Exige fornecer aos usuários dados suficientes para o uso responsável da IA
A.9.1 – Uso responsável	Garante que os sistemas sejam utilizados com clareza e ética
A.8 – Comunicação com partes interessadas	Define como informar de forma transparente sobre riscos e funções do sistema

Seção 2 – O que é explicabilidade?

A explicabilidade se refere à capacidade de entender como e por que um sistema de IA chegou a uma determinada conclusão ou recomendação. Isso é vital quando:

- Uma decisão automatizada afeta diretamente um indivíduo;
- Existe risco à saúde, segurança, direitos ou liberdades;
- A IA está sendo usada em contextos sensíveis, como justiça, crédito, ou saúde.

O AI Act não exige que os algoritmos sejam abertos, mas sim que as organizações consigam explicar de forma acessível:

- Os critérios gerais utilizados pelo sistema;
- Os fatores que influenciaram uma decisão;
- Se houver, as limitações conhecidas do modelo.

Seção 3 – Como aplicar isso na prática?

Empresas e órgãos públicos devem criar processos e materiais que promovam a transparéncia e explicabilidade, como:

- Políticas claras sobre o uso de IA;
- Treinamento dos usuários e stakeholders;
- Documentação técnica acessível;
- Dashboards com visualizações explicativas;
- Canais de atendimento para dúvidas e contestações.

Conexão com a ISO/IEC 42001	
Controle	Aplicação prática
A.6.3 – Documentação técnica	Exige manter registros claros sobre o funcionamento do sistema
A.9.2 – Responsabilidade pelo uso	Assegura que as decisões possam ser explicadas e justificadas
A.6.4 – Logs de eventos	Permite rastrear decisões e reforça a auditabilidade



Capítulo 19 – Sistemas de IA de Uso Geral (GPAI)

Introdução ao Capítulo

Os sistemas de IA de uso geral, também conhecidos como GPAI (General Purpose AI), são modelos poderosos capazes de executar uma grande variedade de tarefas, mesmo aquelas para as quais não foram especificamente treinados. Exemplos incluem grandes modelos de linguagem, como o ChatGPT, ou modelos multimodais que combinam texto, imagem e som.

Neste capítulo, você vai entender:

- O que caracteriza um sistema GPAI;
- Quais são os deveres específicos para fornecedores e usuários;
- Como mitigar riscos mesmo quando a IA tem múltiplos usos;
- Quais controles da ISO/IEC 42001 apoiam a governança desses modelos.

Os sistemas de IA de uso geral ampliam o potencial da tecnologia, mas também os seus riscos. Por isso, a regulamentação exige responsabilidades compartilhadas, tanto de quem cria quanto de quem utiliza.

A ISO/IEC 42001 oferece o suporte necessário para estruturar essas responsabilidades dentro de uma gestão contínua, ética e responsável de IA

Conexão com a ISO/IEC 42001	
Controle	Aplicação prática para GPAI
A.6.1 - Ciclo de vida do sistema	Documentar o uso desde o desenvolvimento até a aplicação final
A.5.2 - Avaliação de impacto	Avaliar impactos em usos não previstos
A.7.2 - Qualidade e origem dos dados	Importante para modelos treinados com dados massivos
A.6.3 - Documentação técnica	Facilita a rastreabilidade e explicabilidade do GPAI

Seção 1 – O que é um sistema de IA de uso geral?

Um sistema GPAI é uma IA que pode ser aplicada em diferentes contextos, sem ajustes específicos. Ele é treinado com grandes volumes de dados e aprende padrões que permitem, por exemplo:

- Gerar texto, código, imagens ou vídeos;
- Traduzir idiomas;
- Realizar análises e recomendações;
- Ser usado em educação, saúde, finanças, etc.

Risco ampliado: Como esses sistemas não têm um único propósito, podem ser utilizados em aplicações de alto risco (ex: decisões médicas, seleção de candidatos, controle de infraestrutura crítica) sem o conhecimento ou controle do fornecedor original.

Seção 2 – Responsabilidades no AI Act

O AI Act estabelece obrigações específicas para GPAIs, dividindo responsabilidades entre:

Fornecedores do modelo GPAI:

- Devem avaliar riscos sistêmicos, como uso indevido ou amplificação de desinformação;
- Implementar medidas de mitigação, como filtros e limites;
- Garantir documentação técnica clara, com explicação do modelo, limitações e contextos de uso;
- Comunicar incidentes graves às autoridades competentes.

Desenvolvedores que criam ou usam GPAIs:

- Precisam testar e validar o uso específico;
- Devem assegurar conformidade com o AI Act se a aplicação final for de alto risco;
- Devem seguir os requisitos de transparência e rastreabilidade.

Seção 3 – Como lidar com GPAIs na prática?

Organizações que adotam ou integram GPAIs devem criar um processo claro para:

1. Identificar quando um sistema usado é de uso geral;
2. Avaliar riscos do uso pretendido com base no contexto local;
3. Definir limites de uso e regras internas para evitar aplicações indevidas;
4. Manter logs e registros para auditorias e eventuais incidentes;
5. Treinar equipes sobre os riscos e responsabilidades associadas.

Exemplo prático:

Uma empresa usa um modelo de linguagem para automatizar respostas de atendimento ao cliente. O modelo GPAI pode sugerir respostas incorretas ou ofensivas. A empresa precisa configurar filtros, testar respostas e manter logs de conversas automatizadas — medidas que alinharam o uso ao AI Act e aos controles da ISO.



Capítulo 20 – Sistemas de IA Proibidos

Introdução ao Capítulo

Nem toda aplicação de Inteligência Artificial é permitida. O AI Act define um conjunto claro de sistemas de IA que são expressamente proibidos na União Europeia — por representarem riscos inaceitáveis aos direitos humanos, à liberdade e à dignidade das pessoas.

Neste capítulo, você vai aprender:

- Quais são os sistemas de IA proibidos pelo AI Act;
- Como identificá-los em sua organização ou cadeia de fornecedores;
- Qual a relação entre esses sistemas e os princípios da ISO/IEC 42001;
- Como evitar a violação das regras e garantir conformidade ética.

A proibição de sistemas de IA com riscos inaceitáveis mostra que a regulação europeia está focada em proteger o ser humano acima da tecnologia. Com base na ISO 42001, é possível construir um sistema de gestão que previna essas práticas desde o planejamento.

Seção 1 – O que são sistemas de IA proibidos?

O AI Act proíbe sistemas de IA que:

1. Manipulem o comportamento humano de maneira que distorça significativamente a autonomia ou o livre-arbítrio da pessoa;
2. Façam exploração de vulnerabilidades, como crianças, idosos ou pessoas com deficiência;
3. Classifiquem pessoas com base em características sociais ou comportamentais (ex: pontuação social);
4. Façam reconhecimento biométrico em tempo real em espaços públicos para fins de vigilância massiva (exceto exceções estritas);
5. Use IA subliminar para influenciar decisões inconscientes de forma perigosa.

Essas práticas são consideradas incompatíveis com os valores fundamentais da União Europeia, como dignidade, privacidade, liberdade e não discriminação.

Seção 2 – Como identificar esses riscos?

Mesmo sem intenção, organizações podem adotar ferramentas de terceiros ou soluções “caixa preta” que, ao serem analisadas, configuram sistemas de IA proibidos.

Passos para identificação:

- Avalie o contexto de uso da IA: há vigilância, controle, manipulação?
- Revise os dados utilizados: envolvem biometria em tempo real?
- Analise se o sistema pode influenciar decisões de forma subliminar.
- Verifique se há avaliação de impacto e registros técnicos claros.

Conexão com a ISO/IEC 42001	
Controle	Aplicação prática ao tema
A.5.2 – Avaliação de Impacto	Ajuda a identificar riscos éticos e legais
A.9.1 – Uso Responsável	Define limites claros para finalidades aceitáveis
A.3.2 – Política de IA	Deve proibir explicitamente práticas vedadas pelo AI Act
A.6.4 – Registro de Eventos	Permite rastrear usos indevidos ou não autorizados

Seção 3 – Exemplo prático

Cenário: Uma empresa adota uma ferramenta de recrutamento com IA para classificar candidatos.

Ao investigar a ferramenta, descobre-se que o sistema aplica uma pontuação de comportamento online dos candidatos, com base em dados de redes sociais e padrões de escrita — criando classificação social automatizada.

Resultado: esse tipo de IA é proibido pelo AI Act. A empresa deve descontinuar seu uso e implementar processos internos de avaliação de risco antes da adoção de novas tecnologias.

Seção 4 – Como sua organização deve agir?

- Crie uma política clara de uso responsável da IA, alinhada à legislação;
- Adote uma matriz de checagem de proibições antes de implementar qualquer sistema de IA;
- Treine áreas técnicas e jurídicas sobre os tipos de sistemas proibidos;
- Exija de fornecedores uma declaração de conformidade com o AI Act.



