REDE ANBIMA DE INOVAÇÃO

GUIA ORIENTATIVO

BOAS PRÁTICAS PARA A CONTRATAÇÃO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

ANBIMA

Sumário

_INTRODUÇÃO <<

A inteligência artificial (IA) vem ganhando cada vez mais espaço como uma aliada estratégica para inovação e eficiência no mercado financeiro e de capitais.

Mas a escolha e a implementação desses sistemas ainda trazem desafios importantes, especialmente em um ambiente regulado e baseado na confiança, como o das instituições que fazem parte da ANBIMA.

É essencial avaliar de forma crítica a capacidade, a segurança e a conformidade dessas soluções, separando o que já está testado e comprovado das promessas ainda vagas de mercado. Também é preciso entender os riscos envolvidos, como possíveis vieses nos algoritmos e questões de segurança de dados.

Este guia tem o objetivo de oferecer um material prático e direto para apoiar instituições do mercado de capitais na contratação de sistemas de IA, ajudando na gestão dos riscos e no cumprimento das regras legais e regulatórias.

Aqui, você vai encontrar orientações que vão desde o mapeamento das necessidades do negócio e a definição de critérios técnicos, éticos e de conformidade, até boas práticas para avaliação de fornecedores, due diligence tecnológica e contratual e acompanhamento após a implementação.

Nosso objetivo é garantir que a adoção da IA seja feita de forma estratégica, segura, responsável e alinhada com as exigências do setor.

_DEFINIÇÕES DE TERMOS IMPORTANTES<<

Ao longo deste guia, usamos alguns termos que precisam estar bem claros para facilitar a leitura e o entendimento do conteúdo. São eles:

Sistema de IA: é qualquer sistema que gera resultados como conteúdos, previsões, recomendações ou decisões com base em objetivos definidos por pessoas. Pode funcionar com diferentes níveis de autonomia e está presente em sites, plataformas, aplicativos, ferramentas e funcionalidades que usam IA — tanto gratuitos quanto pagos, de uso individual ou corporativo.

Governança de IA: é o conjunto de papéis, responsabilidades e processos formais pela qual a empresa é dirigida, supervisionada e responsabilizada com o objetivo de alcançar, garantir e assegurar o uso ético e responsável de IA.

Agentes de IA: são todas as pessoas ou empresas, públicas ou privadas, que têm um papel ativo ao longo do ciclo de vida de um sistema de IA. Eles se dividem em três tipos:

- **Desenvolvedor:** é quem cria o sistema de IA, seja por conta própria ou a pedido de outra empresa. Pode lançar o sistema com sua própria marca ou com a marca de quem encomendou.

  >>> É o caso de grandes empresas como OpenAI, Google ou Microsoft, que oferecem soluções prontas. Mas, se sua instituição desenvolver internamente um sistema ou contratar uma empresa para isso, também estará atuando como desenvolvedora.

- **Distribuidor:** é quem disponibiliza o sistema no mercado, normalmente vendendo licenças, mas sem participar do desenvolvimento.

  >>> Isso costuma acontecer com empresas especializadas na revenda de softwares de IA.

- **Aplicador:** é quem contrata e usa o sistema de IA para suas próprias finalidades. Também pode ser responsável por configurar a ferramenta, fornecer dados para sua operação e acompanhar seu funcionamento.

  >>> Esse é o papel que sua instituição provavelmente vai desempenhar ao adotar uma solução de IA.

NÃO CONFUNDIR OS AGENTES!

Os **agentes de IA** são conceitos da regulação brasileira. Eles não devem ser confundidos com outro tipo de tecnologia chamado agentic AI (ou IA agêntica), que é um sistema de IA capaz de automatizar várias tarefas por meio de diferentes "agentes" internos.

POR QUE É IMPORTANTE ENTENDER OS AGENTES?

A regulação define deveres específicos para cada agente envolvido com sistemas de IA. No caso das instituições financeiras, o papel mais comum será o de aplicadora, o que traz uma série de responsabilidades, como:

- Avaliar os riscos do sistema de IA contratado;
- Garantir transparência às pessoas cujos dados forem tratados pelo sistema;
- Responder por eventuais danos causados pelo uso da IA;
- Customizar ou solicitar adaptações no sistema de forma responsável;
- Seguir as exigências regulatórias na contratação de terceiros, como gestão de riscos, segurança cibernética e cláusulas contratuais que garantam supervisão e possibilidade de substituição do fornecedor, conforme as normas aplicáveis.

Definição conforme a ISO/IEC 22989:2022 – item 3.1.4
Definição conforme a ISO 37000:2021
Definição conforme o Projeto de Lei nº 2.338/2023, na versão aprovada pelo Senado

_1: Avaliando a maturidade em IA do fornecedor<<

Com o crescimento da oferta de sistemas de inteligência artificial, pode ser difícil escolher entre as muitas opções disponíveis no mercado. Por isso, é importante dar preferência a desenvolvedores e distribuidores que tenham alto grau de maturidade em IA.

