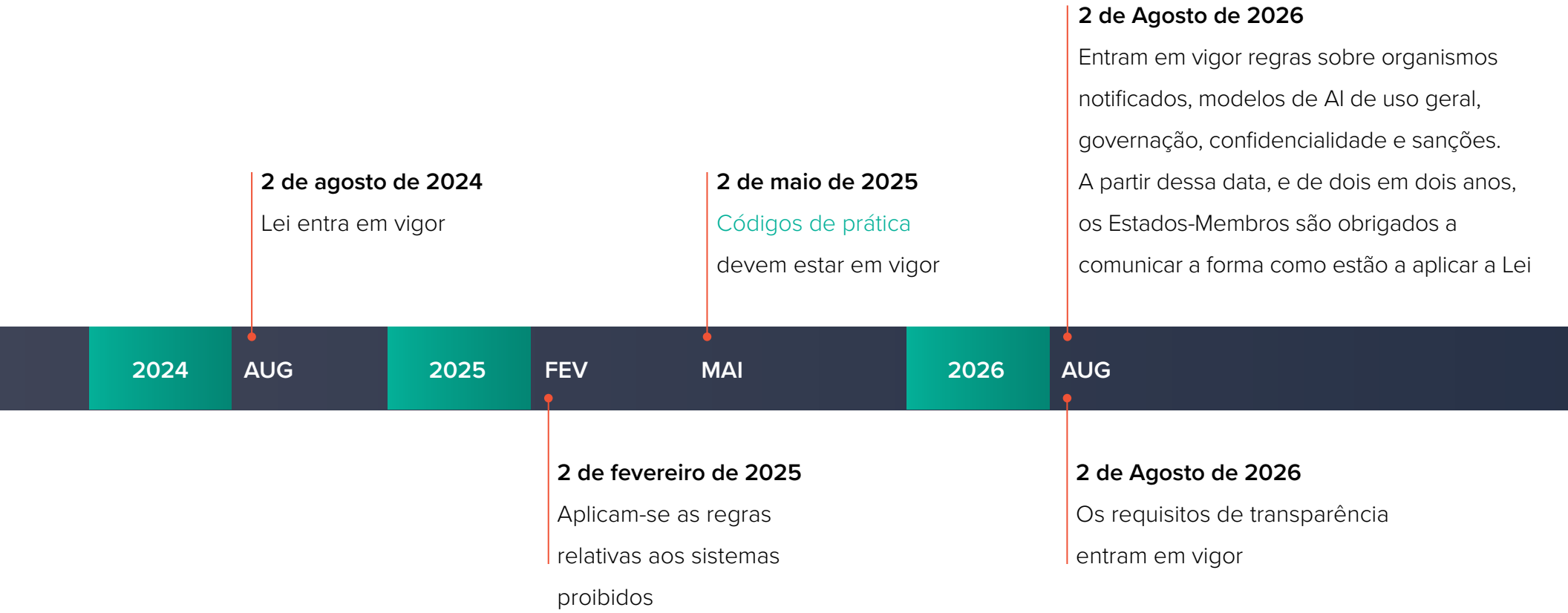
Preparação para o Regulamento Europeu sobre a IA

Barracuda

O Regulamento de Inteligência Artificial (IA) da União Europeia aplica-se a implementadores, fornecedores e importadores de sistemas de IA. O impacto total do Ato decorre num cronograma escalonado — conforme indicado abaixo — pelo que poderá ter de tomar medidas agora. As regulamentações visam tornar os sistemas de AI seguros, transparentes, não discriminatórios e ambientalmente amigáveis. O Ato também exige supervisão humana para evitar resultados prejudiciais para os indivíduos.

Embora os controlos sejam mais onerosos para as empresas que constroem e vendem sistemas de AI, continua a haver um impacto nas organizações que utilizam esses sistemas. No mínimo, a Lei pode significar que tem de confirmar que os seus fornecedores estão devidamente conformes. Na pior das hipóteses, pode significar repensar essas relações ou trabalhar com parceiros para garantir que os seus sistemas e dados estão preparados para cumprir os novos requisitos.



