

CERTIFICAÇÃO · INTELIGÊNCIA ARTIFICIAL

ISO/IEC 42001: sistema de gestão para IA

Quem fornece funcionalidades de IA a clientes da UE recebe perguntas sobre dados, riscos e controle. A ISO/IEC 42001 é a primeira norma internacional que permite dar a essas perguntas uma resposta organizada.

VERSÃO ATUAL	OBJETO	VALIDADE	RELAÇÃO
ISO/IEC 42001:2023	sistema de gestão de inteligência artificial (AIMS)	3 anos, com auditorias de manutenção anuais	Regulamento de IA (UE) 2024/1689

Em resumo

A ISO/IEC 42001 define requisitos para um sistema de gestão de inteligência artificial, conhecido pela sigla em inglês AIMS. A norma foi publicada no fim de 2023. Ela se dirige a organizações que desenvolvem, oferecem ou utilizam sistemas de IA e segue a mesma estrutura básica da ISO/IEC 27001 e da ISO 9001. Quem conhece uma dessas normas se orienta rapidamente.

No centro estão as perguntas que clientes da UE fazem a fornecedores de IA: quais sistemas de IA vocês operam, para quê e com quais dados? Que riscos surgem para as pessoas afetadas, e quem decide sobre eles? Como vocês monitoram os modelos em operação, e o que acontece quando eles erram? A norma exige uma avaliação de impacto dos sistemas de IA, um tratamento de riscos e controles listados em um anexo, de forma parecida com a ISO/IEC 27001.

A norma é neutra em relação à tecnologia. Ela vale tanto para um modelo próprio de previsão de safra quanto para um chatbot de atendimento construído sobre um modelo de linguagem contratado de terceiros. O segundo caso é muito comum na América do Sul: muitos fornecedores não desenvolvem modelos de base próprios e constroem produtos sobre modelos de grandes provedores. A ISO/IEC 42001 exige, nesse caso, que você também gerencie esses fornecedores, conheça os limites deles e documente como lida com erros do modelo.

Por que clientes da UE pedem a norma

O [Regulamento de IA](#) da UE também se aplica a fornecedores de fora da UE quando eles colocam sistemas de IA no mercado da UE ou quando o resultado produzido por um sistema é utilizado na UE (art. 2.º). Uma software house de Buenos Aires que desenvolve para uma seguradora espanhola um modelo de análise de sinistros, portanto, é atingida com facilidade. As obrigações entram em vigor de forma escalonada; as proibições valem desde fevereiro de 2025, e as regras para modelos de IA de

finalidade geral desde agosto de 2025. Os demais prazos e a situação atual de cada um estão na nossa página sobre o Regulamento de IA.

Pelo regulamento, fornecedores de IA de risco elevado precisam, entre outras coisas, de um sistema de gestão da qualidade, gestão de riscos, documentação técnica e supervisão humana. A ISO/IEC 42001 cobre muitos desses temas no nível da organização. Um certificado, porém, não significa que um sistema de IA cumpre o Regulamento de IA. Quais normas geram presunção de conformidade é definido pelas normas harmonizadas publicadas no Jornal Oficial da UE. Para os seus clientes na UE, o certificado ainda assim é um sinal forte de que você gerencia a IA de forma organizada.

As regras já conhecidas continuam valendo. Se houver tratamento de dados pessoais, por exemplo para treinamento, aplica-se o [RGPD \(Regulamento Geral sobre a Proteção de Dados\)](#). Se o sistema de IA rodar em um banco ou seguradora, o [DORA](#) entra em cena por meio do seu cliente.

Quem precisa na América do Sul

- Startups de IA e software houses em São Paulo, Santiago, Bogotá, Medellín, Buenos Aires ou Montevideu que vendem produtos de IA a clientes da UE
- Prestadores de serviços de data science e analytics que treinam ou operam modelos para contratantes europeus
- BPO e contact centers que usam chatbots ou decisões automatizadas para clientes da UE
- Fintechs com score de crédito, prevenção de fraudes ou verificação de identidade
- Empresas de agritech com análise de imagens ou de satélite, por exemplo para rastreabilidade conforme a [EUDR](#)
- Empresas de recursos humanos que usam IA na seleção ou avaliação de candidatos

Etapas até a certificação

1. Montar um inventário de todos os sistemas de IA: finalidade, fontes de dados, modelos, terceiros integrados e o seu papel (desenvolvedor, fornecedor, usuário).
2. Definir o escopo do AIMS e aprovar diretrizes de IA.
3. Avaliar riscos e impactos para as pessoas afetadas e para a sociedade, escolher controles e justificá-los.
4. Implantar processos para qualidade de dados, desenvolvimento, testes, liberação, monitoramento em operação e incidentes.
5. Operar o sistema por alguns meses e realizar auditoria interna e análise crítica pela direção.
6. Auditoria de estágio 1 e de estágio 2 por um organismo certificador acreditado.

7. Certificado válido por três anos, com auditorias de manutenção anuais.

O prazo típico é de 6 a 12 meses. Quem já opera um SGSI conforme a ISO/IEC 27001 pode aproveitar controle de documentos, auditorias e gestão de fornecedores e muitas vezes chega lá mais rápido. Os custos dependem da quantidade e do tipo de sistemas de IA e variam bastante. Comece pelos sistemas que afetam clientes da UE e amplie o escopo depois, quando o sistema estiver funcionando no dia a dia.