O que é maturidade em IA?

Ela não diz respeito apenas à capacidade técnica do fornecedor. O termo se refere ao nível de governança que ele adota e à sua capacidade de cumprir as normas que regulam o uso da inteligência artificial, além de apoiar seus clientes, como a sua instituição, a também atender às exigências regulatórias.

Se o fornecedor já tem uma governança robusta de IA, sua instituição já estará um passo à frente no caminho da adoção segura e responsável dessas tecnologias.

DENTRO DE CASA: ENTENDENDO AS NECESSIDADES INTERNAS

Antes de sair em busca de soluções de IA no mercado, é fundamental que a instituição analise seu próprio contexto. Entender quais são suas necessidades, o que se espera da tecnologia e como ela se encaixa na estrutura atual é o primeiro passo para uma contratação eficiente.

Quais são os objetivos que queremos alcançar e as dores que queremos sanar?

Essas metas precisam ser tratadas com o mesmo peso que qualquer outro objetivo estratégico da instituição. Isso é o que vai orientar o projeto e permitir avaliar se a adoção da IA foi bem-sucedida. Por isso, é importante definir com clareza quais dores internas precisam ser resolvidas, quais resultados se espera alcançar e como esse progresso será medido, ou seja, quais são os indicadores (KPIs) relevantes.

Em vez de uma meta genérica como "melhorar o atendimento ao cliente", por exemplo, a instituição pode estabelecer algo mais específico, como "reduzir o tempo médio de espera no atendimento em 20% nos próximos seis meses com o uso de um chatbot de IA".

Quais são os objetivos que queremos alcançar e as dores que queremos sanar?

Antes de seguir com a contratação, é essencial envolver a equipe de tecnologia para entender se a estrutura atual é compatível com a solução desejada e se os times que vão usar a ferramenta têm as habilidades necessárias para operá-la no dia a dia.

Imagine, por exemplo, que a instituição queira fazer um upgrade nos sistemas usados pelos colaboradores, mas os computadores sejam mais antigos. Antes de seguir com a atualização, é importante verificar se os aparelhos suportam as novas versões e se isso não vai afetar o desempenho das máquinas. Também é preciso garantir que as equipes saibam usar os novos recursos e que isso não traga impactos indesejados para os fluxos de trabalho já existentes.

Outro ponto importante é checar se há estrutura interna para criar, distribuir e gerenciar licenças de uso, sempre seguindo as regras de governança da instituição, os termos definidos pelo fornecedor e as exigências regulatórias, como controle de terceiros, segurança cibernética e continuidade operacional.

A instituição já tem um processo definido para aprovar a aquisição de novos sistemas de IA? Conta com os recursos necessários para garantir uma boa governança no uso dessa tecnologia?

É fácil se empolgar com as promessas da IA e esquecer das responsabilidades que acompanham sua contratação. Se já existe um fluxo interno para aprovação de fornecedores, é importante avaliar se ele contempla questões específicas relacionadas à IA, como o tratamento de dados pessoais, e se está atualizado conforme as exigências previstas na regulação vigente. Manter as normas internas em dia faz parte das boas práticas de governança e gestão de riscos, e é uma obrigação das instituições financeiras.

Se queremos gerenciar os nossos dados e informações interna com IA, como está a qualidade deles?

Quando os dados são inconsistentes ou incompletos, os resultados da IA também podem ser falhos. Por exemplo, se a instituição quer adotar um sistema de IA para detectar fraudes, é essencial que os dados das transações estejam corretos e atualizados. Caso contrário, a ferramenta pode não funcionar como esperado, e isso pode comprometer todo o projeto. Conhecer essas limitações desde o início ajuda a tomar decisões mais realistas e eficientes.

NO MERCADO: O QUE CONSIDERAR NA ESCOLHA DO FORNECEDOR

Depois de entender as necessidades internas, é hora de olhar para fora. Avaliar com atenção os fornecedores disponíveis no mercado é essencial para garantir que a solução escolhida esteja alinhada com os objetivos da instituição, atenda aos requisitos regulatórios e traga segurança, transparência e responsabilidade no uso da IA.

As informações sobre o funcionamento do sistema de IA são claras, inclusive em relação à forma como ele toma decisões?

Esse é um ponto cada vez mais relevante na hora de escolher um fornecedor. A instituição deve buscar entender, de forma objetiva e acessível, como o sistema funciona na prática.

É importante que o fornecedor consiga explicar quais critérios são usados nas decisões tomadas pelo sistema, especialmente nos casos em que essas decisões podem ser revistas. Também deve ficar claro que tipos de dados alimentam o sistema, com que frequência são atualizados e quem é responsável por essa atualização: o próprio fornecedor ou a instituição contratante. Outro ponto fundamental é saber se há riscos envolvidos no uso da solução e quais medidas de segurança foram adotadas para mitigá-los. Além disso, o fornecedor precisa oferecer formas de acompanhar e avaliar continuamente a integridade, a disponibilidade e a confiabilidade do sistema e dos dados tratados.