2 de agosto de 2024
Lei entra em vigor

2 de fevereiro de 2025
Aplicam-se as regras relativas aos sistemas proibidos

2 de maio de 2025
Códigos de prática devem estar em vigor

2 de Agosto de 2026
Os requisitos de transparência entram em vigor

2 de Agosto de 2026
Entram em vigor regras sobre organismos notificados, modelos de AI de uso geral, governação, confidencialidade e sanções. A partir dessa data, e de dois em dois anos, os Estados-Membros são obrigados a comunicar a forma como estão a aplicar a Lei

Antecedentes e regulamentos adicionais

A União Europeia criou um quadro para a regulamentação da AI em 2021. A lei estabelece níveis de risco que os sistemas de AI podem representar para os cidadãos e prevê níveis de regulamentação que correspondem a esse nível de risco. Os sistemas que apresentem níveis de risco inaceitáveis - como os sistemas que recorrem à manipulação cognitivo-comportamental ou à pontuação social - enfrentam uma proibição total a partir de 2 de fevereiro de 2025. Os sistemas de identificação biométrica em tempo real serão igualmente proibidos, exceto em casos de aplicação limitada da lei. A biometria pós-evento para identificar suspeitos só será permitida para ajudar na perseguição de crimes graves e requererá autorização judicial.

A quem a Lei se aplica

Fornecedores — Qualquer pessoa que coloque produtos que utilizam AI no mercado na UE, independentemente de o fornecedor estar localizado dentro ou fora da UE e de o produto ser gratuito ou pago. Exemplos incluem empresas que criam modelos de AI de uso geral, bem como empresas que criam e oferecem produtos, como chatbots, que se baseiam nestes modelos de AI de uso geral.

Deployers — Qualquer pessoa que use AI em conexão com um negócio e não apenas uma atividade pessoal. Um exemplo de implementador pode ser uma instituição financeira que usa um chatbot alimentado por AI para responder àsperguntas dos clientes.

Importadores — Qualquer pessoa localizada ou estabelecida na UE que coloque no mercado um sistema de AI que porte o nome ou marca de uma pessoa singular ou coletiva estabelecida num país terceiro.

Como a Lei é aplicada

O Ato define quatro categorias de sistemas de AI, do nível de risco mais alto ao mais baixo — risco inaceitável, risco alto, risco limitado e risco mínimo. A partir de 2 de fevereiro de 2025, o Ato proíbe qualquer sistema de AI descrito como representando um risco inaceitável, incluindo:

- Sistemas de AI que utilizam técnicas subliminares para alterar o comportamento das pessoas.
- Qualquer sistema de AI que classifique pessoas de acordo com o comportamento social que leve a um tratamento prejudicial ou desfavorável.
- Perfis de sistemas de IA que preveem a probabilidade de uma pessoa cometer uma infração criminal.

A segunda categoria – sistemas de AI de alto risco – inclui aqueles utilizados em produtos abrangidos pela regulamentação de segurança da UE em vigor, como brinquedos, aviação, automóveis, dispositivos médicos e elevadores.

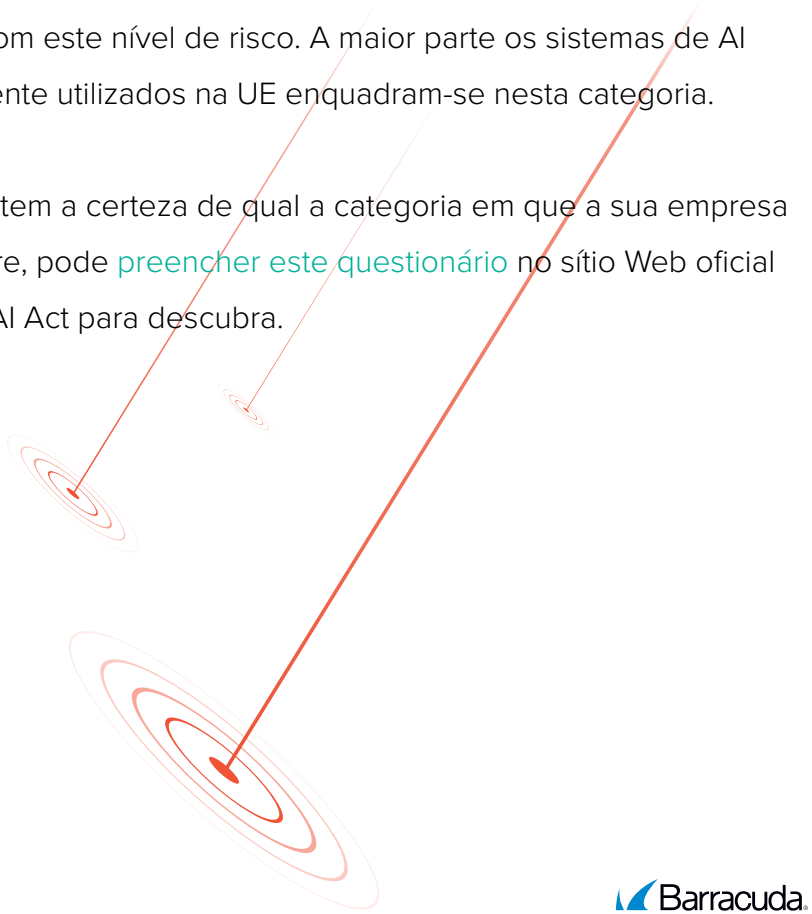
Os sistemas de alto risco terão de ser registados numa base de dados da UE e incluem tudo o que esteja relacionado com a gestão de infraestruturas críticas, educação e formação profissional, gestão de trabalhadores, aplicação da lei, controlo das fronteiras e migração, e sistemas de asilo. Todos eles necessitarão de uma avaliação inicial e de verificações contínuas ao longo da sua implantação e ciclo de vida. Os cidadãos terão o direito de apresentar queixas sobre esses sistemas às autoridades nacionais designadas responsáveis pela aplicação da nova lei.

