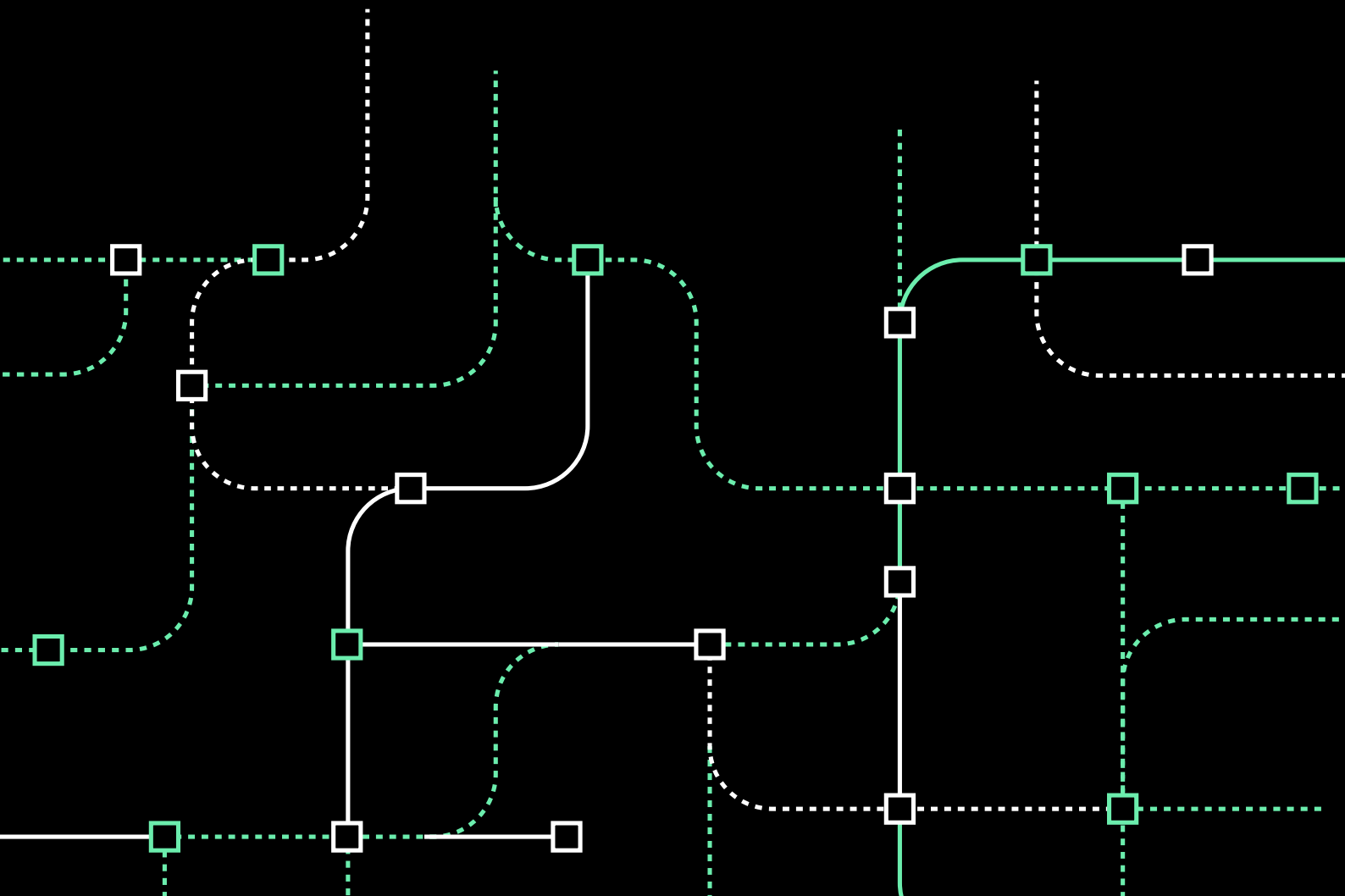
OneTrust

Relatório OneTrust – Projeções para 2027

# A arquitetura da governança de IA:

## modelos para um cenário em transformação

Relatório



# Conteúdo

Introdução – Acesso concedido, autoridade delimitada, confiança comprovada 3

Projeção 1 – Sem comprovação, não há negócio. A segurança da IA se torna um requisito. 4

Projeção 2 – O sinal verde pode levar ao destino errado. Agentes aprovados podem executar tarefas não autorizadas. 7

Projeção 3 – A aprovação não é definitiva. Mudanças significativas na IA exigem novas avaliações de segurança. 10

Projeção 4 – Permissão não significa acesso total. Nas interações com a IA, as decisões sobre o uso de dados fazem parte da jornada. 14

A regulamentação da IA em 2027, segundo especialistas 17

Contraprevisões: três coisas que não acontecerão em 2027 25

**Aviso legal**
Nenhuma parte deste documento pode ser reproduzida sem a permissão por escrito do proprietário dos direitos autorais. O conteúdo deste documento está sujeito a revisão sem aviso prévio, devido ao progresso contínuo na metodologia, design e produção. A OneTrust LLC não se responsabiliza por erros ou danos de qualquer tipo resultantes do uso deste documento. Os produtos, o conteúdo e os materiais da OneTrust têm finalidade unicamente informativa, e não de aconselhamento jurídico. Entre em contato com sua assessoria jurídica para obter aconselhamento em relação a questões legais. Os materiais da OneTrust não garantem a conformidade com as leis e regulamentos aplicáveis.

Direitos autorais: © 2026 OneTrust LLC. Todos os direitos reservados. Informação proprietária e confidencial.

## Introdução

# Acesso concedido, autoridade delimitada, confiança comprovada



**Blake Brannon**
Diretor de inovação
OneTrust

O avanço da inteligência artificial de fronteira levanta uma questão: o que estamos preparados para permitir que esses sistemas façam? Isso é crucial quando agentes de IA podem mudar registros, usar dados dos consumidores ou executar ações em outros sistemas.

Uma pessoa contratada recebe um crachá, é informada sobre o que pode decidir e conquista confiança com o tempo. O agente de IA precisa dessas mesmas coisas, mas de formas diferentes.

Um agente obtém acesso quando alguém o conecta a um sistema, muitas vezes herdando esses acessos de seu criador – geralmente, mais do que a tarefa exige. Na edição de 2026 da pesquisa Governança Preparada para a IA da OneTrust, 87% dos respondentes afirmam que suas empresas incentivam o uso de agentes, 47% já contam com governança e controles claros e 40% ainda estão desenvolvendo essas capacidades. Incentivar o uso é a atitude certa, mas o risco está no que se presume em paralelo. O acesso é concedido.

O que um agente pode fazer com esse acesso é uma decisão à parte, e alguém precisa tomá-la. Acesso é o que o sistema pode alcançar; autoridade é o que ele pode fazer com esse alcance e até que limite. Um agente com acesso a um sistema de pedidos, por exemplo, pode ter autoridade para aplicar reembolsos de até US$ 200 em pedidos com menos de 30 dias, encaminhando a uma pessoa os casos fora dessas condições. Os limites precisam ser documentados e aplicados no momento do reembolso, e não presumidos previamente, pois a atuação de um agente se expande em silêncio. Ele cria conexões, aprende em conversas algo que não seria perguntado em formulários e usa isso para ir além da finalidade original – tudo sob a mesma aprovação e sem sinalização. Só 5% dos respondentes relatam coordenação e responsabilização claras no ciclo de vida da IA. Sem isso, ações permitidas individualmente podem se combinar em algo que ninguém autorizou. A autoridade deve ser delimitada.