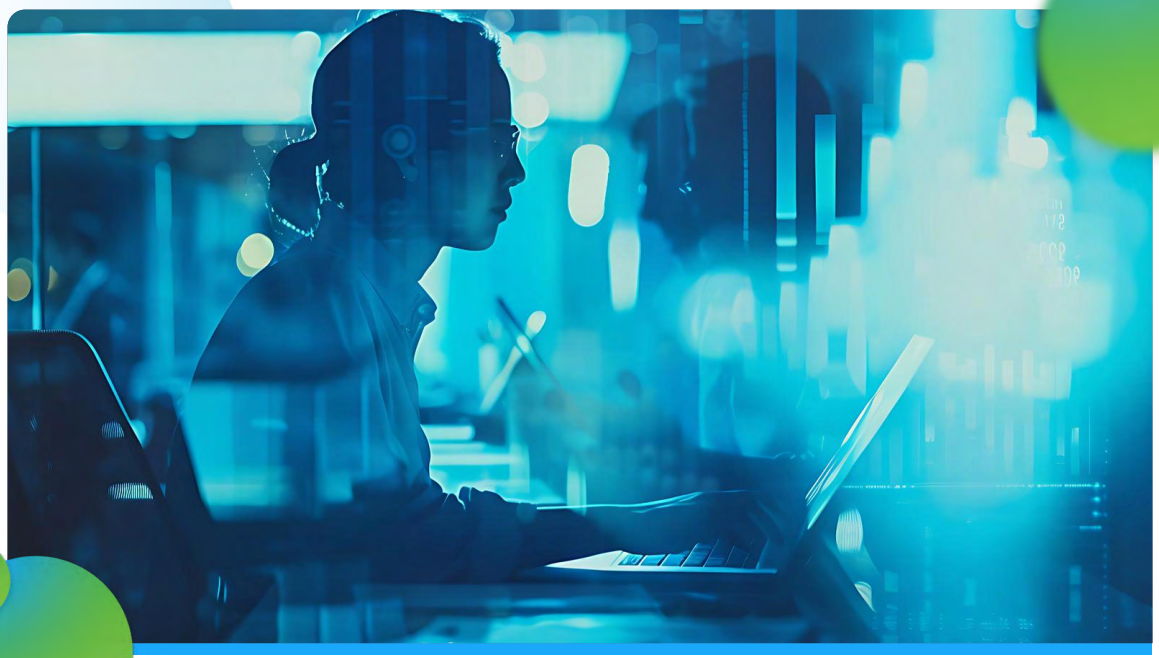
Esses elementos são essenciais para garantir uma contratação segura e alinhada com as obrigações regulatórias.

O fornecedor tem políticas claras de proteção de dados pessoais e de segurança da informação? E o que elas realmente dizem?

É importante ler com atenção a política de privacidade e questionar quais medidas são adotadas para proteger os dados, além de entender quais controles estão em vigor para garantir que essas medidas sejam proporcionais aos riscos da atividade contratada. Essas informações ajudam a avaliar o nível de conformidade do fornecedor e a entender se os dados da sua instituição e dos seus clientes estarão, de fato, bem protegidos. Por exemplo, se o serviço de IA for contratado em nuvem, vale verificar se há transferências internacionais de dados pessoais e se o fornecedor adota criptografia certificada para proteger os dados tanto em repouso quanto em trânsito.

Que tipo de suporte o fornecedor presta? Se a instituição precisar de apoio para cumprir obrigações legais, o fornecedor estará preparado para ajudar?

O suporte oferecido não deve se restringir apenas à parte técnica. O uso de IA envolve responsabilidades importantes por parte das instituições financeiras e, em muitos casos, o cumprimento dessas obrigações depende da cooperação do fornecedor. É importante verificar se há um canal claro para relatar erros ou problemas no sistema, se o fornecedor possui procedimentos para ajudar no atendimento de direitos dos usuários e se está preparado para colaborar em auditorias, fiscalizações ou investigações conduzidas por autoridades regulatórias. Também vale checar se existem boas práticas de governança contratual e gestão documental que garantam o acesso rápido e organizado a dados, registros e demais informações processadas pela solução contratada. Esse tipo de suporte é essencial para garantir segurança jurídica e operacional no uso da IA.



_2: Avaliando contratos e termos & condições<<

Depois de encontrar uma solução de IA que parece ideal para a sua instituição, qual é o próximo passo? Antes de assinar o contrato ou simplesmente clicar em "aceito os termos", é hora de parar e analisar com atenção os detalhes da contratação. Mesmo em contratos de adesão, os termos estabelecem responsabilidades, limites e riscos que podem afetar diretamente a operação da instituição e, no caso do setor financeiro, podem ter implicações regulatórias importantes.