Capítulo 21 – PMEs e Startups: Oportunidades e Obrigações

Introdução ao Capítulo

Pequenas e Médias Empresas (PMEs), bem como startups de base tecnológica, desempenham um papel vital no ecossistema europeu de inovação em inteligência artificial. No entanto, com a entrada em vigor do AI Act, essas organizações se deparam com desafios e responsabilidades específicas – ao mesmo tempo em que se beneficiam de apoios e flexibilizações regulatórias.

Neste capítulo, você vai entender:

- Quais obrigações específicas o AI Act traz para PMEs e startups;
- Quais oportunidades e incentivos estão disponíveis;
- Como a ISO/IEC 42001 oferece um caminho acessível para a conformidade;
- Um passo a passo de adaptação com foco em agilidade e viabilidade econômica.

As PMEs não são coadjuvantes na regulação de IA. Pelo contrário, elas são atores estratégicos, essenciais para o equilíbrio entre inovação e responsabilidade. O AI Act reconhece isso ao oferecer suporte direcionado – e a ISO 42001 fornece um roteiro claro e acessível para que pequenas empresas possam crescer com segurança e ética.

Seção 1 – O que muda para PMEs com o AI Act?

O regulamento europeu prevê obrigações proporcionais ao porte e à capacidade da organização. Isso significa que:

- Startups e PMEs não estão isentas de requisitos;
- Mas há exceções, prazos estendidos e apoio técnico-financeiro para facilitar a adaptação.

Exemplos de obrigações que permanecem válidas:

- Garantia de transparência nos sistemas de IA generativa;
- Avaliação de impacto em sistemas de alto risco;
- Registro e documentação mínima obrigatória;
- Cumprimento das exigências de segurança e direitos fundamentais.

Conexão com a ISO 42001:

- A.2.4 – Análise da política de IA: Revisar as políticas organizacionais mesmo em estruturas enxutas;
- A.6.1 – Controles mínimos no ciclo de vida do sistema de IA: Definir processos com base no escopo de atuação da PME;
- A.5.2 – Avaliação de impactos adaptada: Aplicar proporcionalidade na análise de riscos.

Seção 2 – Flexibilizações e Apoio à Conformidade

O AI Act prevê uma série de medidas para evitar que PMEs sejam sobre carregadas. Entre elas:

Acesso facilitado a:

- Espaços controlados de testes (AI Sandboxes), inclusive em parcerias com governos e universidades;
- Guias simplificados e capacitações específicas para PMEs;
- Suporte técnico via centros de inovação digital.

Menor carga de conformidade:

- Redução na quantidade de documentação exigida;
- Prazos mais longos para adaptação;
- Uso de ferramentas de código aberto recomendadas pela UE.

Seção 3 – Caminho prático para adequação de uma PME

Um roteiro básico pode seguir as seguintes etapas:

1. Mapeie os sistemas de IA em uso ou em desenvolvimento;
2. Classifique o risco de cada sistema conforme as categorias do AI Act;
3. Defina políticas internas mínimas com base na ISO 42001;
4. Implemente controles básicos de segurança e explicabilidade;
5. Documente os fluxos essenciais (dados, decisões e logs);
6. Capacite a equipe técnica e os responsáveis legais;
7. Busque apoio em hubs locais ou iniciativas europeias de sandbox.

Seção 4 – Por que adotar a ISO 42001 é um diferencial competitivo?

Para uma startup ou PME, a certificação (ou adoção interna) da ISO/IEC 42001 pode:

- Evitar multas e barreiras comerciais;
- Gerar confiança em investidores e clientes;
- Aumentar a chance de entrar em parcerias com grandes empresas ou governos;
- Ser um sinal de maturidade de gestão de IA, mesmo em empresas emergentes.



Capítulo 22 – Cadeia de Valor da IA: Responsabilidades Compartilhadas.

Introdução ao Capítulo

A Inteligência Artificial não é construída e operada por um único agente. Ao contrário, ela é resultado de uma cadeia de valor complexa, com múltiplos envolvidos: desenvolvedores, fornecedores, integradores, usuários finais, autoridades reguladoras e terceiros. O AI Act da União Europeia introduz um modelo claro de responsabilidades compartilhadas, atribuindo obrigações específicas a cada elo dessa cadeia.

Neste capítulo, você aprenderá:

- Como a cadeia de valor da IA é organizada segundo o regulamento;
- As responsabilidades de cada ator (desenvolvedor, distribuidor, integrador, usuário etc.);
- A relação com os princípios da ISO/IEC 42001;
- Como garantir rastreabilidade e conformidade em ecossistemas com múltiplos atores.

Com a regulação europeia, a inteligência artificial deixa de ser uma “caixa preta” operada por um único responsável. Cada ator da cadeia de valor – da criação ao uso – precisa entender e cumprir suas obrigações. A ISO/IEC 42001 ajuda as organizações a sistematizarem esse processo, promovendo responsabilidade distribuída e uma cultura de transparência. Afinal, só é possível confiar em um sistema de IA quando se sabe quem faz o quê, como e por quê.

Seção 1 – Quem faz parte da cadeia de valor da IA?

Segundo o AI Act, os principais papéis e responsabilidades se dividem entre:

Cadeia de Valor	
Autor	Responsabilidades Principais
Provedor (Desenvolvedor)	Cria o sistema de IA; realiza testes; garante conformidade antes de colocar no mercado
Distribuidor	Comercializa, sem alterar as funções da IA; garante que o sistema esteja em conformidade
Importador	Traz sistemas de IA de fora da UE para o mercado europeu; verifica se há documentação
Integrador Implementador	Adapta ou combina sistemas de IA para usos específicos em organizações ou produtos
Usuário Profissional	Opera a IA com responsabilidade; registra logs; segue instruções técnicas
Terceiros/Prestadores de serviço	Podem prover dados, infraestrutura, modelos ou serviços auxiliares

Seção 2 – O que muda com o AI Act?

O regulamento europeu traz uma abordagem precisa e preventiva:

- Cada agente tem responsabilidades próprias documentadas;
- Se um agente modifica substancialmente o sistema de IA (ex: reconfigura o modelo), ele assume o papel de provedor;
- Todos os envolvidos devem manter documentação técnica e informações acessíveis às autoridades reguladoras;
- Em casos de sistemas de alto risco, há exigências adicionais: registros, logs, avaliações de impacto e supervisão humana.

Seção 3 – Como se proteger em um ecossistema distribuído?

Empresas que atuam em cadeias de fornecimento complexas devem adotar boas práticas de gestão, como:

Incluir cláusulas contratuais específicas de conformidade com o AI Act;

Solicitar e compartilhar documentação técnica entre parceiros;

Realizar avaliações de impacto colaborativas, especialmente quando houver integração de sistemas;

Definir claramente quem é o “operador primário” em relação ao uso e risco da IA;

Utilizar frameworks como a ISO 42001 para organizar a governança distribuída e documentar os processos.

Seção 4 – Rastreabilidade, Transparência e Confiança

A rastreabilidade do sistema de IA – ou seja, o histórico completo de desenvolvimento, modificações, decisões automatizadas e uso – se torna essencial para:

- Investigações regulatórias;
- Proteção dos direitos dos usuários;
- Confiança comercial e contratual;
- Auditorias internas ou de terceiros.

Conexão com a ISO/IEC 42001:

- A.6.4 – Registro de logs de eventos
- A.2.4 – Análise crítica da política de IA
- B.3.3 – Relato de preocupações
- A.8 – Documentação técnica e comunicação com partes interessadas



Capítulo 23 – Responsabilidade Civil e Direitos dos Usuários

Introdução ao Capítulo

Neste capítulo, vamos tratar de um tema fundamental: o que acontece quando um sistema de IA causa um dano? Quem é o responsável? E como o cidadão pode se proteger?

Você vai entender:

- O que é responsabilidade civil na IA;
- Quais são os direitos assegurados aos usuários e cidadãos pela legislação europeia;
- Como isso se conecta com a ISO/IEC 42001;
- Exemplos práticos de responsabilidade;
- Boas práticas para mitigar riscos e proteger direitos.

Seção 1 – O que é responsabilidade civil na IA?

A responsabilidade civil é o “freio de segurança” do desenvolvimento de IA.

Saber quem responde em caso de dano protege as pessoas e estimula organizações a agirem com mais responsabilidade.

Responsabilidade civil é o dever de reparar um dano causado a outra pessoa. Com a IA, isso pode incluir danos:

- Materiais (financeiros ou físicos);
- Morais (violação de direitos);
- Sociais (discriminação, exclusão, etc.).

Exemplo: Se um sistema de IA de recrutamento rejeita automaticamente currículos com base em um viés de gênero, a empresa pode ser responsabilizada por discriminação.

Na União Europeia, o AI Act se articula com a Diretiva de Responsabilidade por Produtos Defeituosos e outras normas que já preveem compensação por danos causados por tecnologias.

Seção 2 – Quais são os direitos dos usuários?