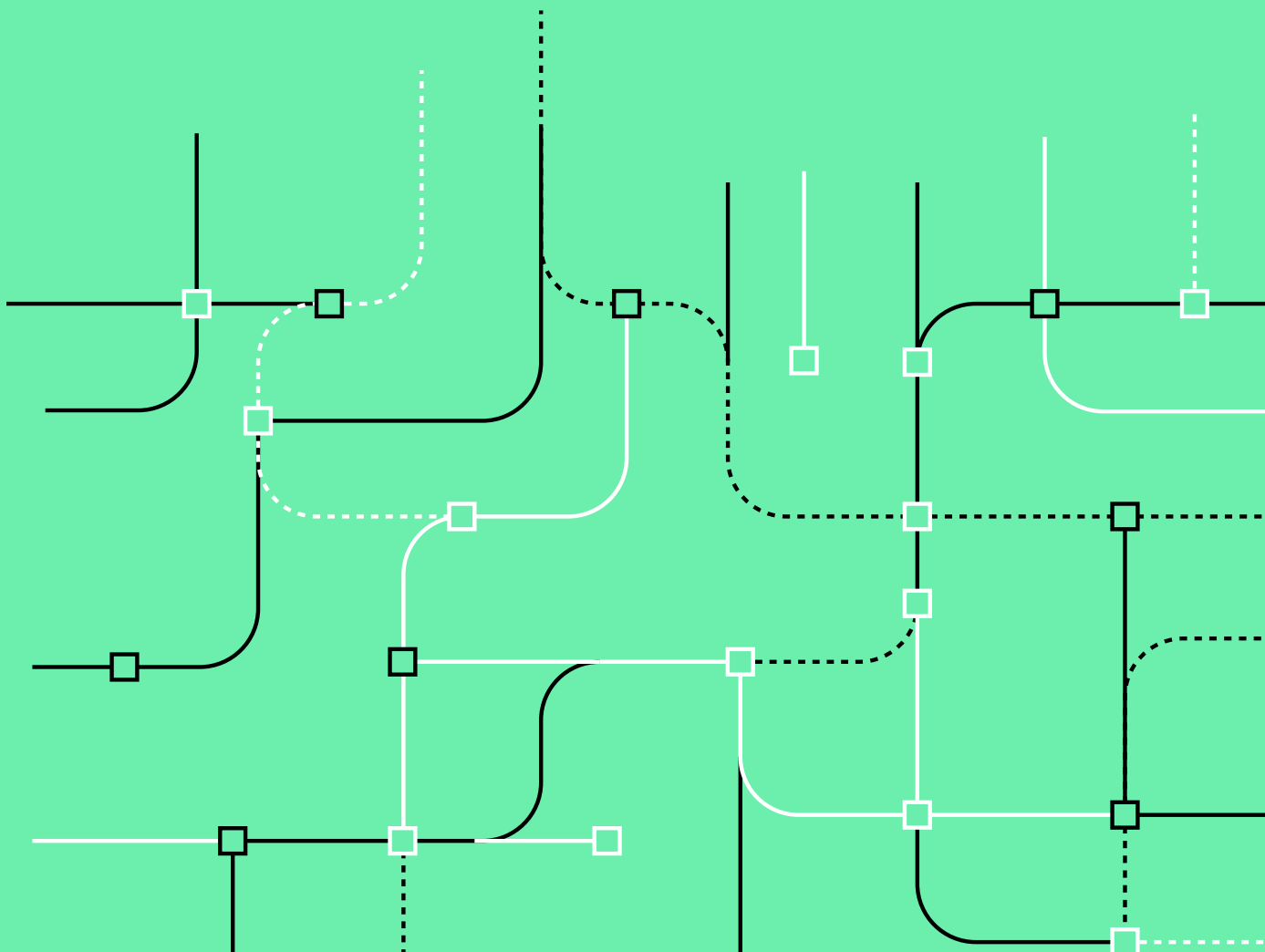
Para ser confiável, o agente precisa demonstrar que fez o que estava autorizado e nada além – o que precisa ser verificável. Um agente pode operar com as credenciais de uma pessoa e usar o nome dela nos sistemas que acessa, mas não carrega o histórico que valida essas credenciais. A identidade é herdada, mas a confiança, não. O agente não pode ser testemunha de si mesmo: seu registro de atuação é só mais uma saída do sistema, que precisa ser mantida fora de seu controle e preservada como evidência. Só 28% dos entrevistados afirmam manter evidências de governança e trilhas de auditoria. A primeira projeção deste relatório mostra quem solicitará essas evidências e quando. A confiança deve ser comprovada.

Nada disso é argumento para desaceleração. Limites claros evitam atrasos, e a governança permite que decisões difíceis sejam tomadas no ritmo certo e os responsáveis pelos riscos sejam nomeados.

As quatro projeções a seguir analisam como o acesso, a autoridade e as evidências moldarão a adoção da IA e seus resultados comerciais em 2027. Antes de expandir a autoridade de um agente, a empresa é capaz de explicar as finalidades permitidas, impedir ações não autorizadas e reconstruir o que foi feito? Esse é o teste para o qual este relatório incentiva os líderes a se prepararem.

# Projeção 1

## Sem comprovação, não há negócio. A segurança da IA se torna um requisito.



**Projeção 1**

# Sem comprovação, não há negócio. A segurança da IA se torna um requisito.

Em 2027, os compradores de serviços baseados em IA com impacto significativo exigirão evidências atuais e relevantes antes de ativar ou ampliar o uso desses serviços. As garantias exigidas refletirão a autonomia da solução, seus efeitos sobre os negócios e possíveis danos. Essa pressão poderá se estender às decisões de orçamento, contratação e renovação.

No caso de um provedor que lança uma nova funcionalidade para um serviço, por exemplo: o recurso é desenvolvido e disponibilizado, mas o cliente hesita em ativá-lo. A questão é se as garantias fornecidas originalmente cobrem o que o serviço passou a ser capaz de fazer.

A prontidão técnica do fornecedor nem sempre se traduz em aceitação do cliente. O valor do lançamento depende, em parte, da abordagem dos riscos que se interpõem entre a disponibilidade e a ativação.

Essa conexão deve ser mais explícita em 2027. Os compradores questionarão se as garantias existentes se aplicam às novas funcionalidades e suas conexões de dados. Evidências insuficientes ou desatualizadas podem atrasar a ativação e limitar o uso ou a expansão.

A pesquisa revela um cenário desigual: 28% dos respondentes afirmam manter evidências de governança e registros de auditoria, enquanto 38% priorizam a preparação para regulamentos, normas ou auditorias nos 12 meses seguintes.

> “Os clientes precisam de garantias adequadas à funcionalidade que são convidados a usar. Quando essa funcionalidade muda, os testes anteriores podem não responder às novas questões. As evidências ajudam a compreender os riscos e decidir se é seguro habilitar o novo recurso".

**Tim Mullen**
Diretor de informação
OneTrust



As evidências devem contribuir com as decisões. Um teste de penetração identifica vulnerabilidades; uma avaliação de controles testa o respeito aos limites. As empresas precisam ainda saber o que foi examinado, que proteções continuam eficazes e quem pode aceitar os riscos remanescentes.

Uma pesquisa recente da Gartner identifica a governança como um critério para a compra de soluções de IA e aponta uma demanda por mecanismos de rastreabilidade e intervenção. A análise também associa a falta de evidências a processos lentos de due diligence e restrições em seguros. Isso reforça as projeções deste relatório, embora não permita determinar até que ponto essas exigências já influenciam os resultados comerciais.

A pressão também atinge as equipes executivas, que, segundo argumenta a Gartner, precisam saber quais decisões comerciais são influenciadas pela IA e quem são os responsáveis pelas consequências. Esse escrutínio deve tornar as evidências mais decisivas para a ativação de novas funcionalidades ou a ampliação de autoridade.

A análise de provedores assistida por IA é uma possibilidade para 2027. Políticas e materiais de segurança publicados podem influenciar a triagem inicial, mas resta saber se terão impacto nas decisões de contratação.

Para diretores financeiros, a questão é se o valor gerado por um recurso justifica o custo operacional e os riscos. Espera-se que as decisões de investimento se baseiem mais explicitamente nessa avaliação, em conjunto com a segurança. Uma nova funcionalidade pode respeitar os limites aprovados e ainda assim não se justificar.

Para os fornecedores, a garantia de segurança passa a ser parte do processo de colocar um recurso em uso. É preciso identificar que evidências faltam e quem pode tomar decisões. Para os compradores, a questão prática é decidir se devem ativar o recurso, impor condições ou esperar.

## O que pode mudar a projeção

Os compradores podem continuar aceitando questionários conhecidos e testes periódicos. Exclusões em seguros podem alterar a exposição ao risco sem novos investimentos em governança, enquanto os litígios evoluem de forma desigual. A projeção perde força se a influência das evidências sobre a ativação, a contratação e a expansão for pequena.

**Probabilidade:** moderada.



## Impacto sobre o setor:

Alto nas áreas em que a segurança afeta a aceitação ou a expansão da IA. As consequências podem atingir a adoção de produtos, os termos comerciais e a confiança ao assumir compromissos.

## Prioridades para os líderes de governança

- Segurança e produto: associar as garantias às funcionalidades oferecidas.
- Equipes comerciais: rastrear solicitações que afetem a aceitação e a implementação.
- Riscos e setor jurídico: identificar questões relevantes em contratos, cobertura e divulgação.
- Finanças: definir o valor esperado, os custos operacionais e as evidências de segurança necessárias antes do investimento.