ANTES DE ASSINAR: ENTENDENDO OS OBJETIVOS DA CONTRATAÇÃO

Toda contratação começa com clareza sobre **o problema que se quer resolver, o papel que a IA vai desempenhar e os riscos e responsabilidades envolvidos.** Essa definição é essencial para garantir uma contratação alinhada às necessidades da instituição e às exigências regulatórias.

Algumas perguntas ajudam a guiar essa análise:

- **Qual é a finalidade específica da IA?** Ela será usada, por exemplo, para análise de crédito, atendimento ao cliente ou prevenção à lavagem de dinheiro? É importante definir com clareza o que a ferramenta deve, e não deve, fazer.
- **A decisão será automatizada ou apenas apoiará quem toma as decisões?** Essa distinção impacta diretamente os controles necessários e os riscos envolvidos.
- **Quais dados serão usados pelo sistema?** A instituição deve identificar se os dados incluem informações pessoais, financeiras ou sensíveis.
- **Como funciona a ferramenta e qual será o seu grau de autonomia?** Trata-se de um sistema que aprende com o tempo (como os baseados em machine learning) ou de uma solução com regras fixas?
- **A IA vai interagir diretamente com clientes ou com áreas sujeitas à regulação?** Isso influencia o nível de risco e o cuidado necessário com supervisão e governança.
- **O fornecedor será considerado prestador de serviço relevante?** É preciso verificar se ele se enquadra dessa forma nas normas do Banco Central ou da CVM.
- **A metodologia usada para avaliar a contratação está em conformidade com as exigências regulatórias?** A instituição precisa garantir que todas as obrigações aplicáveis serão cumpridas.
- **O fornecedor está sediado no exterior?** Se sim, existe acordo de cooperação vigente entre o Banco Central do Brasil e a autoridade supervisora do país do fornecedor? A ausência desse acordo, conforme previsto na Resolução CMN nº 4.893/21, pode exigir diligências adicionais antes da contratação.

Quanto maior o impacto da IA no negócio, maior deve ser o rigor contratual e regulatório.

Nesta etapa, a instituição deve avaliar se a IA será usada **apenas para fins internos** ou se **fará parte, direta ou indiretamente, dos produtos e serviços oferecidos** ao mercado. Esse uso, especialmente quando envolve clientes ou operações reguladas, pode exigir o cumprimento de normas específicas do Banco Central (BACEN), da Comissão de Valores Mobiliários (CVM) e da Autoridade Nacional de Proteção de Dados (ANPD). Aplicações voltadas ao relacionamento com o cliente, em especial nos produtos financeiros, geralmente exigem maior rigor contratual e uma análise mais criteriosa dos termos.

Uma vez definidos os objetivos da contratação, é hora de verificar se o contrato dá conta dos **riscos** e **impactos** associados ao uso da IA. Quando a **tecnologia afeta atividades reguladas ou é considerada um serviço relevante, o contrato deve incluir salvaguardas compatíveis com o grau de criticidade e com as exigências da regulação aplicável.**

Sistemas de IA, especialmente no setor financeiro, raramente são ferramentas neutras. Eles podem:

- Tomar decisões que impactam diretamente os clientes, como negar crédito, bloquear transações ou incluir pessoas em listas restritivas;
- Apoiar áreas críticas que estão sob regulação, como prevenção à lavagem de dinheiro;
- Processar grandes volumes de dados sensíveis, incluindo informações bancárias, comportamentais e pessoais.

Por isso, o contrato deve tratar com clareza de alguns pontos essenciais:

1. **Responsabilidade pelo uso inadequado ou incorreto da IA.** É importante definir quem responde se a IA falhar, apresentar vieses ou gerar resultados imprecisos. Mesmo quando a decisão é sugerida pelo sistema, a instituição continua responsável perante clientes e reguladores. No entanto, é possível incluir cláusulas que distribuam as responsabilidades com o fornecedor.

2. **Medidas de segurança adotadas.** O sistema atende aos requisitos mínimos de cibersegurança previstos na Resolução CMN nº 4.893/21 e na Resolução CVM nº 35/21? O contrato deve deixar claro como a segurança da informação será garantida.

3. **Países onde os dados são processados e tratados:** Se houver transferência internacional de dados pessoais, o contrato precisa cumprir os requisitos da LGPD e, quando aplicável, das normas do BACEN e da CVM citadas acima. Isso inclui informar de forma expressa os países envolvidos e garantir que, independentemente da jurisdição, haja medidas adequadas de segurança e governança sobre os dados.