Os usuários têm o direito de:

- Saber que estão interagindo com um sistema de IA (transparéncia);
- Recusar o uso de IA em decisões sensíveis (como crédito, saúde, justiça);
- Solicitar explicações de decisões automatizadas;
- Apontar falhas e pedir correções;
- Obter compensação por danos.

Exemplo: Uma pessoa pode contestar uma decisão de negação de empréstimo feita exclusivamente por IA e exigir revisão humana.

Esses direitos reforçam o princípio de uma IA centrada no ser humano, como defendido pelo AI Act e pela ISO/IEC 42001.

Conexão com a ISO/IEC 42001	
Controle ISO 42001	Relação com o Tema
A.9.2 - Responsabilidade e accountability	Define papéis e prestação de contas no uso da IA
A.8.3 - Supervisão humana significativa	Garante decisões críticas com possibilidade de contestação
A.7.4 - Comunicação com partes interessadas	Reforça o direito de informação e resposta a incidentes
A.9.1 - Uso responsável	Estabelece limites éticos e legais no uso da IA

Seção 3 – Boas práticas para mitigar riscos

As organizações podem adotar práticas que evitam problemas legais e protegem o usuário, como:

- Design transparente e rastreável dos sistemas;
- Registro de logs para reconstruir decisões automatizadas;
- Procedimentos de resposta rápida a incidentes;
- Formação contínua em ética, direitos digitais e governança de IA.

Dica prática: Inclua cláusulas de responsabilidade e mecanismos de recurso nos contratos com fornecedores de IA.

Seção 4 – Caminhos para uma IA mais justa

Responsabilidade não é apenas evitar processos, mas construir relações de confiança com clientes, usuários e a sociedade.

Adotar princípios claros de justiça algorítmica, respeito aos direitos e prestação de contas é a base de um sistema de IA confiável.



UE AI ACT

Capítulo 24 – Diretrizes para Integração com a ISO/IEC 42001

Introdução ao Capítulo

Até aqui, vimos como o AI Act da União Europeia impõe regras e responsabilidades para o uso de inteligência artificial. Mas como transformar isso em prática dentro de uma empresa?

Neste capítulo, você vai descobrir:

- Como a norma ISO/IEC 42001 ajuda a implementar o AI Act;
- Passo a passo para integrar o sistema de gestão de IA;
- Controles e indicadores recomendados;
- Conexões entre a ISO e os requisitos legais europeus;
- Dicas práticas para auditoria e certificação.

Seção 1 – O que é a ISO/IEC 42001?

A ISO/IEC 42001 é um caminho confiável e estruturado para se adaptar ao AI Act. Ela ajuda a alinhar tecnologia, ética e conformidade – e fortalece a confiança no uso da IA.

É a primeira norma internacional para gestão de sistemas de IA. Publicada em 2023, ela traz uma estrutura semelhante à ISO 9001 (qualidade) e à ISO/IEC 27001 (segurança da informação), mas focada na governança de IA responsável e segura.

Ela oferece:

- Requisitos para políticas, riscos, objetivos, operação e monitoramento de IA;
- Diretrizes para tratar aspectos éticos, legais e técnicos;
- Modelo escalável para empresas de qualquer porte.

Importante: A ISO 42001 não substitui o AI Act, mas facilita sua aplicação e auditoria. Usá-la é um diferencial estratégico.

Seção 2 – Pontos de convergência entre AI Act e ISO 42001

Veja alguns exemplos de como os dois documentos se conectam:

AI Act	ISO/IEC 42001
Avaliação de riscos de sistemas de alto risco	Seção 6.1.2 – Avaliação de riscos de IA
Requisitos de documentação técnica	Seção 7.5 – Informação documentada
Supervisão humana em decisões automatizadas	A.8.3 – Supervisão humana significativa
Canal de denúncias e governança ética	A.3.3 – Relato de preocupações
Transparência e comunicação com usuários	A.8.4 – Informação às partes interessadas
Responsabilidade e prestação de contas	A.9.2 – Accountability

Seção 3 – Como aplicar a ISO/IEC 42001 na prática?

Para integrar os dois frameworks, siga estas etapas:

1. Diagnóstico inicial: Avalie onde sua organização está em termos de uso de IA;
2. Planejamento: Defina uma política de IA e objetivos alinhados ao negócio;
3. Governança: Estabeleça papéis, responsabilidades e comitês de IA;
4. Controles e indicadores: Use a Tabela A.1 da ISO para definir práticas de conformidade;
5. Capacitação: Treine as equipes em riscos, ética e boas práticas com IA;
6. Monitoramento e melhoria: Avalie resultados, trate incidentes e revise periodicamente.

💡 Ferramenta útil: A ISO recomenda o uso de um inventário de sistemas de IA, avaliando risco, propósito, dados usados e controle humano envolvido.

Seção 4 – Indicadores (KPIs) recomendados

Alguns KPIs úteis sugeridos pela norma:

Indicador	Objetivo
% de sistemas de IA avaliados quanto a impacto	Medir governança e responsabilidade
% de incidentes resolvidos no prazo	Avaliar eficiência da resposta a falhas
% de áreas com política de IA implementada	Verificar integração da governança de IA
Nº de treinamentos realizados sobre IA ética	Medir conscientização interna
Transparência e comunicação com usuários	A.8.4 – Informação às partes interessadas

Seção 5 – Caminhos para certificação

A certificação ISO 42001 ainda é voluntária, mas já está sendo adotada por empresas que:

- Desejam provar conformidade com legislações como o AI Act;
- Participam de licitações públicas ou projetos regulados;
- Querem demonstrar transparência para clientes e investidores.

Dica prática: Comece com uma autoavaliação guiada. Depois, avance para uma auditoria interna e finalmente para a certificação por órgão independente.



UE AI ACT

Capítulo 25 – Casos Reais de Aplicação do AI Act na Prática

Introdução ao Capítulo

O AI Act já está moldando o cenário da inteligência artificial na Europa. Mas como as organizações estão aplicando essas regras no dia a dia?

Neste capítulo, você vai conhecer:

- Exemplos práticos de empresas e governos adaptando seus sistemas;
- Como evitar penalidades com base em erros reais;
- Aplicações específicas da ISO/IEC 42001 para facilitar a conformidade;
- Lições aprendidas para aplicar em sua organização.

Os estudos de caso mostram que o AI Act não é uma barreira, mas um guia para uso responsável da IA. A ISO/IEC 42001 funciona como ponte entre a teoria da regulação e a prática do dia a dia.

Com planejamento, adaptação e monitoramento, qualquer organização pode transformar conformidade em diferencial competitivo.

Seção 1 – Estudo de Caso: Hospital Público na Espanha

Contexto:

Um hospital em Barcelona implementou um sistema de IA para priorizar atendimentos de emergência com base em histórico e sintomas dos pacientes.

Desafio:

O sistema, apesar de eficiente, apresentava viés contra pacientes idosos e estrangeiros, que eram preferidos na fila de urgência.

Ação corretiva (AI Act + ISO/IEC 42001):

- Realização de avaliação de impacto algorítmico (A.5);
- Implementação de supervisão humana obrigatória (A.8.3);
- Revisão dos critérios de priorização com base em evidências clínicas.

Conexão ISO: A.6.2 – Desenvolvimento responsável

Resultado: O hospital manteve a IA com correções e evitou sanções de órgãos reguladores.

Seção 2 – Estudo de Caso: Indústria Automotiva na Alemanha

Contexto:

Uma fabricante alemã usava IA para classificar automaticamente candidatos em seu processo seletivo.

Problema:

O algoritmo reproduzia preconceitos históricos – rejeitando mais mulheres para cargos técnicos.

Correções feitas:

- Aplicação do princípio de não discriminação algorítmica;
- Inclusão de comitê interno de ética em IA (A.3.1);
- Treinamento sobre viés algorítmico para a equipe de RH (A.3.2).

Conexão AI Act: Sistemas de risco elevado em recursos humanos

Resultado: Conformidade restaurada e melhoria da reputação da marca.

Seção 3 – Estudo de Caso: Administração Pública em Portugal

Contexto:

A Secretaria de Transportes usava IA para análise de comportamento de motoristas e emissão automática de multas.

Erro:

O sistema penalizava de forma indevida veículos em áreas com sinalização mal interpretada por câmeras.

Medidas adotadas:

- Revisão da documentação técnica e logs de decisão (A.6.4);
- Adoção de processo de contestação transparente (A.8.5);
- Inclusão de supervisão humana em decisões automáticas.

Conexão ISO: A.9.1 – Uso responsável da IA

Resultado: Redução de 35% em reclamações judiciais.

Seção 4 – Lições aprendidas dos casos

1. Supervisão humana não é opcional: Toda decisão crítica precisa de possibilidade de revisão humana.
2. A documentação salva: Manter registros técnicos é éticos evita penalidades.
3. Treinamento recorrente: Equipes bem formadas reduzem riscos e melhoram a cultura organizacional.
4. Transparência é o novo padrão: Cidadãos e clientes querem saber como e por que a IA decide.