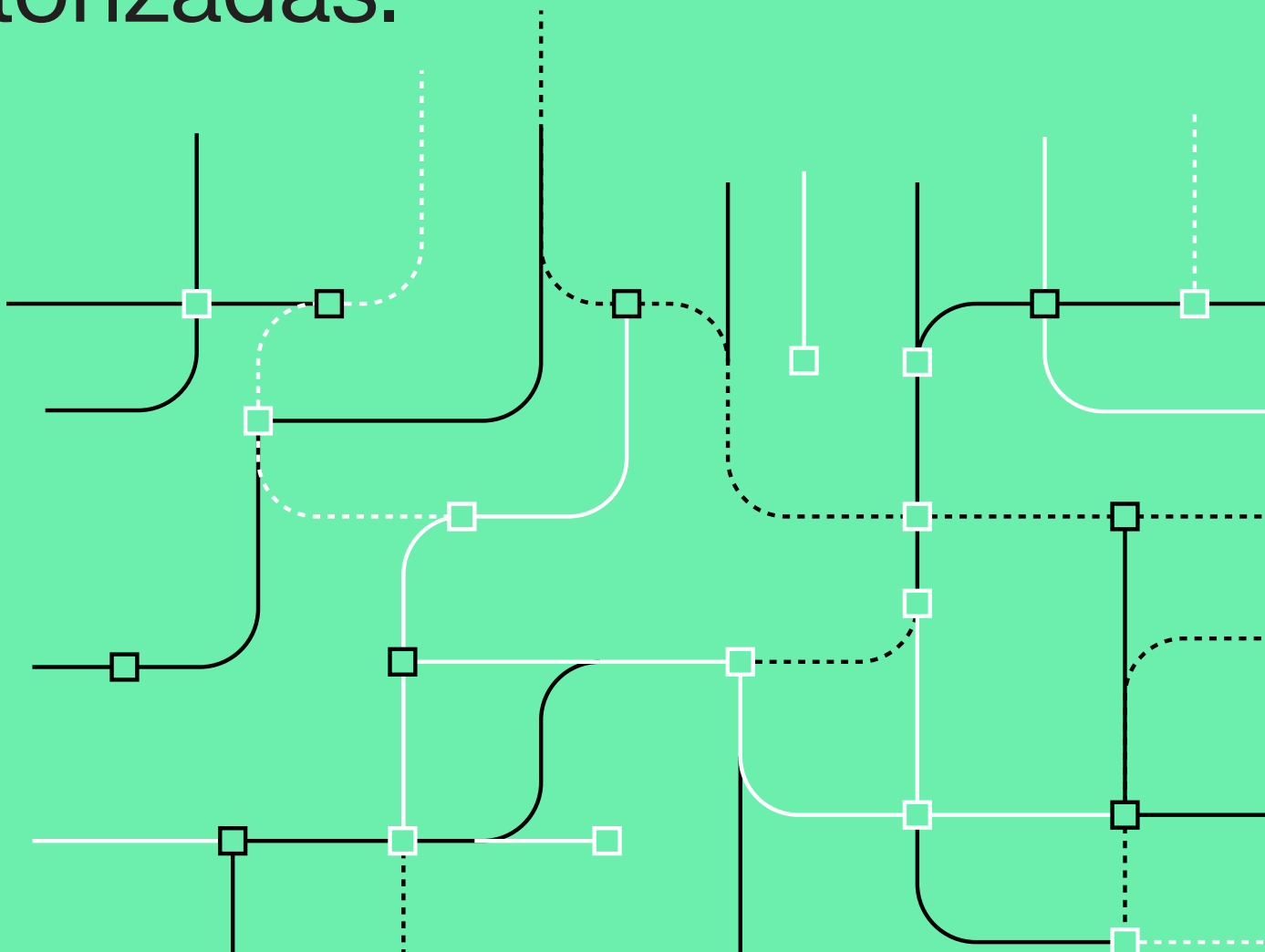
## O que observar em 2027

- Ativações e expansões adiadas até que novas evidências sejam fornecidas.
- Exigências contratuais de segurança após mudanças.
- Questões específicas sobre IA na avaliação de riscos em seguros.
- Decisões de financiamento levando em conta o valor gerado e o custo operacional além de evidências de controle.

[1] *When AI Governance Fails, Revenue and Executives Take the Hit. Gartner, 2026.*

# Projeção 2

O sinal verde pode levar ao destino errado. Agentes aprovados podem executar tarefas não autorizadas.



## Projeção 2

# O sinal verde pode levar ao destino errado. Agentes aprovados podem executar tarefas não autorizadas.

Em 2027, os critérios de implementação de programas baseados em agentes incluirão autoridade específica por tarefa, intervenção testada e registros protegidos. Alguns programas também avaliarão o resultado combinado de ações individualmente permitidas.

> Queremos que o agente faça mais: acesse a internet, atue no Salesforce, acione fluxos de trabalho e envie mensagens. Mas esse agente pode herdar os acessos de seu criador e não seu julgamento. Com mais autoridade, ele continua sendo o mesmo agente aprovado antes"?

**DV Lamba**
Diretor de tecnologia e produtos
OneTrust

Por exemplo: um agente encarregado de reduzir gastos com nuvem sem comprometer os prazos dos pedidos reduz a capacidade ociosa e adia tarefas em lote – ações tecnicamente permitidas.

A fatura diminui, mas o processamento noturno de pedidos não cumpre os prazos. As ações foram validadas individualmente, mas seu efeito combinado viola uma condição.

O desafio é definir o que o agente está autorizado a fazer, incluindo consequências não aceitáveis. A permissão técnica para reduzir a capacidade ou adiar tarefas não autoriza todas as concessões que essas ações podem acarretar. Os limites precisam ser aplicados onde as ações são efetivamente realizadas, com possibilidade de intervenção se forem ultrapassados.

A função do agente pode ainda se expandir após a aprovação. O fluxo de trabalho pode ganhar novas conexões e responsabilidades. A empresa precisa determinar quando essas adições excedem a autoridade originalmente concedida.

Um registro de que cada ação foi validada tecnicamente não estabelece que o resultado final está incluído nessa validação. As tarefas devem ser autorizadas com clareza suficiente para que as as ações sejam avaliadas e os limites sejam testados.

Na pesquisa, 48% dos respondentes relatam ao menos um incidente devido a ações não aprovadas de sistemas de IA no ano anterior. Só 28% afirmam dispor de evidências de governança e registros de auditoria. Autoridade e reconstrução são questões em alta.

> Um agente aprovado para resumir tickets de suporte pode precisar de autoridade para atualizar registros ou emitir reembolsos. As empresas precisam ter a capacidade de testar esses limites após a implementação e reavaliá-los quando a tarefa e a política mudarem".

**Sriram Iyer**
Vice-presidente de estratégia e produtos de IA
OneTrust

“

O ser humano não pode ser um mero espectador. Ele precisa ter conhecimento e senso crítico para questionar a IA, em vez de se deixar persuadir por respostas bem elaboradas. Sua supervisão deve avaliar se a finalidade é válida, a direção é correta e os erros estão sendo minimizados".

**Odia Kagan**
Sócia e codiretora – Privacidade e Segurança de Dados
Fox Rothschild LLP

Os avaliadores também precisam de registros fora do alcance dos agentes que vinculem as ações de impacto à autoridade concedida. Esses registros dão suporte a investigações e comprovam as ações executadas, mas a avaliação dos resultados ainda exige uma análise com base em finalidades e limites.

A inspeção deve continuar após a implementação. As equipes precisam examinar os processos em que a IA atua, identificar comportamentos inaceitáveis e revisar as tarefas e seus controles. Um teste de aprovação não pode antecipar todas as combinações de ações com potencial impacto.

Os limites da autonomia tendem a ser mais claros em 2027. Se uma empresa não puder impor barreiras às tarefas, terá que restringir o acesso a dados, remover ferramentas ou manter controles humanos. A autoridade maior deverá ser condicionada a controles demonstráveis e decisões conscientes sobre os riscos residuais.

## O que pode mudar a projeção

A revisão humana pode permanecer suficiente para tarefas delimitadas. A avaliação da tarefa como um todo pode aumentar os custos sem detectar resultados nocivos. A adoção pode ser mais rápida para mecanismos de autoridade e intervenção do que para a avaliação confiável dos resultados.

**Probabilidade:** moderada



(para critérios rigorosos de implementação. Em estágio inicial para a avaliação da tarefa como um todo).

## Impacto sobre o setor:

Alto nos casos em que a autoridade do agente afeta serviços, transações ou decisões sensíveis.