4. **Garantias contratuais mínimas exigidas pela regulação.** Quando o fornecedor é considerado prestador de serviço relevante, o contrato deve prever cláusulas específicas, como:

- Acesso irrestrito da instituição e dos reguladores aos dados, incluindo documentação técnica e registros de auditoria;
- Garantia de confidencialidade, integridade, disponibilidade e recuperação das informações tratadas;
- Possibilidade de rescisão contratual sem prejuízo à continuidade das operações, principalmente em caso de descumprimento ou descontinuidade do serviço;
- Planos de continuidade de negócios e estratégias de mitigação de riscos operacionais relacionados ao serviço contratado.

ATENÇÃO!

Contratos genéricos, especialmente os de plataformas internacionais, muitas vezes não consideram o ambiente regulado e de alta responsabilidade no qual atuam as instituições financeiras no Brasil. Por isso, é fundamental verificar se a empresa e o contrato estão preparados para atender às exigências de um setor altamente regulado e sujeito a riscos relevantes. Também vale avaliar se há possibilidade de firmar um documento complementar ao contrato principal, com cláusulas específicas que garantam o cumprimento dos requisitos previstos na regulamentação mencionada.

CUIDADO COM OS TERMOS “DE ADESÃO”

Em muitas contratações de IA, a formalização não se dá por meio de um contrato negociado entre as partes. É comum que o processo ocorra por meio de contratos de adesão, com termos e condições pré-definidos, geralmente em inglês e voltados a um público global. Embora esse modelo traga agilidade e facilite a escala, ele costuma conter cláusulas pouco ajustadas à realidade brasileira, especialmente para instituições financeiras que atuam em um ambiente regulado e precisam atender a salvaguardas específicas.

Mesmo grandes instituições financeiras podem enfrentar dificuldades para negociar cláusulas com fornecedores globais de tecnologia. No entanto, isso não afasta a responsabilidade da instituição perante o regulador e seus clientes, nem elimina a necessidade de avaliar previamente os riscos jurídicos e regulatórios da contratação.

TOME CUIDADO!

Esses contratos podem parecer práticos à primeira vista, mas muitas vezes escondem riscos relevantes, como:

- **Isenção ampla de responsabilidade do fornecedor,** inclusive em casos de falhas sistêmicas que causem prejuízos à instituição ou a seus clientes, o que compromete a definição de responsabilidades exigida pelos reguladores;
- **Ausência de garantias mínimas de desempenho,** suporte ou disponibilidade, em desacordo com os princípios de continuidade operacional e robustez contratual esperados em contratações de serviços relevantes;
- **Permissão genérica para uso dos dados da instituição e de seus clientes,** inclusive para treinar modelos de IA, sem distinção entre dados pessoais, sensíveis, financeiros ou estratégicos. Isso pode violar a LGPD, especialmente quanto à limitação de finalidade, minimização de dados e

necessidade de base legal adequada, e também a Lei Complementar nº 105/2001 (Lei do Sigilo Bancário), que impõe às instituições financeiras o dever de manter a confidencialidade sobre informações de clientes e operações, salvo em situações expressamente previstas em lei;

- **Omissão quanto a deveres regulatórios locais,** como notificações de incidentes de segurança à ANPD, BACEN e CVM, atendimento aos titulares de dados, obrigações de auditoria, rastreabilidade, governança, cibersegurança e exigência de acesso irrestrito da instituição e dos reguladores aos dados, nos casos de serviços considerados relevantes.

Termos de uso desenvolvidos para o mercado global geralmente não consideram as exigências específicas aplicáveis a instituições supervisionadas pelo Banco Central do Brasil e pela CVM, nem estão alinhados com as obrigações previstas na Lei Geral de Proteção de Dados (LGPD).

Além disso, como muitos fornecedores estão sediados fora do Brasil, eles podem:

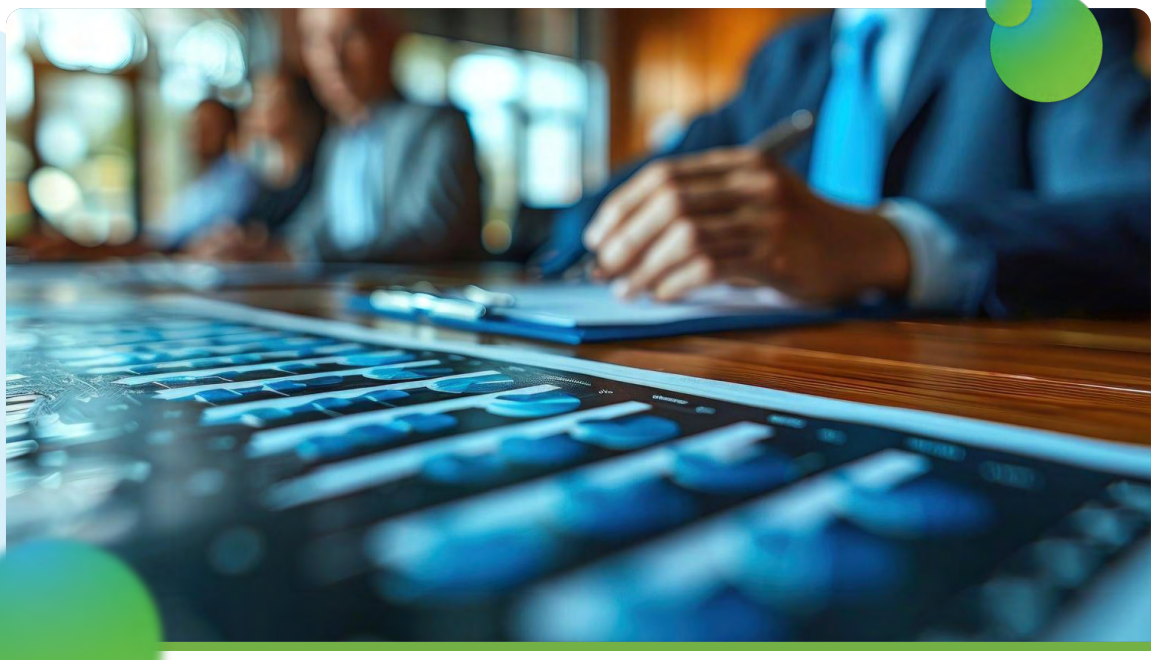
- Não ofereçam suporte em português ou tenham tempos de resposta incompatíveis com os riscos envolvidos;
- Não permitam auditorias nem forneçam documentação técnica adequada;
- Não cumpram ordens de autoridades nacionais, como o BACEN, a ANPD ou a CVM.

Nesses casos, a instituição deve adotar uma postura ainda mais cuidadosa, lembrando que a responsabilidade pela prestação do serviço continua sendo da própria instituição contratante. Algumas ações recomendadas incluem:

1. Verificar se o contrato permite **personalizações, aditivos** ou a **assinatura de instrumentos adicionais** válidos e vinculados ao termo de adesão (contrato principal), para atender às exigências regulatórias aplicáveis;

2. Solicitar **esclarecimentos formais** e **compromissos adicionais por e-mail** ou em documento separado, mesmo que fora do contrato principal;

3. Registrar internamente os riscos assumidos, com validação formal das áreas de risco, compliance e jurídico, conforme os deveres de governança e os procedimentos previstos nas normas internas da instituição.



CHECKLIST: O QUE OBSERVAR COM ATENÇÃO NA HORA DE CONTRATAR UMA SOLUÇÃO DE IA?

1. Qual é o modelo de contratação?

Por que isso importa? Porque os riscos e responsabilidades mudam conforme o tipo de contratação.

Pergunte-se

- Estou contratando uma IA pronta (SaaS), um plugin conectado a outro sistema (API) ou desenvolvendo algo sob medida?
- A licença cobre todos os usos pretendidos ou é restrita?
- Se for desenvolvimento próprio, a propriedade intelectual (código, modelo treinado) será minha?
- Se o modelo for SaaS ou API, o fornecedor se enquadra como prestador de serviço relevante?

2. O que o contrato diz sobre os dados usados pela IA?

Por que isso importa? A IA opera com dados — muitas vezes pessoais, sensíveis, financeiros ou estratégicos — e o tratamento inadequado dessas informações pode gerar riscos legais, regulatórios e reputacionais.

Pergunte-se

- Os dados da minha instituição ou dos meus clientes podem ser usados pelo fornecedor para treinar outros modelos de IA?
- Essa prática está de acordo com os princípios da LGPD?

- O contrato traz salvaguardas específicas para dados protegidos por sigilo bancário?
- Onde os dados ficam armazenados? Há transferência internacional? O contrato informa claramente em quais países os dados são processados ou armazenados?
- Quem pode acessar esses dados?
- O contrato impõe limites técnicos e jurídicos para o uso e o acesso por terceiros?
- Existem cláusulas claras sobre a devolução ou a destruição segura dos dados ao término da contratação?

> **Evite contratos genéricos que autorizem o uso amplo dos dados sob justificativas vagas, como "melhoria do sistema", ou que não estabeleçam o que deve ser feito com os dados ao término da contratação.**

3. De quem são os resultados gerados por IA (outputs)? E quem é responsável por eles?

Por que isso importa? A IA pode tomar decisões que afetam diretamente os clientes ou gerar conteúdos usados em atividades reguladas. Por isso, é fundamental definir com clareza quem é o titular dos resultados gerados e quem responde por eles. Essa definição ajuda a mitigar riscos legais e regulatórios, especialmente em um setor sujeito à supervisão constante.

Pergunte-se

- O contrato define com clareza quem é o titular dos resultados gerados pela IA? Os conteúdos criados, como análises, materiais criativos ou estratégicos, pertencem à instituição?
- A instituição tem o direito de auditar ou revisar as decisões geradas pela IA, garantindo transparência e conformidade regulatória?
- Em caso de erro, viés ou decisão ilegal, quem assume a responsabilidade? O contrato prevê que o fornecedor responderá por eventuais danos causados por falhas no sistema?
- O contrato inclui mecanismos para mitigar riscos regulatórios, como a obrigação de revisar e corrigir decisões automatizadas?