Capítulo 26 – Conclusão: Inteligência Artificial com Propósito e Responsabilidade

Introdução ao Capítulo

Depois de percorrer todos os aspectos regulatórios, técnicos, éticos e estratégicos da nova era da inteligência artificial, este capítulo final tem como objetivo:

- Recapitular os principais aprendizados do livro;
- Reforçar o papel central da ISO/IEC 42001 como guia de governança;
- Refletir sobre os caminhos possíveis para o futuro da IA;
- Inspirar líderes e profissionais a construírem um ecossistema confiável, seguro e ético.

Seção 1 – O que aprendemos com o AI Act?

O AI Act representa um marco histórico ao trazer regras claras, proporcionais e baseadas em risco para regular a IA em todo o mercado europeu — com reflexos globais.

Principais aprendizados:

- Nem toda IA será regulada da mesma forma: o risco define o nível de exigência;
- Transparéncia, explicabilidade, supervisão humana e proteção de direitos são pilares centrais;
- Os deveres não são apenas para desenvolvedores — usuários, fornecedores e autoridades também têm obrigações claras;
- A IA deve ser centrada no ser humano, protegendo a dignidade, a democracia e os valores fundamentais.

Conclusão Final

Este livro mostrou que é possível — e necessário — alinhar inovação com responsabilidade.

A inteligência artificial é uma ferramenta poderosa. Mas, como qualquer ferramenta, precisa ser guiada por valores, ética e transparéncia. Com o AI Act, a União Europeia assume a liderança global neste movimento, e a ISO/IEC 42001 nos dá o mapa do caminho.

O futuro da IA será confiável, humano e justo — se escolhermos construí-lo assim.

Seção 2 – A ISO/IEC 42001 como suporte prático

Se o AI Act mostra o “o que deve ser feito”, a norma ISO/IEC 42001 mostra “como fazer”. Ela permite transformar as exigências legais em processos organizacionais reais, por meio de:

- Controles por tema (dados, impacto, uso, ciclo de vida, terceiros etc.);
- Gestão de riscos e melhoria contínua;
- Cultura ética e governança participativa;
- Auditorias internas e planos de conformidade documentados.

ISO como base para certificações futuras e diferencial competitivo global.

Seção 3 – Oportunidades para inovação responsável

A regulação não é o fim da inovação — é o início de uma nova era de inovação com propósito. Com regras claras, o ambiente se torna mais seguro para:

- Investidores;
- Consumidores;
- Startups;
- Governos;
- Grandes corporações.

A IA responsável não é uma opção: é o padrão para crescer com confiança e sustentabilidade.

Seção 4 – Uma nova mentalidade

Para além das regras, o AI Act nos convida a repensar a relação entre tecnologia e humanidade.

Mais do que cumprir regulamentos, é hora de:

- Criar confiança nas soluções algorítmicas;
- Garantir que a tecnologia amplifique o bem-estar;
- Inspirar novos modelos de negócio, governo e sociedade.



11

IA NO BRASIL

Entendendo o PL 2338/2023 na Prática



O EU AI Act e a ISO/IEC 42001 representam duas abordagens complementares para garantir o uso responsável da inteligência artificial. Enquanto o AI Act é uma lei obrigatória da União Europeia que regula sistemas com base em níveis de risco, a ISO 42001 é uma norma internacional voluntária focada na criação de um sistema de gestão organizacional da IA. Ambos enfatizam a importância da transparência, gestão de riscos, responsabilidade e direitos humanos. A principal diferença está na obrigatoriedade legal do AI Act, com sanções aplicáveis, e no caráter orientador da ISO. Juntos, oferecem uma base robusta para empresas que buscam conformidade e governança de IA. A adoção integrada fortalece a confiança, segurança e inovação ética.

PROLÓGICO
PREFÁCIO

CONTEXTO DE IA

LIDERANÇA

PLANEJAMENTO

SUPORTE

OPERAÇÃO

DESEMPENHO

MELHORIA

CONTROLES

POLÍTICA

ORGANIZAÇÃO

RECURSOS

IMPACTOS

CICLO

DADOS

INFORMAÇÃO

SISTEMA

RELACIONAMENTO

OBJETIVOS ORGANIZACIONAIS POTENCIAIS E FONTES DE RISCO RELACIONADOS À IA

REGULAMENTAÇÃO UE ACT

INTELIGÊNCIA ARTIFICIAL NO BRASIL - ENTENDENDO O PL 2338/2023 NA PRÁTICA



Capítulo 1 – Fundamentos e Princípios da IA no Brasil

Introdução ao Capítulo

O Projeto de Lei 2338/2023 tem como objetivo estabelecer um marco legal para o desenvolvimento e uso de sistemas de Inteligência Artificial (IA) no Brasil. Neste capítulo, explicamos os princípios fundamentais que orientam a proposta, com foco na proteção de direitos, na promoção da inovação responsável e na criação de um ambiente seguro e ético para o uso da IA no país.

Você vai entender:

- Os principais objetivos da regulação de IA no Brasil;
- Quais são os princípios que guiarão o desenvolvimento e uso da IA;
- Como esses princípios se conectam com boas práticas internacionais, como a ISO/IEC 42001.

Seção 1 – Por que regular a Inteligência Artificial?

A IA está cada vez mais presente na vida dos brasileiros — desde algoritmos que recomendam conteúdo em plataformas digitais até sistemas que auxiliam decisões no setor público e privado. A regulação surge como uma forma de:

O PL 2338/2023 dá os primeiros passos rumo a um futuro tecnológico mais ético, seguro e humano no Brasil. Os princípios apresentados neste capítulo serão a base para as regras e obrigações que veremos nos próximos capítulos, conectando os valores brasileiros a uma governança moderna e eficaz em IA.

- Proteger direitos fundamentais;
- Garantir segurança jurídica para empresas;
- Promover o desenvolvimento científico e tecnológico;
- Evitar abusos no uso da tecnologia.

O PL reconhece que a IA pode tanto impulsionar o bem-estar social quanto representar riscos à privacidade, à dignidade humana e à justiça.

Conexão com a ISO/IEC 42001

A ISO/IEC 42001 também estabelece a necessidade de sistemas de gestão de IA responsáveis, enfatizando riscos, transparéncia e direitos fundamentais.

Seção 2 – Princípios norteadores da IA no Brasil

O PL define os princípios que deverão guiar a criação, uso e supervisão de sistemas de IA no país:

1. Centralidade na pessoa humana
2. A tecnologia deve servir às pessoas, e não o contrário.
3. Respeito aos direitos fundamentais
4. Garantia de que a IA não viole direitos como privacidade, igualdade e não discriminação.
5. Transparéncia
6. Os sistemas devem ser compreensíveis e auditáveis.
7. Responsabilização
8. Os agentes envolvidos no desenvolvimento e uso da IA devem ser responsáveis por seus impactos.
9. Segurança
10. A IA deve ser confiável, segura e robusta em todas as etapas do seu ciclo de vida.
11. Inovação e promoção da livre iniciativa
12. Incentivo à pesquisa e ao desenvolvimento econômico.
13. Promoção da inclusão e redução das desigualdades
14. A IA deve contribuir para o bem coletivo, sem excluir grupos vulneráveis.

Conexão com a ISO/IEC 42001

Esses princípios são equivalentes aos fundamentos que guiam o sistema de gestão de IA da ISO 42001, especialmente os controles relacionados a ética, impacto social e responsabilidade organizacional.

Seção 3 – Aplicação da lei e seus limites

O PL se aplica a todos os sistemas de IA utilizados em território nacional, independentemente da origem do sistema. Isso significa que:

- Empresas estrangeiras que operam no Brasil também devem respeitar os princípios da lei;
- A responsabilidade não recai apenas sobre quem desenvolve, mas também sobre quem usa ou toma decisões com apoio da IA.



IA NO BRASIL - Entendendo o PL 2338/2023 na Prática

Capítulo 2 – Direitos das Pessoas Afetadas pela IA

Introdução ao Capítulo

A Inteligência Artificial já faz parte da nossa vida — nas redes sociais, no atendimento ao cliente, na educação e até na saúde. Mas como garantir que ela seja usada de forma justa, transparente e respeitosa com as pessoas?

O PL 2338/2023 reconhece que os cidadãos precisam ser protegidos contra abusos e decisões injustas tomadas por sistemas automatizados. Neste capítulo, vamos entender os direitos garantidos às pessoas que são afetadas por tecnologias de IA — e como eles devem ser respeitados por empresas e órgãos públicos.

Você vai aprender sobre:

- O direito de saber quando está lidando com uma IA;
- O direito de pedir explicações e contestar decisões;
- A obrigação de haver supervisão humana;
- Como a lei combate discriminação e viés algorítmico.