Mas é a terceira categoria – sistemas de risco limitado – que tem mais probabilidades de criar problemas para os utilizadores empresariais dos sistemas de AI mais comuns. Os produtos de AI generativa, como o ChatGPT, devem cumprir a legislação da UE em matéria de direitos de autor e seguir as novas regras de transparência.

Estas incluem a rotulagem clara de qualquer conteúdo gerado por AI, quer seja visual, de texto ou áudio. Os criadores de serviços de AI generativa são obrigados a conceber modelos para garantir que não geram conteúdos ilegais.

A categoria final - sistemas de risco mínimo - abrange aplicações que envolvem o processamento básico de dados, como filtros de spam ou jogos de vídeo com AI. Esta categoria de risco não é regulamentada. O Ato da AI permite a utilização livre de sistemas de AI com este nível de risco. A maior parte os sistemas de AI atualmente utilizados na UE enquadram-se nesta categoria.

Se não tem a certeza de qual a categoria em que a sua empresa se insere, pode preencher este questionário no sítio Web oficial do EU AI Act para descubra.



O que precisa de fazer — Quatro passos para a conformidade

O esforço de conformidade será diferente consoante a categoria de AI que a sua empresa utiliza nos seus produtos e atividades. Controlar a conformidade deve trazer outros benefícios para a sua organização.

Em primeiro lugar, tem de especificar exatamente quais os produtos que contêm AI e sistemas de AI (por exemplo, ChatGPT; Llama, etc.) que estão a ser utilizados na sua empresa, quem os utiliza e com que finalidade. Isto deve ser enquadrado como um mero exercício de recolha de informação e não como um programa de conformidade. Certifique-se de que nada do que está em utilização se enquadra na categoria de risco inaceitável. Esta etapa traz os maiores benefícios potenciais e pode fornecer uma ótima base para construir uma melhor visão estratégica do uso da AI pela organização.

O segundo passo é avaliar quais as alterações que terá de fazer nesses sistemas para alcançar a conformidade. Pense na avaliação dos riscos, na verificação de preconceitos e na formação do pessoal. Também precisa de pensar nos seus fornecedores. Se terceirizar partes do recrutamento, verifique se a seleção de CV está a ser feita com assistência de AI. As equipas de marketing estão a utilizar a AI para gerar textos ou imagens?

Em terceiro lugar, pense em implementar sistemas para continuar e documentar essa monitorização ao longo do tempo, à medida que as regulamentações e o uso de AI pela organização mudam. Os fornecedores previamente aprovados podem adicionar AI a uma funcionalidade, por isso certifique-se de avaliar essa nova funcionalidade antes de as pessoas começarem a utilizá-la. Os modelos estão a evoluir rapidamente, pelo que mesmo que não esteja a introduzir novos sistemas, precisa de estar ciente das alterações que possam afetar a sua avaliação de riscos. Se estiver baseado no Reino Unido, poderá ter de lidar com diferentes regulamentos num futuro próximo.

E, em quarto lugar, agora você tem os dados de que precisa para criar, ou atualizar, sua Política de Uso de AI. Que verificações e proteções você precisa para ajudar a equipe a fazer o melhor uso da AI? Como incentivar a inovação e, ao mesmo tempo, minimizar os riscos? Que regras precisa para os seus parceiros e fornecedores?