4. O contrato limita demais a responsabilidade do fornecedor?

Por que isso importa? Limitações amplas de responsabilidade podem deixar a instituição exposta, mesmo quando a falha é do fornecedor. Isso compromete a segurança da operação e pode colocar em risco o cumprimento das exigências regulatórias.

Pergunte-se

- O contrato exclui totalmente a responsabilidade do fornecedor, mesmo em casos de falhas que causem prejuízos à instituição ou aos seus clientes?
- Há algum limite de indenização que não condiz com os riscos envolvidos na contratação?
- A responsabilidade atribuída ao fornecedor é compatível com o uso pretendido e com o nível de risco da atividade? O contrato prevê medidas para mitigar riscos, como incidentes de segurança de dados ou violações de normas regulatórias do setor financeiro?

5. O sistema permite auditoria, explicabilidade e supervisão humana?

Por que isso importa? Sem rastreabilidade e transparência, a instituição não consegue revisar ou justificar as decisões tomadas pela IA, o que dificulta a correção de erros e pode comprometer tanto a conformidade regulatória quanto a confiança dos clientes e do mercado.

Pergunte-se

- A IA permite acesso a registros (logs) e explicações claras sobre os resultados que gera?
- Existe algum mecanismo de supervisão humana para revisar ou intervir em decisões automatizadas, especialmente quando envolvem clientes ou operações reguladas? Esse mecanismo está em conformidade com as diretrizes regulatórias sobre monitoramento e supervisão de tecnologias utilizadas por instituições financeiras?

- O fornecedor disponibiliza documentação técnica detalhada e permite auditorias independentes para garantir que o sistema opera conforme os requisitos legais, regulatórios e contratuais?

A instituição deve ser capaz de entender e explicar como e por que a IA chegou a determinada decisão, especialmente quando o sistema afeta diretamente o cliente.

6. Como o contrato trata segurança da informação e proteção de dados?

Por que isso importa? A responsabilidade pelo uso adequado e pela segurança dos dados continua sendo da instituição, mesmo quando o sistema é terceirizado. As normas regulatórias exigem que sejam adotadas medidas concretas de proteção, governança e resposta a incidentes.

Pergunte-se

- O fornecedor adota práticas de segurança compatíveis com as normas do setor, como as do BACEN, CVM e ANPD?
- O contrato prevê cláusula de notificação de incidentes de segurança em prazo adequado, compatível com os deveres de comunicação às autoridades competentes?
- O sistema conta com criptografia, controle de acesso, segregação de dados, políticas de minimização e planos de continuidade e recuperação em caso de falhas?
- As medidas de segurança adotadas são proporcionais ao nível de criticidade do serviço, especialmente quando o fornecedor for considerado prestador de serviço relevante?

7. O fornecedor presta suporte e coopera para o cumprimento de obrigações legais pela instituição contratante?

Por que isso importa? A falta de suporte técnico ou de colaboração efetiva compromete a governança, a conformidade regulatória e a capacidade da instituição de responder de forma adequada a crises, fiscalizações e exigências legais.

Pergunte-se

- O suporte técnico oferecido é compatível com o horário de operação e com o nível de criticidade da aplicação, especialmente em sistemas que exigem alta disponibilidade?
- O fornecedor se compromete a auxiliar no atendimento a titulares de dados, à ANPD, ao BACEN, à CVM e a outras autoridades competentes?
- O contrato prevê cooperação em auditorias, investigações, fiscalizações e processos judiciais, incluindo fornecimento de documentação técnica e acesso a registros e logs?
- A instituição e os reguladores têm garantido o acesso às informações, dados, contratos e documentos necessários, inclusive em caso de encerramento contratual ou troca de fornecedor?

Quanto mais estratégica for a IA para o negócio, maior deve ser o nível de suporte e a obrigação de colaboração formalizada em contrato.

Com base nesta checklist, é possível mapear os principais pontos de atenção, riscos e oportunidades de melhoria no contrato. Mesmo que nem todos os critérios estejam plenamente atendidos, isso não significa necessariamente que a contratação precise ser descartada. A lista representa um cenário ideal, que orienta uma decisão mais segura. Cabe à instituição decidir seguir em frente, desde que os riscos estejam identificados, documentados e acompanhados de medidas de mitigação compatíveis.

Por outro lado, se o contrato for de adesão e não atender aos critérios mínimos necessários para garantir a segurança jurídica da operação, a instituição deve avaliar com cuidado os impactos dessa contratação. Quando os riscos são altos e as possibilidades de mitigação são limitadas, especialmente em questões regulatórias, de responsabilidade civil e de proteção de dados, a contratação pode se mostrar incompatível com as exigências legais e regulatórias aplicáveis.