Seção 1 – Direito à informação e transparência

Toda pessoa tem o direito de ser informada de forma clara quando estiver interagindo com um sistema de IA, especialmente se esse sistema:

- Influencia decisões que afetam sua vida (ex: crédito, contratação, serviços públicos);
- Realiza análises de comportamento ou perfil;
- Toma decisões automatizadas sem contato humano.

Exemplo prático:

Se você for avaliado por um sistema automatizado em uma seleção de emprego, tem o direito de saber disso antecipadamente e entender como ele funciona.

Seção 2 – Direito à explicação e contestação

Pessoas têm o direito de:

- Receber explicações compreensíveis sobre como uma decisão foi tomada pela IA;
- Contestar decisões automatizadas, especialmente se forem negativas ou impactarem seus direitos;
- Ter a possibilidade de revisão por um ser humano, quando necessário.

Exemplo prático:

Se um banco negar seu pedido de empréstimo com base em um algoritmo, você pode exigir uma explicação da lógica usada e solicitar reavaliação.

Seção 3 – Intervenção humana nas decisões automatizadas

Mesmo com o avanço das tecnologias, o projeto de lei deixa claro: decisões críticas não devem ser deixadas exclusivamente nas mãos das máquinas.

É obrigatório haver supervisão humana significativa, com profissionais capacitados para revisar e intervir sempre que necessário — especialmente em sistemas de alto risco.

Exemplo prático:

Uma IA pode sugerir um diagnóstico médico, mas a decisão final sempre será de um profissional de saúde.

Seção 4 – Correção de vieses e proteção à não-discriminação

Sistemas de IA podem reproduzir preconceitos se forem treinados com dados tendenciosos. Por isso, o PL garante:

- O direito à igualdade de tratamento, sem discriminação por raça, gênero, orientação sexual ou origem;
- A obrigação de empresas e órgãos públicos de corrigir algoritmos enviesados;
- Medidas específicas para proteger grupos vulneráveis.

Exemplo prático:

Um algoritmo de triagem para bolsas de estudo que favorece apenas alunos de determinada região pode estar violando esse direito e deve ser ajustado.

Coneção com a ISO/IEC 42001:

A ISO também prevê diretrizes para proteção dos direitos das pessoas:

- A.9 – Uso responsável: Garante que a IA seja usada com ética e justiça.
- A.7 – Privacidade e proteção de dados: Protege informações pessoais e sensíveis.



IA NO BRASIL - Entendendo o PL 2338/2023 na Prática

Capítulo 3 – Classificação de Riscos em Sistemas de IA

Introdução ao Capítulo

Este capítulo apresenta como o Projeto de Lei 2338/2023 organiza a classificação de riscos nos sistemas de Inteligência Artificial no Brasil. Com base no impacto que esses sistemas podem causar à sociedade, às liberdades individuais e aos direitos fundamentais, o projeto define três categorias principais de risco: risco excessivo, alto risco e demais sistemas. A categorização é o ponto de partida para determinar quais obrigações legais e de governança serão exigidas.

Você aprenderá:

- O que é uma avaliação preliminar de risco;
- Quais sistemas de IA são proibidos no Brasil (risco excessivo);
- Quais sistemas são considerados de alto risco e as suas obrigações específicas;
- Como a ISO 42001 auxilia na estruturação dessa governança.

Seção 1 – Avaliação Preliminar

Antes de um sistema de IA ser colocado no mercado ou usado em serviços, ele deve passar por uma avaliação preliminar, feita pelo fornecedor, para classificar seu grau de risco.

Ponto-chave: A avaliação deve ser documentada, mesmo que o sistema não seja considerado de alto risco.

A autoridade reguladora poderá reavaliar a classificação e exigir medidas adicionais, como a avaliação de impacto algorítmico. Uma avaliação fraudulenta ou incompleta pode gerar sanções.

A categorização de riscos é um instrumento essencial para balancear inovação e segurança. Ela determina quem precisa cumprir o quê e evita que sistemas com grande potencial de dano operem sem o devido controle.

Empresas devem estar atentas à documentação e justificativas técnicas para suas classificações e manter atualizações sempre que houver mudanças significativas no uso ou no contexto do sistema.

Conexão com ISO/IEC 42001:

- A.5.2 – Avaliação de risco
- A.6.1 – Planejamento do ciclo de vida

Seção 2 – Sistemas de Risco Excessivo

São proibidos os sistemas de IA que:

- Induzem comportamentos prejudiciais por meio de técnicas subliminares;
- Exploram vulnerabilidades de pessoas com deficiência ou em situação de fragilidade (como crianças e idosos);
- Criam sistemas de pontuação social pelo poder público com base em comportamento ou traços pessoais.

Além disso, o uso de reconhecimento biométrico à distância pelo Estado só é permitido com autorização judicial, em situações específicas de investigação criminal.

Conexão com ISO/IEC 42001:

- A.9 – Uso responsável
- A.7 – Privacidade e proteção de dados

Seção 3 – Sistemas de Alto Risco

Sistemas são classificados como de alto risco quando utilizados em atividades críticas como:

- Gestão de infraestrutura (energia, trânsito);
- Educação e avaliação de alunos;
- Recrutamento e RH;
- Assistência social e concessão de benefícios;
- Classificação de crédito;
- Saúde e diagnóstico médico;
- Justiça e segurança pública;
- Veículos autônomos.

Esses sistemas exigem governança robusta, documentação técnica, registro de logs e avaliação de impacto algorítmico contínua.

Conexão com ISO/IEC 42001:

- A.6.4 – Registro de logs
- A.8 – Gestão da mudança
- A.5.2 – Avaliação de impacto

Seção 4 – Atualização da Classificação

A autoridade competente poderá atualizar a lista de sistemas de risco com base em critérios como:

- Número de pessoas afetadas;
- Impacto a direitos e liberdades;
- Probabilidade e gravidade dos danos;
- Nível de transparéncia e explicabilidade do sistema.

Essas atualizações devem ser precedidas de consultas públicas e análise de impacto regulatório.



IA NO BRASIL - Entendendo o PL 2338/2023 na Prática

Capítulo 4 – Governança e Boas Práticas de IA

Introdução ao Capítulo

A governança dos sistemas de Inteligência Artificial (IA) é essencial para garantir que seu uso seja seguro, transparente e alinhado aos direitos fundamentais das pessoas afetadas. O Projeto de Lei 2338/2023 estabelece diretrizes que devem ser seguidas por empresas, poder público e organizações no desenvolvimento e na operação de sistemas de IA. Neste capítulo, você aprenderá:

- Quais estruturas de governança devem ser criadas;
- Quais práticas são obrigatórias para sistemas de alto risco;
- Como promover transparência, segurança e participação social no uso da IA.

Seção 1 – Requisitos Gerais de Governança

O PL 2338/2023 determina que todos os agentes de IA (fornecedores e operadores) estabeleçam processos internos de governança para garantir a segurança dos sistemas e a proteção dos direitos dos usuários. Esses processos devem incluir:

- Medidas de transparência sobre a presença e funcionamento da IA em interações humanas;
- Governança clara sobre dados utilizados, evitando vieses discriminatórios;
- Garantia da privacidade e proteção de dados, com minimização de coleta e uso;
- Medidas de segurança da informação e separação entre dados para treinamento, testes e validação.

A governança é a espinha dorsal de um ecossistema de IA confiável. Mais do que seguir leis, ela garante que a IA seja usada para gerar valor real, respeitando direitos e minimizando riscos.

Essas práticas se aplicam ao longo de todo o ciclo de vida do sistema de IA: do desenvolvimento até a descontinuação.

Seção 2 – Procedimentos para Sistemas de Alto Risco

Sistemas classificados como de alto risco exigem cuidados adicionais. Segundo o PL, nesses casos, os agentes devem:

- Documentar todo o processo de desenvolvimento, testes, operação e encerramento;
- Manter registros automáticos de uso e desempenho do sistema;
- Realizar testes regulares de confiabilidade (acurácia, robustez, cobertura);
- Implementar medidas para explicabilidade do sistema, com explicações claras e acessíveis;
- Formar equipes diversas e inclusivas para concepção dos modelos.

No setor público, é obrigatório também realizar consultas públicas, garantir acesso a explicações humanas e publicar avaliações de impacto.

Seção 3 – Transparência e Documentação Técnica

A documentação é essencial para a prestação de contas. O PL exige que:

- Todos os sistemas de alto risco tenham documentação técnica disponível antes de seu uso;
- Os órgãos públicos divulguem avaliações de risco em seus sites;
- Sejam implementados protocolos de acesso e registro de uso de IA no setor público;
- Os operadores garantam a explicação humana sempre que decisões impactarem significativamente os direitos de uma pessoa.

A ausência de documentação e explicações pode resultar em penalidades, inclusive a suspensão do uso da tecnologia.