## Prioridades para os líderes de governança

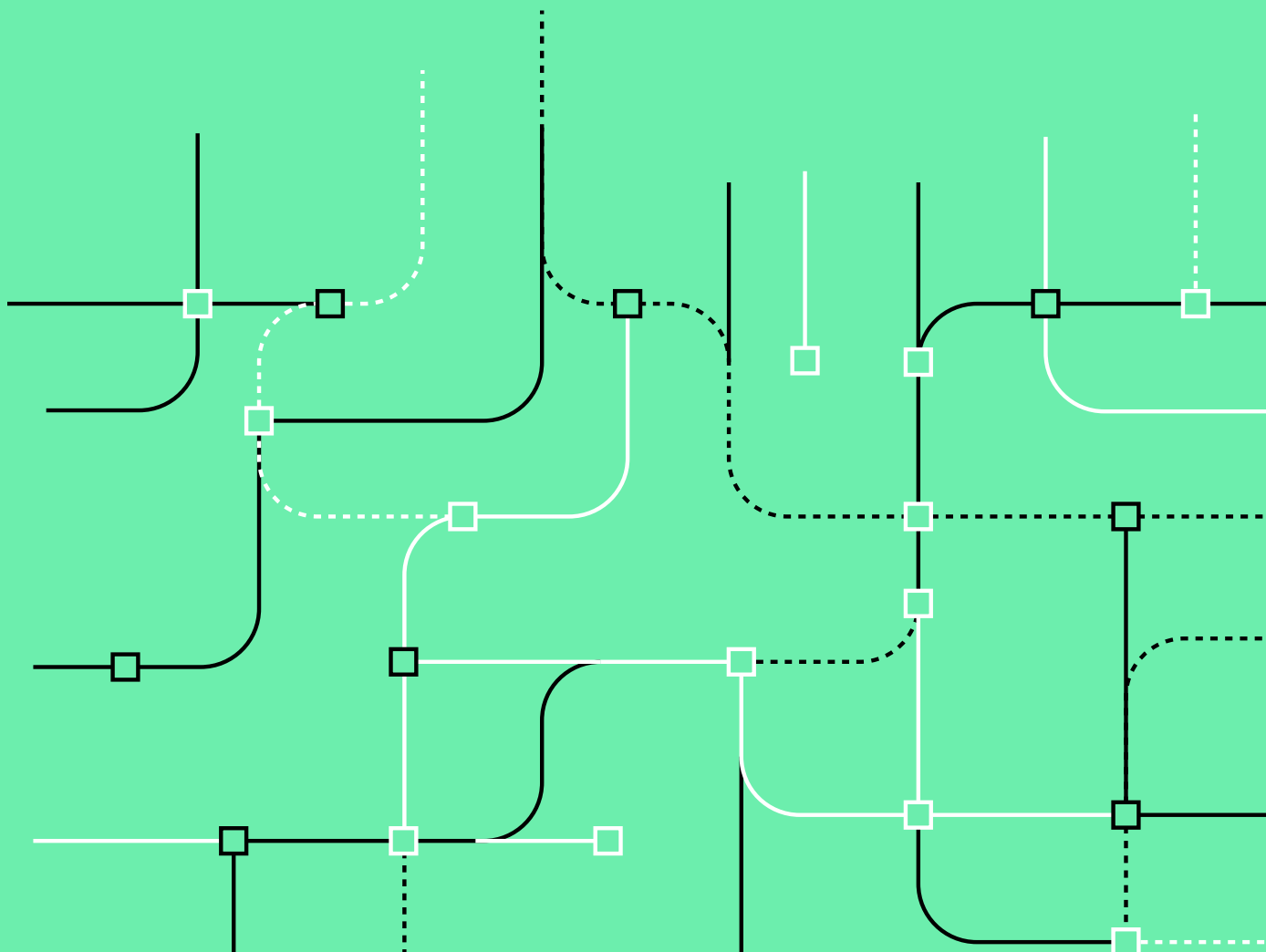
- Responsáveis pelos negócios: definir resultados inaceitáveis, revisar o comportamento em execução e atribuir responsabilidades pela remediação.
- Segurança e engenharia: testar negação, expiração e revogação.
- Privacidade e governança de IA: converter finalidades e apetite ao risco em condições aplicáveis.
- Auditoria: definir como uma tarefa pode ser reconstruída.

## O que observar em 2027

- Exigência de limites e testes de intervenção nas revisões.
- Registros protegidos da ação dos agentes.
- Avaliações que detectam combinações inseguras de ações permitidas.
- Suporte e desativação de agentes com base em controles de acesso.
- Evidências de que as mudanças em políticas chegam aos agentes e são testadas.
- Constatações pós-implementação levando à revisão dos limites, controles e procedimentos.

# Projeção 3

A aprovação não é definitiva. Mudanças significativas na IA exigem novas avaliações de segurança.



## Projeção 3

# A aprovação não é definitiva. Mudanças significativas na IA exigem novas avaliações de segurança.

Em 2027, mudanças significativas em soluções de IA serão tratadas como eventos de avaliação, mesmo quando não houver incorporação de fornecedores. A análise levará em conta os recursos afetados, as ferramentas conectadas, o acesso aos dados e a eficácia dos controles.

Uma equipe de suporte ao cliente usa um aplicativo de IA hospedado. O setor de engenharia opera um modelo público. Uma plataforma aprovada adiciona um assistente que se conecta a registros internos.

Esse ecossistema inclui soluções desenvolvidas internamente, compradas e incorporadas a ferramentas existentes. A responsabilização é diferente em serviços hospedados, modelos internos e de parâmetros abertos. Esses parâmetros, por si só, não informam quem opera a implementação.

> “
>
> Não é possível governar algo que não se pode ver. Todos os dias surgem agentes que executam ações e acessam dados pessoais e sensíveis. Precisamos ter visibilidade sobre esses agentes e formas de identificar quando eles exigem uma avaliação mais profunda".

**Manuel Manuel**
Especialista em proteção de dados e IA
Scania

Essa diversificação não requer um programa de governança separado para cada modelo ou ferramenta. É preciso ampliar as responsabilidades já estabelecidas em termos de segurança, privacidade, risco, compras e negócios para novas combinações de tecnologias.

> “
>
> A IA não criou uma nova categoria de governança. Ela se soma à governança que as organizações já precisam. Com o crescimento da adoção da IA e das exigências de privacidade, a governança como um todo terá uma posição mais central na atividade das empresas".

**Damian Apone**
Diretor de segurança cibernética – Varejo Global
Genuine Parts Company

O mais importante é saber quais responsabilidades cabem a cada parte envolvida.

Um fornecedor pode operar um serviço enquanto o cliente controla a configuração. Uma equipe interna pode operar um modelo enquanto o responsável comercial define os usos aceitáveis. Conectores e ferramentas podem introduzir novos acessos.

> O mais difícil é manter a visibilidade operacional enquanto a IA atua em processos existentes. Com muitos envolvidos, pode ser complicado definir responsabilidades. Com a evolução dos modelos, provedores e casos de uso, a conformidade se torna um trabalho contínuo: monitorar mudanças e decisões e reavaliar riscos em diferentes setores".

**Olivia Roth**
Encarregada pela proteção de dados e governança de IA
Yves Rocher Germany

Na pesquisa, 39% dos respondentes apontam a visibilidade limitada sobre soluções de terceiros como fator de atraso. Outros 28% afirmam que ferramentas de terceiros foram adotadas antes de uma avaliação completa. A visibilidade sobre essas relações é essencial para determinar quais mudanças exigem novas aprovações.

Uma mudança é significativa quando altera uma premissa que fundamentava uma aprovação original. Um novo conector pode expor dados de clientes; permissões mais amplas podem autorizar um assistente a atualizar registros que antes só podia ler; uma mudança no modelo pode afetar controles. A revisão deve considerar a mudança na exposição ao risco e reaproveitar evidências aplicáveis.

> Uma avaliação registra uma decisão sobre uma funcionalidade específica. Um novo modelo, conector ou fonte de dados pode alterar as premissas por trás dessa decisão. Uma notificação ajuda a identificar a mudança, mas a empresa precisa decidir se a aprovação original continua válida ou se a funcionalidade afetada deve ser reavaliada, restringida ou desabilitada".

**Sriram Iyer**
Vice-presidente – Estratégia e Produtos de IA
OneTrust

Se o recurso modificado der suporte a um processo crítico, restringi-lo pode interromper operações. Prosseguir sem reavaliação pode gerar riscos não considerados na aprovação original. A definição de responsabilidades e medidas de contingência determina a agilidade da resposta.

A revisão manual de cada componente é repetitiva e difícil. A priorização deve se basear nos possíveis danos, na sensibilidade dos dados e nas dependências da empresa. Usos de alto impacto requerem responsabilidades claras quanto à detecção de mudanças e às medidas a serem tomadas. Nem toda atualização exige reavaliação completa.

> Os clientes exigirão garantias, mas verificar cada fornecedor por análises convencionais não é viável. Devemos priorizar os sistemas com maior potencial de dano e entender seus resultados. O desafio é criar um processo que responda às mudanças".

**Ojas Rege**
Vice-presidente – Produtos e Tecnologias Emergentes
OneTrust

## O que pode mudar a projeção

Os provedores podem fornecer controles suficientes para que os programas se adaptem, mas a visibilidade limitada pode prejudicar a reavaliação. A projeção depende de que as mudanças gerem decisões documentadas, e não só novas notificações.