Acreditação: qual organismo vale

O organismo certificador deve ser acreditado expressamente para a ISO/IEC 42001, por um organismo de acreditação signatário do acordo internacional de reconhecimento. Até o fim de 2025, esse acordo era o IAF MLA; desde 01/01/2026, é o MRA da Global Accreditation Cooperation Incorporated (Global ACI). Com uma norma tão recente, vale a pena olhar com atenção o certificado de acreditação: nem todo organismo que certifica a ISO/IEC 27001 também é acreditado para a ISO/IEC 42001.

PAÍS	ORGANISMO DE ACREDITAÇÃO
Argentina	OAA, Organismo Argentino de Acreditación
Bolívia	DTA-IBMETRO, Dirección Técnica de Acreditación do Instituto Boliviano de Metrología
Brasil	Cgcre (Coordenação-Geral de Acreditação) do INMETRO
Chile	INN, Instituto Nacional de Normalización
Colômbia	ONAC, Organismo Nacional de Acreditación de Colombia
Equador	SAE, Servicio de Acreditación Ecuatoriano
Paraguai	ONA, Organismo Nacional de Acreditación (vinculado ao CONACYT)
Peru	INACAL, Dirección de Acreditación
Uruguai	OUA, Organismo Uruguayo de Acreditación

Os nove organismos constam como signatários na Global ACI (situação em 11/10/2026). Se algum deles já acreditou organismos certificadores para a ISO/IEC 42001, isso precisa ser verificado caso a caso. Um organismo certificador acreditado em outro país signatário é reconhecido da mesma forma.

Erros comuns

- O inventário de IA está incompleto. Faltam modelos de linguagem de terceiros integrados ou a IA embutida em ferramentas contratadas.
- O certificado é vendido como prova de conformidade com o Regulamento de IA. Clientes da UE com departamento jurídico próprio percebem isso.
- A avaliação de impacto considera apenas riscos técnicos, e não os efeitos sobre as pessoas a respeito das quais o sistema decide.
- Falta monitoramento em operação: os modelos são liberados e depois não são mais verificados.
- A gestão de IA corre separada da proteção de dados e da segurança da informação, embora os mesmos dados e sistemas estejam envolvidos.
- Os contratos com os provedores de modelos não são analisados. É neles que consta se os dados do cliente podem ser reutilizados para treinamento, e é exatamente isso que o seu cliente na UE pergunta.
- A responsabilidade não está definida. Se ninguém tem autoridade para parar um sistema de IA que entrega resultados errados, qualquer auditor verá isso como uma lacuna.

Como o Sightadel ajuda

O [Sightadel](#) reúne inventário de IA, riscos, avaliações de impacto, controles e evidências em um só lugar e os conecta à ISO/IEC 27001 e à proteção de dados, quando já existirem. Com um pacote de consultoria, consultores experientes acompanham você até a certificação.

FAQ

Com a ISO/IEC 42001 cumprimos o Regulamento de IA?

Não automaticamente. A norma cobre muitos requisitos organizacionais. Obrigações relativas a cada sistema de IA, como documentação técnica ou identificação, continuam sendo tarefas à parte.

O Regulamento de IA se aplica a nós mesmo estando fora da UE?

Sim, se vocês oferecem sistemas de IA na UE ou se o resultado produzido pelo seu sistema é utilizado na UE. Os detalhes estão na nossa página sobre o Regulamento de IA.

Precisamos primeiro da ISO/IEC 27001?

Não, as normas podem ser certificadas de forma independente uma da outra. Mas um SGSI já implantado facilita bastante a ISO/IEC 42001, porque a estrutura e muitos processos são os mesmos.

Qual ferramenta ajuda a montar o AIMS?

Uma plataforma GRC que suporte a ISO/IEC 42001. O **Sightadel** suporta a norma e também o Regulamento de IA da UE, é desenvolvido e hospedado na Alemanha, e os dados ficam na UE. Quem já usa o Sightadel para a ISO/IEC 27001 reaproveita ali o que já elaborou.

Fontes · Atualizado em: 11 de outubro de 2026

ISO: ISO/IEC 42001:2023: <https://www.iso.org/standard/42001>

Regulamento (UE) 2024/1689 (Regulamento da Inteligência Artificial): <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

Regulamento (UE) 2016/679 (RGPD): <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

Global ACI: organismos de acreditação reconhecidos: <https://global-aci.org/en/recognised-abs/>

Informações gerais, sem caráter de consultoria jurídica. Valem os textos oficiais.

COLOQUE EM PRÁTICA COM FERRAMENTAS FEITAS NA ALEMANHA



Sightadel

O Sightadel conduz sua equipe por a ISO 42001: modelos, tarefas, evidências e preparação para auditoria em um só lugar. Desenvolvido e hospedado na Alemanha, com pacote de consultoria opcional.

[Conhecer o Sightadel →](#)

Sightadel, veyrisk e Valar são produtos da neonotu GmbH, empresa que opera o MercoEU.

O que disso se aplica à sua empresa?

O Diagnóstico UE gratuito mostra isso por setor e país em 10 minutos.

<https://www.mercoeu.com/pt/diagnostico-ue>