Conexão com ISO/IEC 42001

As boas práticas e governança do PL 2338/2023 se conectam diretamente com os seguintes controles da norma ISO:

- A.3 – Estrutura organizacional: define responsabilidades e papéis claros na gestão de IA.
- A.4 – Recursos: assegura que recursos técnicos, humanos e processuais estejam alocados para uma IA segura.
- A.8 – Gestão da mudança: trata da adaptação e controle contínuo dos sistemas de IA durante sua evolução.



Capítulo 5 – Avaliação de Impacto Algorítmico

Baseado no PL 2338/2023 | Conexão com ISO/IEC 42001: A.5.2 – Avaliação de impacto | A.6.1 – Planejamento do ciclo de vida

Introdução ao Capítulo

Neste capítulo, você entenderá como a Lei Brasileira de Inteligência Artificial exige que empresas e órgãos públicos realizem avaliações de impacto algorítmico (AIA) para sistemas considerados de alto risco. O objetivo é prevenir danos antes que a tecnologia afete a sociedade, garantindo segurança, responsabilidade e respeito aos direitos fundamentais.

Você vai aprender:

- Quando é obrigatória a avaliação de impacto;
- Como ela deve ser realizada e atualizada;
- A importância de envolver a sociedade no processo.

Seção 1 – Quando a Avaliação é Obrigatória?

A AIA é obrigatória sempre que um sistema for classificado como de alto risco na avaliação preliminar. Essa avaliação deve ser realizada antes da colocação do sistema no mercado ou do seu uso efetivo.

A Avaliação de Impacto Algorítmico é uma ferramenta essencial para garantir que a IA respeite valores humanos e evite danos. Não é apenas um requisito legal – é uma prática de responsabilidade ética e social.

A autoridade competente deve ser notificada, com o envio dos relatórios de avaliação preliminar e de impacto.

Seção 2 – Quem Deve Realizar?

A avaliação deve ser feita por profissionais com conhecimentos técnicos, jurídicos e científicos. Em certos casos, pode ser exigida a realização por equipe externa independente, conforme regulamentação da autoridade competente.

Seção 3 – Etapas da Avaliação

A metodologia da AIA deve conter, no mínimo, as seguintes fases:

1. Preparação: coleta de informações sobre o sistema.
2. Cognição de riscos: identificação dos impactos previsíveis.
3. Mitigação: definição de medidas para reduzir os riscos.
4. Monitoramento: acompanhamento contínuo durante o ciclo de vida da IA.

Além disso, o relatório da AIA deve documentar:

- Riscos conhecidos e seus impactos;
- Benefícios esperados;
- Consequências adversas e sua gravidade;
- Estratégias de mitigação e controle de qualidade;
- Ações de transparéncia ao público e às partes interessadas.

Casos com riscos irreversíveis devem considerar evidências incipientes, mesmo que incompletas ou especulativas.

Seção 4 – Transparéncia e Participação Pública

A avaliação de impacto deve ser pública em suas conclusões, respeitando segredos comerciais. As informações mínimas a serem divulgadas incluem:

- Finalidade e contexto do sistema;
- Medidas de mitigação e riscos residuais;
- Participação de grupos afetados, quando houver.

Além disso, atualizações periódicas são exigidas e devem incluir consulta pública simplificada.

Seção 5 – Conexão com ISO/IEC 42001

A ISO 42001 fortalece a governança da IA ao exigir que organizações documentem:

- O planejamento do ciclo de vida (A.6.1);
- A avaliação e mitigação contínua de riscos (A.5.2).

Essas exigências são alinhadas com a AIA prevista no PL 2338, promovendo transparéncia, responsabilidade e melhoria contínua.



Capítulo 6 – Responsabilidade Civil e Reparação de Danos

Introdução ao Capítulo

Quando um sistema de Inteligência Artificial (IA) causar danos a alguém – seja um cidadão, cliente ou empresa – como funciona a responsabilização? Este capítulo responde a essa pergunta de forma clara e acessível. Você vai aprender:

- Quais são as regras de responsabilidade quando há dano causado por IA;
- Como funciona a responsabilização em casos de sistemas de alto risco;
- Em que situações a empresa pode ser isenta;
- Como a ISO 42001 fortalece a prestação de contas e a documentação.

Seção 1 – Responsabilidade Objetiva em Sistemas de Alto Risco

O Projeto de Lei 2338/2023 estabelece que sistemas de IA classificados como alto risco ou risco excessivo geram responsabilidade objetiva.

Isso significa que a empresa ou fornecedor responde pelo dano mesmo que não tenha tido culpa, se houver prejuízo decorrente do sistema de IA.

Exemplo:

Se um sistema de IA utilizado para triagem de currículos excluir injustamente uma candidata por viés de gênero, a empresa poderá ser responsabilizada mesmo que não tenha intenção de discriminar.

Seção 2 – Inversão do Ônus da Prova

Nos casos em que não for possível à vítima entender como a IA tomou a decisão, o projeto prevê a inversão do ônus da prova:

A empresa deverá provar que seguiu todos os requisitos legais e técnicos.

Essa regra vale especialmente quando:

- Não há transparência no sistema;
- Faltam registros ou logs;
- A empresa negligenciou controles de risco.

Seção 3 – Limites da Responsabilidade

A responsabilidade não se aplica quando:

- A empresa provar que não usou ou não se beneficiou do sistema de IA;
- O dano for causado por terceiros ou por evento imprevisível (força maior);
- Houve fraude, uso indevido ou alteração externa no sistema.

Essa cláusula protege empresas de situações em que não há controle direto sobre a causa do problema.

Seção 4 – Código de Defesa do Consumidor e Complementaridade

Mesmo com a nova lei, as regras do Código de Defesa do Consumidor continuam válidas.

Ou seja, as vítimas mantêm seus direitos de reparação total, e o fornecedor deve garantir:

- Suporte ao consumidor;
- Transparéncia nos serviços automatizados;
- Acesso a canais de contestação e revisão humana.

Conexão com ISO/IEC 42001

A responsabilidade está alinhada com:

- A.9.2 – Responsabilidade e prestação de contas: exige que a organização defina papéis e mantenha registros sobre as decisões automatizadas.
- A.6.4 – Logs de eventos: reforça a importância de registrar todas as ações do sistema para fins de auditoria e prova em casos de incidentes.



Capítulo 7 – Códigos de Boas Práticas e Ética na IA

Baseado no Projeto de Lei 2.338/2023

Introdução ao Capítulo

Para além das obrigações legais previstas no PL 2.338/2023, o incentivo à criação de códigos de boas práticas representa uma das ferramentas mais poderosas para garantir o uso ético, seguro e responsável da Inteligência Artificial (IA). Esses códigos funcionam como instrumentos voluntários de autorregulação e governança, capazes de aumentar a confiança pública, fortalecer a reputação institucional e demonstrar o compromisso com os direitos fundamentais e a inovação sustentável.

Neste capítulo, você irá entender:

- O que deve conter um código de boas práticas em IA;
- A relação entre esses códigos e a governança interna das organizações;
- Como esses códigos podem ser reconhecidos como evidência de conformidade;
- Quais benefícios as organizações podem obter ao adotá-los.

Seção 1 – Conteúdo Mínimo dos Códigos

A adoção de códigos de boas práticas representa um avanço essencial na construção de uma governança ética e preventiva para a IA no Brasil. Além de garantir alinhamento com os princípios legais, esses instrumentos posicionam as organizações como líderes em inovação responsável.

De acordo com o artigo 30 do PL 2.338/2023, os códigos de boas práticas e governança podem ser elaborados por agentes de IA, individualmente ou por meio de associações. Eles devem conter elementos como:

- Regras de organização e funcionamento dos sistemas de IA;
- Normas de segurança, padrões técnicos e procedimentos internos;
- Tratamento de reclamações e mecanismos de mitigação de riscos;
- Ações educativas e medidas de supervisão, técnicas e organizacionais;
- Planos de resposta para resultados prejudiciais e mecanismos de atualização constante.

Importante: Esses códigos devem estar ajustados à escala, ao volume de operações e ao potencial de risco da tecnologia desenvolvida ou utilizada.

Seção 2 – Integração com Políticas Internas e Governança

O código de boas práticas não deve ser um documento isolado. Ele deve integrar a estrutura geral de governança da organização, servindo como um desdobramento prático da política de IA, conforme previsto no Capítulo IV do PL.

Exemplo prático:

Se a política institucional determina o compromisso com a não discriminação, o código operacionaliza isso por meio de auditorias regulares de viés algorítmico e canais internos para denúncias.

Vantagem: A existência de um código articulado com a política geral de IA ajuda a demonstrar boa-fé e pode atenuar sanções em caso de incidentes, conforme o art. 36, §1º, inciso IX do PL.

Seção 3 – Reconhecimento e Incentivos

A autoridade competente poderá aprovar, publicizar e incentivar a adesão a esses códigos, que serão considerados:

- Critério de boa-fé, influenciando positivamente na aplicação de sanções;
- Evidência de conformidade, especialmente em fiscalizações;
- Instrumento de supervisão preventiva, facilitando a autorregulação setorial.