**Probabilidade:** moderada.

As lacunas na visibilidade e na avaliação de terceiros reforçam a necessidade de uma revisão atrelada às mudanças. Em 2027, espera-se uma adoção ampla em casos de alto impacto e uma reavaliação menos consistente nos ecossistemas de IA.

## Impacto sobre o setor:

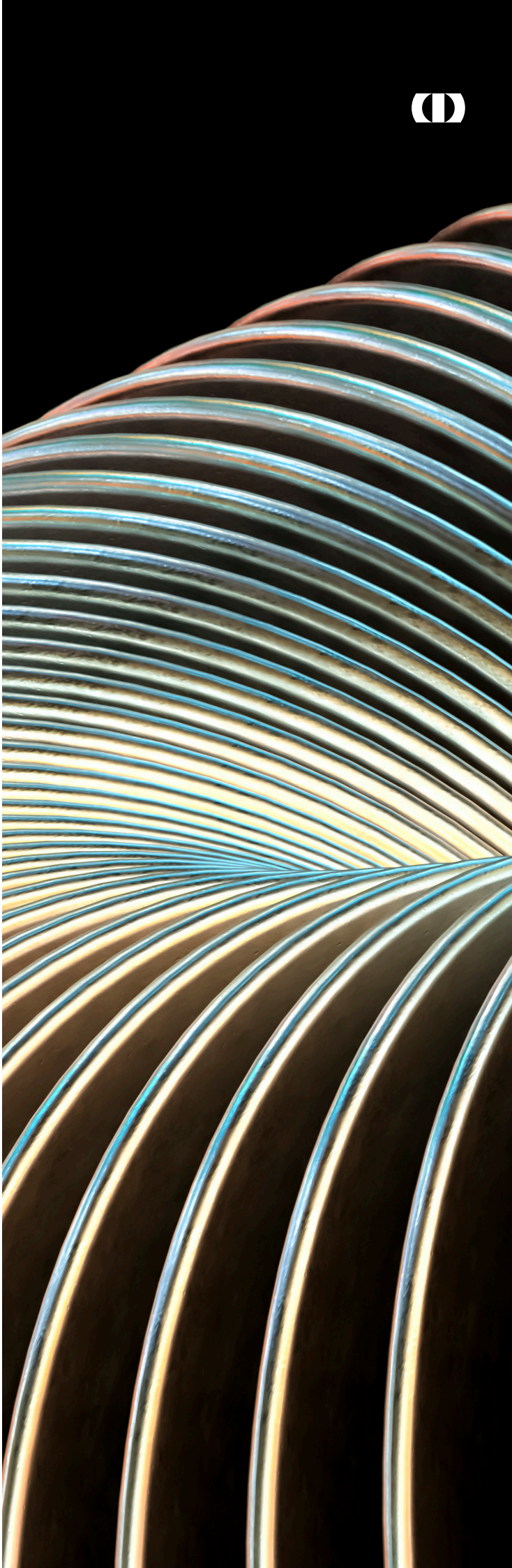
Alto para a continuidade, a segurança e a prestação de contas em implementações existentes.

## Prioridades para os líderes de governança

- Tecnologia e dados: mapear modelos, aplicativos, conectores e fluxos de dados de impacto.
- Compras e setor jurídico: estabelecer direitos de notificação de mudanças, restrição e desativação.
- Segurança: reavaliar a eficácia de acessos e controles alterados.
- Responsáveis pelos negócios: definir quem pode continuar, limitar, interromper ou remediar um uso, com alternativas de contingência.

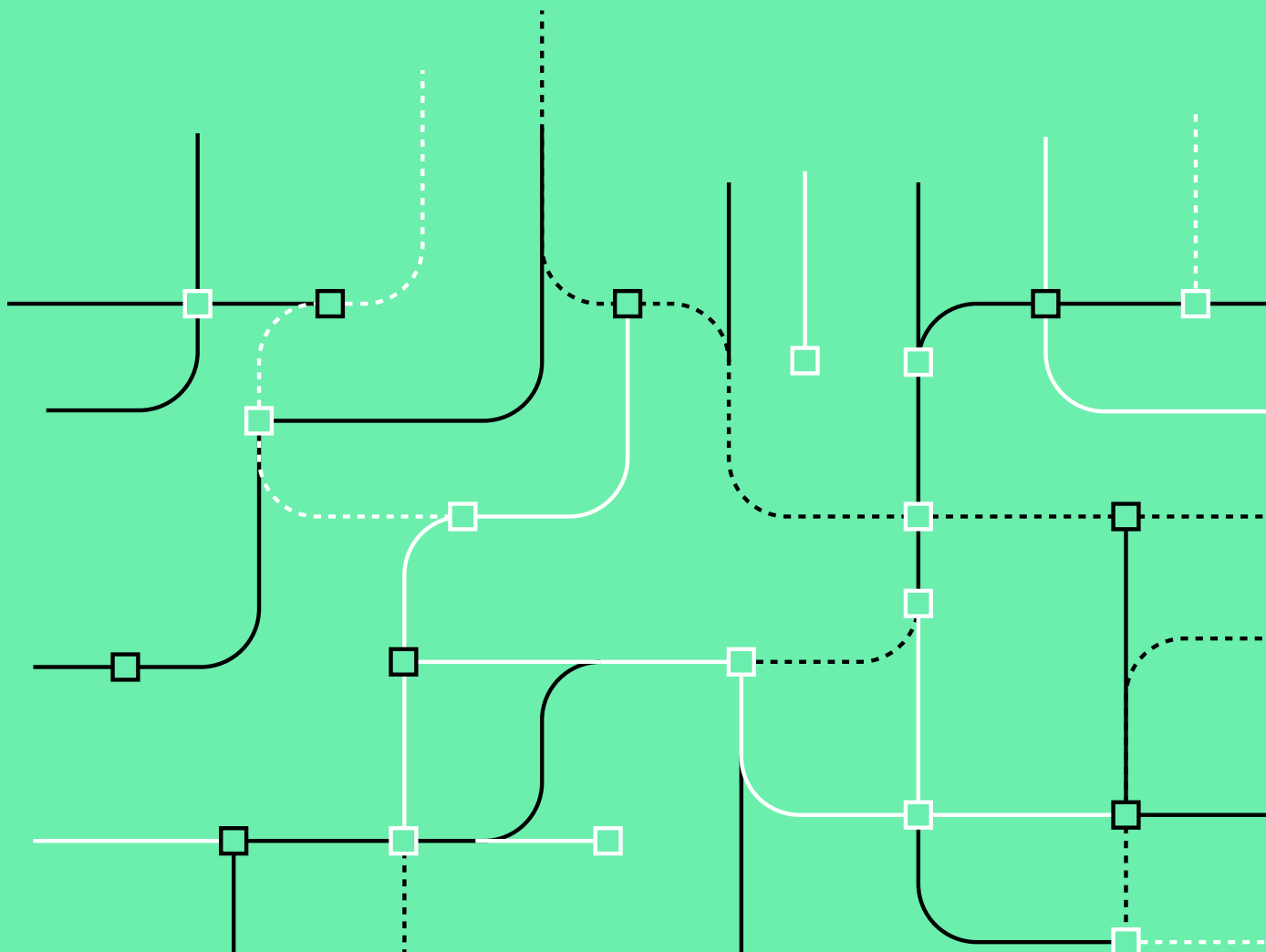
## O que observar em 2027

- Reavaliações não só em novas aquisições.
- Avisos sobre mudanças vinculados aos usos afetados.
- Revisões desencadeadas por novos recursos e pela redução da eficácia dos controles.
- Decisões documentadas sobre a continuidade, restrição ou substituição de serviços modificados.
- Planos de contingência testados para processos críticos.



# Projeção 4

Permissão não significa acesso total. Nas interações com a IA, as decisões sobre o uso de dados fazem parte da jornada.



## Projeção 4

# Permissão não significa acesso total. Nas interações com a IA, as decisões sobre o uso de dados fazem parte da jornada.

Em 2027, as empresas que adotarem a IA nas relações com o consumidor vincularão escolhas mais explícitas sobre o uso de dados às atividades autorizadas. As interações com a IA podem revelar mais informações que o necessário para atender a uma solicitação – as quais podem ser reutilizadas com finalidades diferentes das originais.

Por exemplo: um comprador pede a um assistente de IA que reserve um produto em uma loja. Na conversa com o assistente, ele explica que é um presente e descreve as preferências de quem vai recebê-lo. A interação dá contexto à operação, incluindo detalhes que não seriam solicitados em um formulário.

A finalidade imediata continua sendo encontrar o item e reservá-lo. O reaproveitamento dos dados para publicidade introduz uma permissão de uso à parte. Quando uma escolha adicional é solicitada, o serviço precisa explicá-la e garantir que a resposta do cliente seja aplicada na sequência.