Nesses casos, vale reavaliar a viabilidade do contrato à luz das obrigações regulatórias. A instituição financeira pode considerar outras opções no mercado que ofereçam termos mais alinhados ao nível de responsabilidade e estabilidade exigido. Fornecedores com maior flexibilidade contratual, suporte local ou histórico de atuação junto a instituições reguladas tendem a ser escolhas mais adequadas, permitindo um alinhamento mais sólido com os requisitos normativos e com a governança esperada em soluções críticas, como as baseadas em inteligência artificial.

_O QUE FICA DE LIÇÃO?<<

Ao longo deste guia, buscamos apresentar os principais pontos de atenção na contratação de fornecedores de sistemas de inteligência artificial. Mostramos como é fundamental avaliar tanto a conformidade das soluções quanto a capacidade do fornecedor em apoiar as instituições no cumprimento de suas obrigações regulatórias.

Reforçamos que o cenário de IA é dinâmico e está em constante evolução. Isso exige uma atenção contínua aos riscos envolvidos e a revisão periódica das políticas internas sobre o uso da tecnologia.

A ANBIMA está ao seu lado para acompanhar as tendências, promover o conhecimento e fortalecer o compartilhamento de experiências.

Juntos, podemos explorar o potencial da IA de forma estratégica, ética, segura e sustentável, construindo um futuro mais eficiente e inclusivo para o nosso mercado.

_REFERÊNCIAS E RECOMENDAÇÕES DE LEITURA ADICIONAL<<

BRASIL. Lei Complementar nº 105/2001. Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências. [↗]

BRASIL. Lei nº 13.709/2018. Lei Geral de Proteção de Dados Pessoais (LGPD). [↗]

BRASIL. Projeto de Lei nº 2338/2023. Dispõe sobre o desenvolvimento, o fomento e o uso ético e responsável da inteligência artificial com base na centralidade da pessoa humana. [↗]

BANCO CENTRAL DO BRASIL. Resolução CMN nº 4.893/2021. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de

computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil. [↗]

BANCO CENTRAL DO BRASIL. Resolução BCB nº 265/2022. Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações de instituição classificada como Tipo 3 enquadrada no Segmento 2 – S2, Segmento 3 – S3 ou Segmento 4 – S4. [↗]

COMISSÃO DE VALORES MOBILIÁRIOS. Resolução CVM nº 35/2021. Estabelece normas e procedimentos a serem observados na intermediação de operações realizadas com valores mobiliários em mercados regulamentados de valores mobiliários. [↗]

IBM. Artificial Intelligence implementation: 8 steps for success [↗]

IBM. Agentic AI vs. Generative AI [↗]

EUROPEAN COMMISSION. Commentary: Model Contractual Clauses for the public procurement of AI (MCC-AI) [↗]

OCDE. The Adoption of Artificial Intelligence in Firms: New Evidence for Policy Making [↗]

OCDE. Artificial Intelligence (AI) in finance [↗]

UNIÃO EUROPEIA. Proposta de cláusulas contratuais-tipo para a contratação de sistemas de inteligência artificial por Organizações Públicas. [↗]

Expediente

Guia orientativo:
Boas práticas para a contratação de sistemas de inteligência artificial

Presidente
Carlos André

Diretores
Adriano Koelle, Andrés Kikuchi, Aquiles Mosca, Carlos Takahashi, César Mindof, Eduardo Azevedo, Eric Altafim, Fernanda Camargo, Fernando Rabello, Flavia Palacios, Giuliano De Marchi, Gustavo Pacheco, Gustavo Pires, Julya Wellisch, Pedro Rudge, Roberto Paolino, Roberto Paris, Rodrigo Azevedo, Sergio Bini, Sergio Cutolo, Teodoro Lima e Zeca Doherty

Comitê executivo
Amanda Brum, Eliana Marino, Francisco Vidinha, Guilherme Benaderet, Lina Yajima, Marcelo Billi, Soraya Alves, Tatiana Itikawa, Thiago Baptista e Zeca Doherty

Superintendência de Sustentabilidade, Inovação e Educação
Marcelo Billi

Gerência de Sustentabilidade e Inovação
Luiz Pires

Organização técnica
Lucas Lucena

Apoio técnico
Opice Blum

Diagramação
João Silva

REDE ANBIMA DE INOVAÇÃO

Endereço

Rio de Janeiro
Praia de Botafogo,
501 – 704, Bloco II, Botafogo,
Rio de Janeiro, RJ
CEP: 22250-911

Tel.: (21) 2104-9300

São Paulo
Av. Doutora Ruth Cardoso,
8501, 21° andar,
Pinheiros São Paulo, SP
CEP: 05425-070

Tel.: (11) 3471 4200

www.anbima.com.br

ANBIMA