Dica: Incluir mecanismos de participação pública e feedback contínuo no código fortalece a transparência e a confiança.

Conexão com a ISO/IEC 42001

Este capítulo conecta-se fortemente com os seguintes controles da ISO/IEC 42001:

- A.2 – Política de IA: Apoia a formulação de princípios organizacionais claros sobre a IA.
- A.3.2 – Funções e responsabilidades: Reforça que práticas éticas devem estar claramente atribuídas entre áreas e funções, com governança distribuída.



Capítulo 8 – Comunicação de Incidentes Graves

Introdução ao Capítulo

Quando um sistema de IA apresenta falhas graves ou viola direitos fundamentais, é essencial agir com rapidez e transparência. Este capítulo aborda como os agentes de inteligência artificial devem relatar incidentes à autoridade competente, garantir ações corretivas e proteger os afetados.

Você aprenderá:

- Quais tipos de incidentes devem ser comunicados;
- Como e em quanto tempo essa comunicação deve ocorrer;
- Qual o papel da autoridade pública e das organizações envolvidas.

A comunicação rápida e transparente de incidentes graves é um dos pilares para garantir a confiança pública no uso da Inteligência Artificial. O

Projeto de Lei 2338/2023 deixa claro que não basta desenvolver tecnologias inovadoras – é preciso estar preparado para responder aos riscos que elas trazem.

Ter processos claros de notificação, manter registros atualizados e agir de forma imediata diante de falhas não é apenas uma obrigação legal, mas um compromisso ético com a sociedade. Além disso, alinhar essas práticas aos padrões da ISO/IEC 42001 fortalece a governança e demonstra maturidade institucional.

Em um cenário de transformação digital acelerada, quem se antecipa na gestão responsável da IA se posiciona não só como líder em inovação, mas também como referência em integridade e segurança.

Seção 1 – Quando comunicar e a quem

De acordo com o Art. 31 do PL 2338/2023, os agentes de inteligência artificial são obrigados a comunicar imediatamente à autoridade competente qualquer incidente grave que envolva:

- Risco à vida ou à integridade física das pessoas;
- Interrupção de funcionamento de operações críticas de infraestrutura;
- Danos graves à propriedade ou ao meio ambiente;
- Graves violações de direitos fundamentais.

Isso significa que empresas, órgãos públicos ou qualquer operador de IA devem ter protocolos prontos para identificar e relatar rapidamente qualquer falha com impacto significativo.

Seção 2 – Prazo e formas de resposta

O projeto determina que a comunicação deve ser feita em prazo razoável, a ser regulamentado. A autoridade competente, após receber o relato, pode:

- Solicitar informações complementares;
- Exigir ações corretivas imediatas;
- Determinar a suspensão ou limitação do uso do sistema envolvido;
- Monitorar a execução das medidas de mitigação.

Exemplo prático: uma IA usada em hospitais para triagem de pacientes apresenta falha que prioriza mal os casos. A empresa fornecedora deve comunicar o incidente às autoridades e interromper temporariamente o sistema até garantir sua confiabilidade.

Seção 3 – Obrigações das empresas e poder público

Organizações públicas e privadas devem manter um sistema interno de monitoramento e resposta a incidentes, com:

- Registro de logs do sistema (Art. 20, II);
- Planos de contingência;
- Equipe capacitada para resposta rápida;
- Procedimentos de reporte ao público e às autoridades, conforme exigido.

A transparência com os afetados também é incentivada, especialmente nos casos com alto impacto.

Conexão com a ISO/IEC 42001

- A.6.4 – Registro de logs: exige registros automáticos e rastreáveis para facilitar a identificação de falhas e responsabilidades.
- A.9.3 – Resposta a incidentes: estabelece que organizações devem ter processos definidos para tratar e relatar incidentes relacionados à IA, com comunicação estruturada e ações de mitigação.



Capítulo 9 – Fiscalização e Supervisão

Introdução ao Capítulo

Neste capítulo, você vai entender como o governo brasileiro supervisionará o uso da Inteligência Artificial (IA), quem será a autoridade responsável, e quais são os mecanismos previstos para garantir que empresas e órgãos públicos cumpram as regras estabelecidas na lei.

A criação de uma autoridade nacional é essencial para aplicar as normas, fiscalizar o uso da IA e garantir que os direitos das pessoas sejam protegidos. Além disso, será possível aplicar sanções em caso de descumprimento.

Seção 1 – Autoridade Competente

O Projeto de Lei define que o Poder Executivo será responsável por designar uma autoridade competente para implementar e fiscalizar a Lei da IA.

Essa autoridade terá, entre suas funções:

A criação de uma autoridade nacional para fiscalizar a Inteligência Artificial no Brasil é um passo decisivo para garantir que a tecnologia seja usada de forma segura, ética e conforme os direitos fundamentais. Ao estabelecer mecanismos claros de supervisão, aplicação de sanções e cooperação com outros órgãos reguladores, o PL 2338/2023 busca não apenas prevenir abusos, mas também promover a confiança e a transparência no ecossistema de IA.

A atuação coordenada entre entes públicos, empresas e sociedade civil será fundamental para garantir a efetividade da norma. Mais do que punir, a fiscalização deverá educar, orientar e construir uma cultura de responsabilidade digital. Afinal, uma IA confiável não depende apenas da tecnologia, mas da vigilância constante sobre o seu uso.

- Zelar pela proteção dos direitos fundamentais afetados pelo uso da IA;
- Elaborar e implementar a Estratégia Brasileira de Inteligência Artificial;
- Promover boas práticas e códigos de conduta;
- Fiscalizar o cumprimento da lei e aplicar sanções quando necessário;
- Estabelecer regulamentações específicas, como:
 - Como devem ser feitas as avaliações de impacto algorítmico;
 - Quais informações devem ser públicas sobre os sistemas de IA;
 - Como certificar sistemas de alto risco.

Além disso, poderá atuar em cooperação com outras agências reguladoras, como Anatel, Anvisa ou Bacen, nos respectivos setores.

Seção 2 – Fiscalização e Aplicação de Sanções

A autoridade competente poderá fiscalizar diretamente ou junto a outros órgãos, além de:

- Solicitar relatórios e documentação sobre qualquer sistema de IA em operação;
- Aplicar sanções administrativas que variam de advertências a multas de até R\$ 50 milhões, ou 2% do faturamento da empresa, em casos mais graves;
- Suspender temporariamente ou definitivamente o uso de sistemas que descumprem a lei;
- Impedir o uso de bancos de dados sensíveis;
- Aplicar penalidades específicas para uso de sistemas de risco excessivo, como a suspensão imediata.

Importante: Empresas que adotarem práticas éticas, realizarem avaliações de impacto e tiverem governança responsável poderão ter penalidades reduzidas, conforme avaliação da autoridade.

Seção 3 – Cooperação com Outras Agências

A autoridade deverá manter um fórum de cooperação com órgãos reguladores dos setores econômicos e governamentais, para assegurar:

- Alinhamento das regulamentações;
- Fiscalização coordenada;
- Participação nos ambientes de testes regulatórios (sandbox), quando aplicável.

Isso evita conflitos regulatórios e aumenta a segurança jurídica, além de estimular a inovação responsável.

Conexão com ISO/IEC 42001:

- 4.2 – Liderança e comprometimento: reforça a necessidade de envolvimento de alto nível nas ações de supervisão e conformidade.
- 9.2 – Auditoria interna: promove avaliações periódicas e estruturadas para verificar se os sistemas estão em conformidade com os requisitos legais e éticos.



Capítulo 10 – Penalidades e Sanções

Introdução ao Capítulo

Quando organizações descumprem as regras da futura Lei Brasileira de Inteligência Artificial (PL 2338/2023), elas estão sujeitas a penalidades rigorosas. Este capítulo explica quais são essas sanções, como são aplicadas e o que pode ser feito para atenuá-las.

Você vai entender:

- Quais são as sanções previstas;
- Como funciona a aplicação das penalidades;
- O papel da conformidade e da boa-fé;
- Conexões com práticas internacionais e com a norma ISO 42001.

Seção 1 – Multas e Suspensão de Atividades

O Projeto de Lei prevê seis sanções administrativas principais:

1. Advertência
2. Multa (até R\$ 50 milhões por infração ou até 2% do faturamento anual da empresa no Brasil)
3. Publicização da infração
4. Proibição de participar de sandboxes regulatórios
5. Suspensão parcial ou total da operação do sistema
6. Proibição de tratar determinadas bases de dados

Essas sanções são aplicadas gradualmente, considerando a gravidade da infração.

Exemplo prático: Uma empresa usa IA de alto risco sem realizar a avaliação de impacto. Caso cause danos, pode ser multada, suspensa ou impedida de continuar operando com aquele sistema.