Para a empresa, o desafio é preservar uma personalização útil sem deixar o cliente inseguro sobre o que foi autorizado na conversa. Várias solicitações de consentimento podem interromper o atendimento, mas o uso inesperado dos dados pode comprometer a confiança.

A escolha precisa mudar o que ocorrerá em seguida. Se o cliente recusar o uso de seus dados para publicidade, o serviço deverá respeitar essa escolha ao efetivar a reserva. Se uma escolha for posteriormente revogada, será necessário identificar os processos afetados e aplicar a alteração.

A empresa precisa ser capaz de verificar se tratamentos de dados posteriores estão de acordo com as finalidade e usos permitidos em seu mapa de dados e nas avaliações de privacidade. Propostas fora desse escopo devem passar por revisão. Se não for possível determinar o contexto original, o serviço deverá esclarecer essa incerteza antes de prosseguir.

Os requisitos da Califórnia (EUA) para decisões automatizadas ilustram um desafio operacional: explicar uma decisão exige compreender como um fluxo de trabalho usa dados pessoais e gera seus resultados. Isso reforça a necessidade de contexto e responsabilização transversal.

> “
>
> Um aviso prévio ao uso pode parecer só um requisito de divulgação, mas sua elaboração exige que as empresas mapeiem antecipadamente e com precisão a contribuição das informações pessoais para os resultados das decisões automatizadas e a própria influência desses resultados sobre as decisões".

**Jake Harrison**
Associado
Crowell & Moring LLP

“

A privacidade se refere ao que ocorre com os dados depois que entram no fluxo de trabalho. A IA pode combiná-los ou usá-los para finalidades diferentes das originais. As equipes precisam analisar os usos subsequentes e assegurar que as condições aplicadas permaneçam significativas".

**Brett Tarr**
Diretor de privacidade e governança de IA
OneTrust

A pesquisa revela a amplitude do desafio em relação aos dados: 52% dos respondentes identificam preocupações com a qualidade, a acessibilidade, a privacidade e a segurança das informações como fatores de atraso, enquanto 39% apontam a visibilidade dos riscos e do uso de dados.

As preferências do cliente, as permissões técnicas e o consentimento legal permanecem distintos. Uma instrução a um assistente não estabelece automaticamente o consentimento, e uma autorização registrada não garante a licitude do processo.

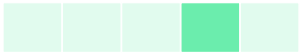
Transferências entre provedores dificultam a aplicação de controles, pois um status de permissão pode não incluir a finalidade ou os limites associados. O serviço precisa de contexto para avaliar o uso proposto. Quando esse contexto não existe, pode ser preciso suspender ou esclarecer o uso.

Espera-se que as primeiras implementações vinculem as escolhas feitas em interações com a IA ao processamento nos mesmos serviços. O valor dessas implementações dependerá da compreensão, por parte do cliente, dessas escolhas e das alterações que elas impõem aos serviços.

## O que pode mudar a projeção

Os avisos e confirmações existentes podem ser suficientes em muitos casos. Solicitações adicionais podem afetar as transações, e os provedores podem interpretar as permissões de formas diferentes. A adoção pode se limitar a serviços isolados, com poucas evidências de aplicação subsequente.

**Probabilidade:** em estágio inicial.



## Impacto sobre o setor:

Alto no âmbito da experiência do consumidor e do uso de dados, com adoção inicialmente limitada.

## Prioridades para os líderes de governança

- Produto e marketing: identificar mudanças de finalidade e destinatários.
- Privacidade e setor jurídico: determinar as escolhas e requisitos aplicáveis.
- Engenharia: testar usos permitidos e a retirada de permissões.
- Equipes de dados: preservar o contexto para decisões subsequentes.

## O que observar em 2027

- Experiências que requerem a escolha do cliente no momento do uso proposto.
- Registros que especificam a finalidade e o destinatário.
- Mudança no tratamento de dados quando uma permissão é recusada.
- Interrupção ou nova solicitação quando o escopo original é excedido.
- Testes que indicam como a retirada da permissão chega aos sistemas subsequentes.

# A regulamentação da IA em 2027, segundo especialistas



# A regulamentação da IA em 2027, segundo especialistas

A regulamentação da IA entra em 2027 com cronogramas desiguais e diferenças entre jurisdições. Alguns governos estão introduzindo requisitos específicos, enquanto outros aplicam regras de privacidade e proteção do consumidor já existentes, além de normas setoriais.

O desafio comum é cada vez mais operacional: determinar onde a IA é usada, que obrigações se aplicam, quem a controla e que evidências podem demonstrar conformidade.



# Estados Unidos: regulamentação nos fluxos de trabalho

O cenário nos EUA continua fragmentado, mas isso não reduz a carga operacional – apenas a distribui.

No nível federal, o Marco de Políticas de IA da Casa Branca, de março de 2026, apresenta recomendações legislativas não vinculantes, incluindo propostas de prevalência da legislação federal sobre a estadual. As competências dos órgãos federais e as exigências estaduais continuam a ditar a conformidade.

> Considero pequenas as chances de vermos novas leis abrangentes sobre IA no âmbito estadual ou federal em 2027. Em vez de aguardar a próxima regulamentação, as empresas devem se concentrar em ferramentas de governança transparentes e ficar atentas aos riscos que podem surgir".

**Tyler J. Thompson**
Sócio e copresidente – Prática Global de IA
Reed Smith LLP

## Destaques regulatórios

- Califórnia: a regulamentação de tecnologias de decisão automatizada entrou em vigor em janeiro de 2026. Entre as obrigações para 2027 estão os avisos prévios ao uso e os direitos de acesso e recusa para decisões significativas.
- Colorado: o governo sancionou a Lei de Tecnologias de Tomada de Decisão Automatizada, revogando uma lei estadual mais abrangente sobre IA de alto risco.
- Illinois: requisitos para o uso de IA em relações empregatícias entraram em vigor em janeiro de 2026. O governo também sancionou a Lei de Medidas de Segurança para IA de Fronteira.

Esses requisitos afetam cada vez mais as decisões de aquisição e implementação de sistemas de IA.



“

As questões importantes são mais específicas e precisam ser abordadas durante a contratação de fornecedores, e não no processo de conformidade. O modelo fornecido por um terceiro tem permissão para ser treinado com dados pessoais? Que mecanismos contratuais existem para impedir isso? Os administradores têm a autoridade necessária para ativar um novo recurso incorporado? A ferramenta de transcrição por IA usa dados de voz, estando, assim, sujeita a leis de privacidade biométrica"?

**Abigail Walker**
Associada – Tecnologias Emergentes
Reed Smith LLP

O estado de Illinois também chama a atenção para a intersecção entre a supervisão da IA e os direitos individuais em decisões trabalhistas.

Para as empresas, a resposta prática é conectar os requisitos legais à aquisição e configuração de ferramentas, às decisões com alto impacto e aos registros de supervisão antes que os problemas surjam.

“

Até 2027, Illinois deverá se consolidar como referência em governança de IA, com foco em adoção e prestação de contas. Com base em leis já existentes sobre IA em contratações, os empregadores lidarão com expectativas maiores de transparência, avaliação de vieses, explicação e contestação de decisões automatizadas. Ao mesmo tempo, a Lei de Medidas de Segurança para IA de Fronteira sinaliza uma mudança mais ampla em direção à segurança, exigindo que os desenvolvedores publiquem normas de mitigação de riscos, comuniquem incidentes significativos e se preparem para auditorias independentes a partir de 2028. Essas iniciativas reforçam uma abordagem responsável e centrada nas pessoas".

**Megan M. Miller**
Fundadora e advogada – Miller Mosaic
The Identity Counsel



# União Europeia: a implementação levanta a questão das evidências

A Lei de Inteligência Artificial da União Europeia entrou em vigor em 2024, com aplicação geral a partir de agosto de 2026. Seus requisitos priorizam a classificação de riscos, a documentação, a transparência e a supervisão.

As disposições do pacote legislativo Digital Omnibus para a IA, em vigor desde julho de 2026, revisaram os cronogramas. As exigências para sistemas de alto risco – incluindo aplicações em trabalho, educação e biometria – se aplicam a partir de 2 de dezembro de 2027. As regras para IA de alto risco incorporada a produtos entram em vigor em 2 de agosto de 2028.

As datas revisadas aumentam a clareza, embora ainda haja dúvidas sobre a prontidão das normas harmonizadas e das autoridades nacionais.

> **A mudança mais marcante na IA em 2027 será sua incorporação à infraestrutura. A IA já não é só objeto de disputa tecnológica, militar e energética entre EUA, Europa e China, mas está integrada a áreas como saúde, controle de fronteiras, mercado de trabalho, distribuição de recursos e ao cotidiano das pessoas.**
>
> **Mahdi Barkabian Zanjani**
> Profissional independente

A distinção entre obrigações existentes e adiadas é importante. Os requisitos do Regulamento Geral de Proteção de Dados da UE (GDPR), por exemplo, continuam se aplicando ao tratamento de dados pessoais.