Categorias diferentes, requisitos diferentes

Cada categoria de risco diferente tem as suas próprias responsabilidades em termos de conformidade, que também exigem ações para além das etapas acima descritas.

Os sistemas de alto risco têm de cumprir os requisitos estabelecidos no Capítulo 3, Secção 2 de a EU AI Act, intitulada Requirements for High-Risk AI Systems. Este capítulo abrange obrigações como a gestão do risco, a manutenção de registos e a necessidade de supervisão humana.

Os sistemas de risco limitado devem fornecer aos utilizadores divulgações de transparência e informá-los se e quando estão a interagir, por exemplo, com um chatbot de AI. Leia o artigo 50 do Regulamento Europeu sobre a AI para mais pormenores sobre as obrigações dos sistemas de risco limitado.

Os sistemas de risco mínimo não requerem qualquer ação de conformidade, mas é importante ter a certeza de que os sistemas da sua empresa se enquadram nesta categoria.

Aproveite a oportunidade oferecida

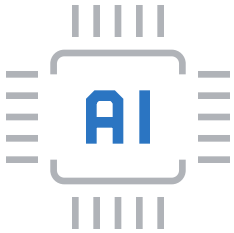
Embora seja principalmente uma questão de conformidade, a introdução das novas regulamentações oferece uma oportunidade de obter algum benefício empresarial.

As organizações devem aproveitar este tempo para auditar quanto das suas operações já utilizam AI. Independentemente de essa utilização de AI não se enquadrar nos regulamentos futuros, estes casos de uso podem ainda representar riscos potenciais para a sua organização ou empresa.

Um risco que precisa compreender é a "AI sombra" — o uso não autorizado de ferramentas de AI por utilizadores finais dentro de uma organização sem aprovação ou supervisão dos departamentos de compras ou TI. Assim como o uso da cloud, a AI precisa ser usada em toda a empresa de forma segura, protegida e económica, em Conformidade com as leis aplicáveis e com supervisão estratégica adequada. Os departamentos de compras, TI, jurídico e segurança precisam conhecer e entender como as pessoas estão a usar os recursos da empresa para utilizar a AI. Esses departamentos devem colaborar com outras funções da empresa para criar e implementar uma Política de Uso de AI.

Dada a rapidez com que os sistemas de AI e os regulamentos aplicáveis estão a evoluir, é benéfico rever anualmente a sua Política de Utilização de AI.

O uso da AI não é apenas um desafio de segurança mas também uma fonte de potencial vantagem comercial. As práticas de melhor utilização podem ser partilhadas entre departamentos para tornar todo o negócio mais consciente da AI e fluente. Com muitas organizações a lutar para encontrar benefícios comerciais ou demonstrar retorno sobre investimento de gastos com AI, saber exatamente quem está a fazer o que é crucial.



Barracuda

Construir para o futuro

Esperamos que este processo tenha proporcionado alguns conhecimentos interessantes sobre o ponto em que a sua organização se encontra no seu percurso de AI. Deveria ter mostrado quais as partes da empresa que estão a utilizar melhor a AI e como podem ajudar outros departamentos.

Pode também ter destacado algumas áreas de fraqueza onde a melhoria da formação do pessoal, o acesso a ferramentas e os guias de best practice poderiam aumentar e melhorar a eficácia da utilização da AI.

Por último, é importante que encare este processo como um processo contínuo. A AI está a evoluir a um ritmo vertiginoso, por isso precisa de revisitar regularmente os quatro estágios da Conformidade. As sanções disponíveis para os reguladores incluem multas substanciais, pelo que é fundamental compreender a utilização da AI nos produtos da sua empresa.

Leitura complementar

O Parlamento Europeu escreveu um resumo claro e de bom senso da Lei.

Para ir mais fundo, a Act tem o seu próprio website com orientação completa Conformidade.

Sobre a Barracuda

A Barracuda é uma empresa global de cibersegurança líder, que oferece proteção completa contra ameaças complexas para empresas de todos os tamanhos. A nossa plataforma BarracudaONE, potenciada por IA, protege e-mail, dados, aplicações e redes com soluções inovadoras, XDR gerido e um painel de controlo centralizado para maximizar a proteção e reforçar a resiliência cibernética. Confiada por centenas de milhares de profissionais de TI e provedores de serviços geridos em todo o mundo, a Barracuda oferece defesas poderosas que são fáceis de comprar, implantar e usar. Para mais informações, visite pt.barracuda.com.