Seção 2 – Critérios para Dosimetria da Penalidade

A dosimetria – isto é, o cálculo da penalidade – leva em conta critérios como:

- Gravidade da infração e violação de direitos
- Boa-fé e cooperação da empresa
- Vantagens obtidas com a infração
- Existência de políticas de governança e códigos de ética
- Reincidente
- Rapidez na correção dos problemas
- Condição econômica do infrator

Quanto maior o grau de dano ou negligéncia, maior a penalidade.

Seção 3 – Reincidente e Agravantes

Empresas reincidentes ou que ignoram obrigações essenciais (como avaliação de impacto, governança de dados, transparéncia) estão mais sujeitas às sanções mais severas.

No caso de sistemas de risco excessivo, a multa é obrigatória, e pode haver suspensão definitiva da operação do sistema.

A ausência de medidas preventivas, como a não adoção da ISO 42001 ou de códigos de boas práticas, é considerada agravante.

Conexão com a ISO/IEC 42001

A ISO 42001 oferece diretrizes que ajudam as organizações a evitar sanções, incluindo:

- A.5.1 – Conformidade: exige estrutura de controle interno para acompanhar as obrigações legais e técnicas;
- A.10.1 – Melhoria contínua: obriga as organizações a revisar regularmente seus processos, corrigir falhas e atualizar medidas de segurança e ética.



IA NO BRASIL - Entendendo o PL 2338/2023 na Prática

Capítulo 11 – Inovação e Sandboxes Regulatórios

Introdução ao Capítulo

A Lei Brasileira de Inteligência Artificial (PL 2338/2023) não se limita a regular e fiscalizar o uso de IA. Ela também reconhece a importância de fomentar a inovação de forma segura e ética. Este capítulo apresenta os mecanismos previstos para permitir que startups, PMEs e outras organizações testem soluções inovadoras em ambientes regulatórios flexíveis – os chamados sandboxes regulatórios.

Você vai entender:

- Como funcionam os sandboxes regulatórios no Brasil;
- Quais são os critérios e proteções exigidas;
- Como essa abordagem favorece a inovação responsável e alinhada com os direitos fundamentais.

Seção 1 – Requisitos para Participar de Sandbox

A autoridade competente pode autorizar ambientes regulatórios experimentais para projetos de IA inovadores. Para isso, a empresa ou instituição interessada deve apresentar um plano claro que demonstre:

- Inovação no uso ou no modelo de aplicação da tecnologia de IA;
- Ganhos potenciais em eficiência, segurança, custo ou impacto social;
- Um plano de descontinuidade (o que será feito ao final do experimento).

O sandbox regulatório não é um “vale tudo” para experimentações descontroladas. Ele é um espaço com regras claras para testar inovações que podem transformar o país – desde que com responsabilidade, supervisão e foco na proteção dos direitos fundamentais.

Essa medida mostra que o Brasil está pronto para equilibrar segurança jurídica e incentivo à criatividade no setor de inteligência artificial

Essa autorização não é automática: é preciso submeter um projeto à autoridade, que avaliará se os requisitos estão atendidos.

Exemplo prático: uma startup de educação quer testar um sistema de tutoria por IA para alunos do ensino público. Para isso, solicita a entrada no sandbox com um projeto detalhado, garantindo proteção de dados e transparéncia.

Seção 2 – Proteções Mínimas Exigidas

Mesmo em caráter experimental, os participantes do sandbox continuam responsáveis por possíveis danos causados. Isso significa que:

- Devem garantir o respeito aos direitos fundamentais (ex.: não discriminação, privacidade, segurança);
- O ambiente de teste não pode comprometer a integridade de consumidores ou cidadãos;
- As autoridades podem interromper ou limitar o projeto se identificarem riscos elevados.

Além disso, a regulamentação exige que dados utilizados no sandbox respeitem a Lei Geral de Proteção de Dados (LGPD), e que as experiências sejam conduzidas com total transparéncia.

O PL reforça que inovação não pode ser desculpa para colocar vidas ou direitos em risco.

Seção 3 – Incentivo a Startups e PMEs

O projeto de lei reconhece que as pequenas empresas, startups e projetos acadêmicos são importantes motores de inovação no Brasil. Por isso:

- A adesão a sandboxes pode ser facilitada para PMEs;
- Pode haver procedimentos simplificados de registro e acompanhamento;
- A autoridade poderá emitir recomendações específicas para que tais projetos aproveitem o ambiente regulatório com segurança.

 Ao estimular a inovação com segurança, o PL 2338/2023 cria um equilíbrio entre proteção social e liberdade tecnológica.

Conexão com ISO/IEC 42001

A abordagem dos sandboxes regulatórios dialoga diretamente com os seguintes controles da norma ISO/IEC 42001:

- A.6.3 – Testes e validação: estabelece a importância de validar sistemas de IA em ambientes controlados antes da adoção plena;
- A.7.3 – Transparéncia: reforça que mesmo os testes devem ser claros, documentados e acessíveis para partes interessadas.



Chegamos ao final desta jornada de aprendizado sobre o novo marco regulatório da Inteligência Artificial no Brasil. Ao longo dos capítulos, exploramos como o Projeto de Lei 2338/2023 estabelece uma base sólida para que a IA seja desenvolvida e utilizada com ética, segurança, transparência e foco no ser humano.

Mais do que impõe limites, essa legislação aponta caminhos: ela incentiva a inovação, protege os direitos fundamentais e fortalece a confiança da sociedade no uso de tecnologias que estão transformando todos os setores – da saúde à educação, da segurança pública ao comércio digital.

Vimos que a classificação de riscos, a avaliação de impactos, a governança organizacional, a transparência algorítmica e a responsabilidade civil não são apenas obrigações legais, mas também práticas recomendadas pela norma ISO/IEC 42001, que serve como referência técnica global para sistemas de gestão de IA.

Além disso, aprendemos que boas práticas voluntárias, como a criação de códigos de ética, uso de sandboxes regulatórios e capacitação contínua de equipes, são ferramentas essenciais para garantir a adaptação sustentável a esse novo cenário regulatório.

A IA é um instrumento poderoso – capaz de ampliar capacidades humanas e gerar valor social, econômico e ambiental. Mas, para isso, precisa estar sob controle ético, jurídico e técnico. O futuro da IA no Brasil será construído com base na confiança, e essa confiança nasce da governança inteligente.

Este livro é um convite à ação: que cada profissional, gestor público, empreendedor, desenvolvedor e cidadão participe ativamente da construção de um ecossistema de IA seguro, responsável e centrado em valores humanos.

O desafio é grande. Mas o potencial é ainda maior.

Vamos liderar esta transformação juntos.



Conclusão do Autor – Paulo S.O. Carvalho

O avanço da Inteligência Artificial representa mais do que uma transformação tecnológica – ele impõe um novo paradigma para a humanidade. Governar algoritmos passou a ser uma necessidade ética, política e social. O Manual do Auditor de IA foi elaborado com o objetivo de apoiar líderes públicos e privados, auditores, gestores e desenvolvedores na construção de um Sistema de Governança de IA ético, auditável e confiável, alinhado às normas internacionais (ISO/IEC 42001), ao AI Act Europeu e ao PL 2338/2023 no Brasil .

A governança de IA é, ao mesmo tempo, uma nova ciência e uma nova consciência. É um campo emergente que exige metodologias práticas e princípios sólidos. Neste manual, propõe-se um caminho claro: desde a definição do escopo de IA e avaliação de riscos, até a implementação de um Sistema de Gestão de IA com diretrizes específicas sobre explicabilidade, supervisão humana significativa e avaliação de impacto algorítmico.

Ao encerrar este guia, reforçamos o compromisso com uma IA que respeite os direitos fundamentais, promova a justiça distributiva e mantenha o humano no centro das decisões. Convidamos todos os profissionais da era digital a assumirem sua responsabilidade neste novo pacto social.

Este é apenas o começo. A missão de auditar inteligências exige coragem, conhecimento e visão.

Considerações Finais

A inteligência artificial está moldando a próxima geração de serviços, produtos e políticas. Mas só haverá futuro com responsabilidade algorítmica. As instituições que se comprometerem com práticas transparentes, auditáveis e sustentáveis estarão liderando um movimento de confiança tecnológica.

Este manual é uma contribuição concreta da ALGOR Association para consolidar o Brasil entre os países líderes na implementação responsável da inteligência artificial, respeitando os princípios de ética, inclusão, explicabilidade e segurança.
Contato do Autor

E-mail:
paulocarvalho9311@gmail.com

🌐 Instituição:

XPER BRASIL GESTÃO EM INOVAÇÃO TECNOLÓGICA LTDA
Av. Desembargador Moreira, 1300, Sala 16A – Aldeota, Fortaleza – CE, 60170-002
CNPJ: 33.173.492/0001-76
Site: www.xper.social
E-mail institucional: ai@xper.social
Representante: www.algor.uk





Association for Algorithmization and
Logic Governance Organization

WWW.ALGOR.UK

PROGRAMA CERTIFICAÇÃO

A U D I T O R D E I A