As empresas precisam de avaliações e documentação que reflitam os sistemas em execução. Um modelo alterado, um novo provedor ou uma conexão ampliada podem reabrir questões aparentemente resolvidas em aprovações anteriores.



# Reino Unido: a legislação existente pode ter mais peso que uma nova lei de IA

O Reino Unido está seguindo um caminho diferente, sem uma Lei de IA abrangente que defina a abordagem regulatória. Os requisitos existentes de supervisão setorial e segurança cibernética podem gerar mudanças mais imediatas do que uma lei específica.

“

É pouco provável que o anunciado projeto de lei de IA do Reino Unido se concretize em 2027. No entanto, especula-se que o governo acrescentará medidas de segurança para a IA ao projeto de segurança cibernética e resiliência – relativas, por exemplo, à notificação de incidentes e à supervisão de prestadores de serviços gerenciados e operadores de data centers".

**Katie Hewson**
Sócia
Stephenson Harwood

Um projeto de lei de segurança cibernética e resiliência está em tramitação. Suas possíveis exigências devem ser diferenciadas dos requisitos de supervisão existentes.

Para empresas de setores regulados, a prioridade é entender como a IA altera as responsabilidades existentes de prestação de contas, supervisão de fornecedores, gestão de riscos e resiliência operacional. Esperar uma lei específica para a IA pode afetar o cumprimento dessas obrigações.

# Coreia do Sul: as políticas dão lugar às evidências operacionais

A Lei Básica de IA da Coreia do Sul entrou em vigor em 22 de janeiro de 2026. Sua aplicação gradual dá ênfase à implementação, especialmente à identificação de IA de alto impacto e à documentação dos controles aplicados previamente.

“

A carga mais subestimada provavelmente será a de inventariar e classificar sistemas. A IA está cada vez mais incorporada a softwares comuns e serviços de terceiros, e a regulação sul-coreana para IA de alto impacto abrange usos sensíveis, incluindo recrutamento, concessão de crédito, saúde, educação e decisões governamentais. O mais difícil será identificar a IA incorporada aos processos existentes e determinar os sistemas que requerem obrigações adicionais".

**Timothy Dickens**
Sócio
DR&AJU Law Group LLC

O requisito operacional vai da descoberta de sistemas à explicação sobre classificação, garantias selecionadas, supervisão humana e evidências de apoio.

# Brasil: o atraso na lei de IA não significa a ausência de regras

O abrangente marco regulatório proposto no Brasil para a IA – projeto de lei 2338/2023 – foi aprovado pelo senado em dezembro de 2024, mas ainda precisa passar por outras etapas de aprovação legislativa.

Leis existentes já regulamentam atividades envolvendo IA. A Lei Geral de Proteção de Dados Pessoais (LGPD) – em particular, o artigo 20, sobre decisões automatizadas – e o Código de Defesa do Consumidor incluem obrigações que as empresas não podem adiar enquanto uma legislação abrangente é desenvolvida.



> “
>
> As empresas precisam abandonar a abordagem de "esperar para ver" e construir arquiteturas de governança em torno das regras atuais – ou seja, a LGPD, as orientações da Agência Nacional de Proteção de Dados e as normas setoriais de proteção ao consumidor. A norma ISO/IEC 42001 pode comprovar processos de due diligence, mas não substitui obrigações legais nem elimina a responsabilidade por resultados prejudiciais da IA".

**Adriana Ruggeri Quinelo**
Assessora jurídica e consultora
Ruggeri Quinelo

A distinção é particularmente importante para organizações que se apoiam em normas de governança voluntárias. Certificações podem contribuir como evidências de diligência, mas não determinam se as decisões automatizadas estão em conformidade com a legislação.

# Diferentes regimes, questões de governança convergentes

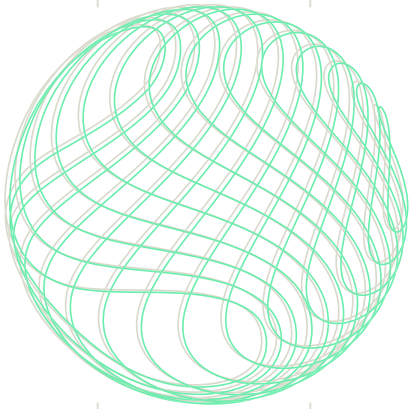
Essas jurisdições não estão convergindo para regras idênticas. Os especialistas apontam para algo mais útil: muitas das questões operacionais estão se tornando semelhantes.

**Descoberta:**

Sabemos onde a IA está sendo usada, incluindo recursos incorporados a softwares comuns e fornecidos por terceiros?

**Contexto:**

Sabemos quais pessoas, decisões, dados, processos comerciais e obrigações regulatórias podem ser afetados pela IA?



**Controle:**

A organização consegue demonstrar onde se aplicam as permissões, a intervenção humana, a transparência e as restrições?

**Evidências:**

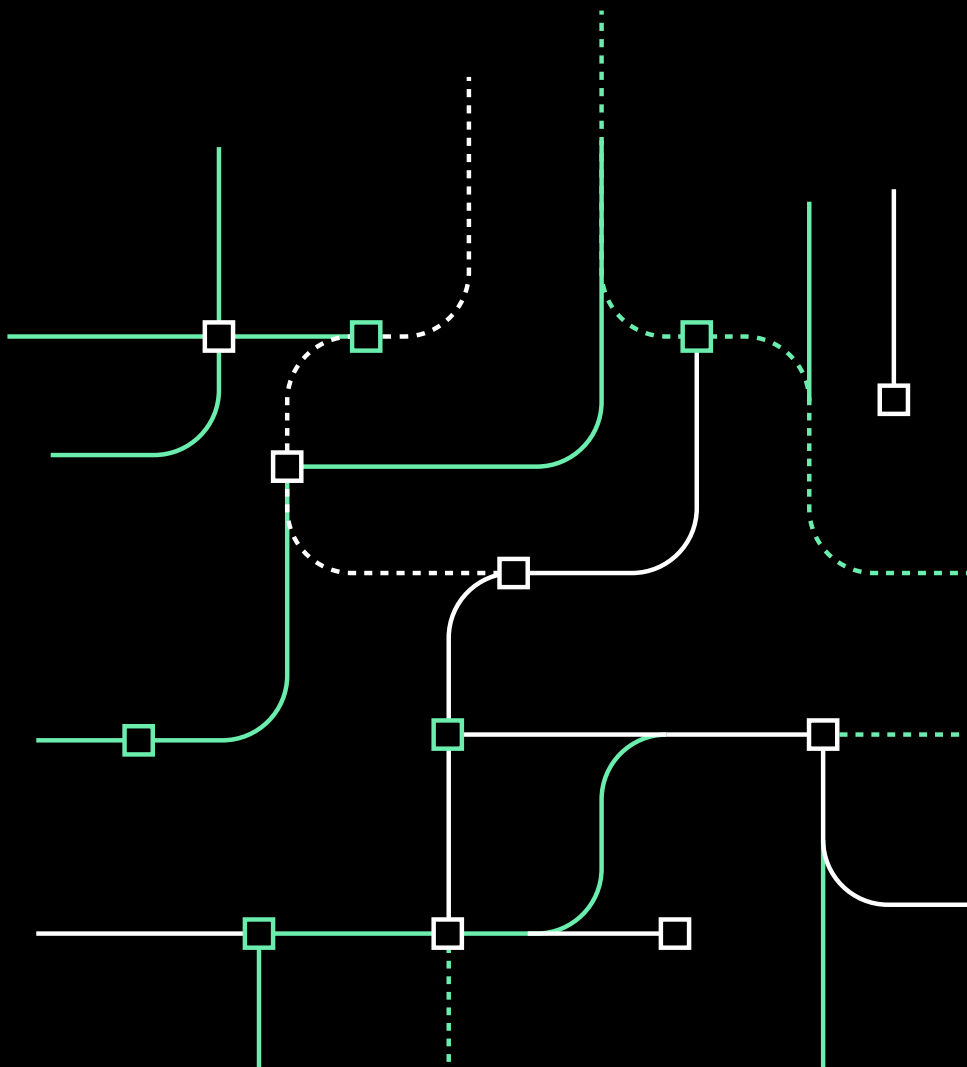
Conseguimos reconstruir o que foi avaliado, que sistema ou versão estava em operação, o que mudou, que controles foram aplicados e quem eram os responsáveis?

Essas capacidades permanecem relevantes mesmo quando os cronogramas regulatórios mudam. Elas permitem que uma organização responda quando uma nova regra entra em vigor, uma lei existente é aplicada à IA ou um órgão regulador pede informações.

As rotas jurídicas continuarão sendo diferentes. Os requisitos operacionais estão se tornando mais claros: a governança deve permanecer conectada à IA quando ela passa da aprovação para o uso.

# Contraprevisões:

## três coisas que *não* acontecerão em 2027



## Contraprevisão 1

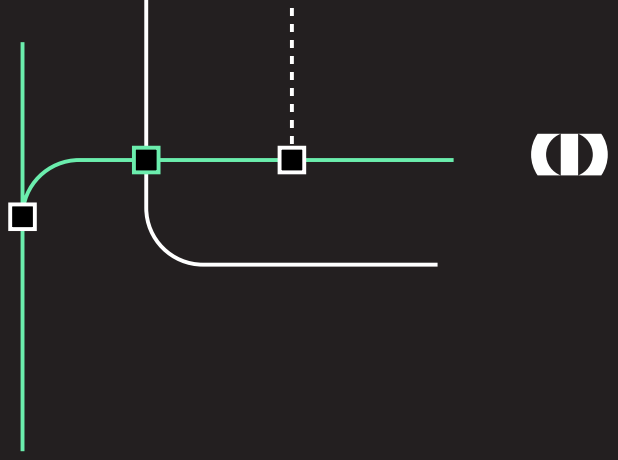
# Um nível básico de garantia não será suficiente para todas as decisões de implementação

Uma avaliação válida em seu escopo original pode deixar uma implementação que passou por mudanças sem a análise adequada. A questão é se as evidências ainda se aplicam ao recurso em questão, ao uso previsto e aos controles dos quais a aprovação depende.

> A certificação pode demonstrar diligência a reguladores, investidores e parceiros, mas não garante segurança jurídica. As empresas ainda precisam entender as leis e as obrigações setoriais aplicáveis aos sistemas de IA que implementam".

**Adriana Ruggeri Quinelo**
Assessora jurídica e consultora
Ruggeri Quinelo

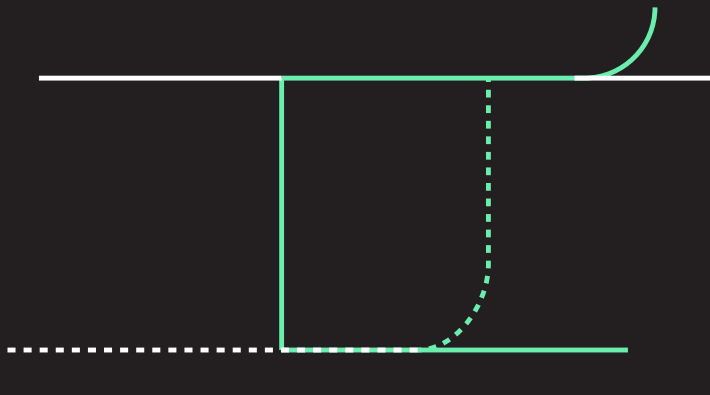
Um teste de penetração concluído em janeiro pode não abranger funcionalidades introduzidas em março. O mesmo princípio se aplica às premissas que fundamentam uma aprovação: uma nova conexão, uma autoridade mais ampla ou a redução da eficácia dos controles podem reabrir uma decisão, enquanto a garantia mais ampla permanece relevante.



> Um cliente pode aceitar a garantia de segurança para um serviço e ainda assim solicitar novos testes antes de habilitar uma funcionalidade alterada. A questão prática é saber se as evidências cobrem o que ele irá usar. As garantias existentes fornecem uma base, mas é preciso identificar o que mais a mudança exige".

**Tim Mullen**
Diretor de informação
OneTrust

Em 2027, as empresas ainda terão que determinar se as garantias existentes abrangem implementações de IA modificadas. A revisão adicional deverá se concentrar nas premissas reabertas pela alteração, mantendo as evidências relevantes.



## Contraprevisão 2

# Aumentar o número de profissionais não fará com que a supervisão se expanda na escala necessária

As empresas continuarão recorrendo ao julgamento humano em questões de políticas, decisões sensíveis e exceções. A expansão da ação dos agentes tornará mais difícil ter uma pessoa em cada etapa de execução.

A decisão operacional é determinar quando o julgamento humano é necessário e o que pode avançar sob as condições definidas. Em um fluxo de trabalho delimitado, pode ser viável exigir aprovação antes de cada ação de impacto. Em outro, pode ser necessário delegar uma autoridade mais limitada, com o encaminhamento a instâncias superiores em caso de mudanças.

O monitoramento automatizado também precisa ser avaliado. Os líderes devem testar se ele identifica desvios e permite uma intervenção eficaz.

O objetivo é ter a IA adequada no ritmo certo. O tempo entre a solicitação e a aprovação de uma funcionalidade pode revelar uma espera desnecessária. A qualidade das decisões e o tratamento de exceções e incidentes mostram se o processo é responsável.

> “
>
> A supervisão humana não acompanhará a escala que descrevemos. Acredito que o monitoramento será cada vez mais baseado em agentes. Isso mudará a supervisão e criará uma nova responsabilidade: avaliar o próprio sistema de monitoramento".

**Ojas Rege**
Vice-presidente – Produtos e Tecnologias Emergentes
OneTrust

> “
>
> À medida em que a IA é incorporada ao trabalho cotidiano, todos precisam entender como usá-la de forma responsável. O desafio é facilitar a governança e, ao mesmo tempo, garantir a segurança".

**Federico Sembolini**
Gerente – Transformação e Governança de IA
BBVA

O aumento das equipes não faz com que a análise humana opere na velocidade das máquinas. Um modelo de supervisão dependente da análise humana em cada ação não acompanha o ritmo de agentes conectados atuando em diferentes sistemas. As empresas precisam de limites efetivamente aplicáveis e de mecanismos de monitoramento que identifiquem a necessidade de julgamento humano. A contratação de profissionais pode reforçar a supervisão, mas não substitui a necessidade de mudar a forma como o trabalho é administrado.

## Contraprevisão 3

# Não teremos todas as certezas antes de tomar decisões

A promessa menos confiável sobre 2027 é saber exatamente o que está por vir.

Modelos serão modificados. Novos usos colocarão à prova decisões que pareciam definidas. Algumas projeções deste relatório se concretizarão mais rápido que o esperado; outras levarão mais tempo. O cenário de negócios também influenciará as soluções adotadas.

As empresas continuarão tendo que decidir sobre os usos de IA permitidos e os responsáveis pelas consequências.

Em 2027, muitas dessas decisões terão que ser tomadas sem evidências conclusivas sobre a próxima tecnologia ou modelo operacional. Ao aguardar um modelo de governança definitivo, as equipes manterão as aprovações e práticas já adotadas, mesmo com mudanças nas atividades.

> Não há uma resposta única. Com a pressão pelo uso da IA, o desafio é decidir quem é responsável pela governança e como ela deve funcionar na empresa".

**Bruna Baccini**
Chefe de conformidade e encarregada pela proteção de dados
GOL Airlines

> Não devemos ter medo das possibilidades da IA, mas também não devemos nos precipitar em relação ao que ela pode fazer. A tecnologia pode estar avançando na velocidade da luz, mas as pessoas precisam de tempo para mudar. Temos que pensar tanto no aspecto humano quanto na tecnologia".

**Aaron Weller**
Líder de inovação e garantia em privacidade
HP

A resposta prática é tornar as decisões passíveis de revisão. Uma aprovação deve especificar as condições que a mantêm válida e o que exigiria uma nova análise. Os líderes também precisam saber quem tem autoridade para alterar decisões quando essas condições deixam de se aplicar.

Arquitetar esse labirinto significa criar espaço para rever uma decisão sem deixar de assegurar a responsabilização por ela. O teste para as lideranças em 2027 será identificar se a empresa consegue alterar o grau de autoridade de um fluxo de trabalho de IA e, ainda assim, explicar quem aprovou uma alteração, o que ela permite e como interrompê-la.



www.onetrust.com

**Aviso legal**
Nenhuma parte deste documento pode ser reproduzida sem a permissão por escrito do proprietário dos direitos autorais. O conteúdo deste documento está sujeito a revisão sem aviso prévio, devido ao progresso contínuo na metodologia, design e produção. A OneTrust LLC não se responsabiliza por erros ou danos de qualquer tipo resultantes do uso deste documento. Os produtos, o conteúdo e os materiais da OneTrust têm finalidade unicamente informativa, e não de aconselhamento jurídico. Entre em contato com sua assessoria jurídica para obter aconselhamento em relação a questões legais. Os materiais da OneTrust não garantem a conformidade com as leis e regulamentos aplicáveis.

Direitos autorais: © 2026 OneTrust LLC. Todos os direitos reservados. Informação proprietária e confidencial.