

Guia de preparação EXIN AI Compliance

Tudo o que a prova cobra, organizado por domínio: conceitos-chave, comparações que confundem, pegadinhas reais, gatilhos do enunciado, questões comentadas e um plano para chegar pronto ao exame.

6
capítulos por domínio

36
questões comentadas

65%
nota de corte

6
provas completas no curso

ANTES DE COMEÇAR

Como usar este guia

Este guia foi feito para ser estudado junto com as 6 provas completas do curso EXIN AI Compliance: o guia explica o que cai e onde estão as armadilhas; as provas treinam o ritmo e mostram o que você ainda não domina.

Quando	O que fazer
Semana 1	Faça o teste diagnóstico (página seguinte) e leia os capítulos 1 e 2. No fim da semana, faça a Prova 1 do curso no tempo do exame.
Semana 2	Leia os demais capítulos, começando pelos domínios em que você errou mais no diagnóstico. Faça as provas 2 e 3.
Semana 3	Releia os alertas de pegadinha e as tabelas de comparação. Faça as provas 4 e 5 e revise cada erro pela explicação.
Semana 4	Estude a folha de cola, faça a Prova 6 e refaça as provas abaixo de 80%. Agende o exame quando estiver acima de 80% em todas (a nota de corte é 65%).

Mapa do exame

Cada prova do curso tem 40 questões e 90 minutos, no formato do exame. Referência de aprovação: 65%.

Domínio (capítulo)	Peso	Neste guia
1. Domínio 1: Contexto da Lei da IA (AI Act)	—	16 conceitos · 14 pegadinhas
2. Domínio 2: Lei da IA detalhada	37,5%	18 conceitos · 14 pegadinhas
3. Domínio 3: IA confiável	12,5%	17 conceitos · 14 pegadinhas
4. Domínio 4: IA ética	10%	16 conceitos · 14 pegadinhas
5. Domínio 5: Lei da IA na prática	15%	17 conceitos · 14 pegadinhas
6. Domínio 6: Diretrizes para apoiar a conformidade	20%	17 conceitos · 14 pegadinhas

Como ler os capítulos: os **tópicos-chave** são o que mais cai; a **tabela de memorização** separa o que a prova costuma confundir; os **alertas de prova** mostram as armadilhas das alternativas erradas; os **gatilhos** ligam palavras do enunciado à resposta; e o **checklist** diz se você está pronto para o domínio.

Estude um pouco todo dia, de graça

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o “não confunda” de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

DIAGNÓSTICO

Você já sabe isso?

Responda às 12 questões sem consultar nada. As respostas, com a explicação e o capítulo para revisar, estão no fim do guia. Comece o estudo pelos capítulos em que errou.

D1 · Domínio 1: Contexto da Lei da IA (AI Act)

Um importador vai colocar no mercado da UE um sistema de IA de risco elevado desenvolvido por um fornecedor estrangeiro. O que o AI Act exige que ele verifique antes?

A. Treinamento do sistema com dados coletados na própria UE
B. Filial do fornecedor aberta em algum Estado-Membro da UE
C. Auditoria prévia do código-fonte por uma universidade europeia credenciada
D. Avaliação de conformidade, documentação, marcação CE e representante

D2 · Domínio 1: Contexto da Lei da IA (AI Act)

Uma empresa sediada em Portugal compra de um fabricante coreano sistemas de IA com a marca do fabricante e é a primeira a colocá-los no mercado da UE. Outra empresa, na Espanha, compra esses sistemas da portuguesa e os revende. Quais são os papéis no AI Act?

A. As duas são importadoras, por venderem sistemas de fora
B. A portuguesa é distribuidora e a espanhola é importadora
C. A portuguesa é importadora e a espanhola é distribuidora
D. As duas são fornecedoras, por colocarem o sistema à venda

D3 · Domínio 1: Contexto da Lei da IA (AI Act)

Um fornecedor europeu desenvolve um sistema de IA de reconhecimento de alvos destinado exclusivamente às forças armadas de um Estado-Membro. Como o AI Act se aplica?

A. Aplica-se só se o sistema for exportado depois para fora da União Europeia
B. Aplica-se como prática proibida, por permitir o uso de força letal pelo Estado
C. Aplica-se como risco elevado, por envolver identificação de pessoas e de objetos
D. Não se aplica, pois sistemas de uso exclusivamente militar estão fora do âmbito

D4 · Domínio 2: Lei da IA detalhada

Uma engenheira de um fornecedor de IA quer denunciar à autoridade competente uma violação da Lei da IA cometida pelo empregador. Que norma da União o Art. 87 manda aplicar à denúncia e à proteção de quem denuncia?

A. O Regulamento (UE) 2019/1020, sobre fiscalização
B. A Diretiva (UE) 2019/790, sobre direitos autorais
C. A Diretiva (UE) 2019/1937, sobre denunciantes
D. O Regulamento (UE) 2016/679, o GDPR

D5 · Domínio 2: Lei da IA detalhada

Um fornecedor concluiu com sucesso a avaliação de conformidade de um sistema de IA de risco elevado. O que ele deve emitir ou aplicar antes de colocar o sistema no mercado da UE?

A. Certificado de auditoria financeira anual
B. Licença de operação emitida pelo Gabinete de IA
C. Declaração UE de conformidade e marcação CE
D. Selo voluntário de IA ética da Comissão

D6 · Domínio 2: Lei da IA detalhada

Um fornecedor de sistema de IA de risco elevado já no mercado descobre que o sistema apresenta risco à saúde de um grupo de usuários, embora tenha passado na avaliação de conformidade. O que o artigo 20 exige dele?

A. Deixar ao distribuidor a decisão de comunicar o risco, por ser ele quem vende o sistema
B. Registrar o risco no sistema de gestão da qualidade e esperar a próxima auditoria interna
C. Suspender as vendas em toda a UE e aguardar instruções da Comissão antes de agir
D. Investigar as causas e informar as autoridades de fiscalização do mercado competentes

D7 · Domínio 3: IA confiável

Um portal de notícias da Bélgica publica textos sobre as eleições municipais redigidos por IA. Um editor revisa cada texto antes da publicação, e o portal assume a responsabilidade editorial pelo conteúdo. Pelo Art. 50(4) da Lei da IA, o portal precisa divulgar que os textos foram gerados por IA?

A. Não, porque o texto passou por revisão humana e há responsabilidade editorial pela publicação
B. Não, porque o dever de divulgação do Art. 50(4) abrange imagens, áudio e vídeo, mas não textos
C. Sim, mas basta um aviso discreto no rodapé, como o previsto para obras artísticas e satíricas
D. Sim, porque o dever de divulgar textos de interesse público só admite a exceção de investigação penal

D8 · Domínio 3: IA confiável

O fornecedor de um sistema de IA de risco elevado para triagem de candidatos a emprego quer tratar dados sobre origem étnica para detectar e corrigir vieses do modelo, com base no Art. 4a da Lei da IA (versão consolidada). Qual condição faz parte das exigências cumulativas desse artigo?

A. Obter autorização prévia do Gabinete de IA, que avalia se o tratamento é estritamente necessário
B. Conservar os dados com a documentação técnica por dez anos, para eventual pedido da fiscalização
C. Compartilhar os dados com um auditor externo independente, que confirma a correção do viés detectado
D. Demonstrar que a detecção não pode ser feita com outros dados, como dados sintéticos ou anonimizados

D9 · Domínio 3: IA confiável

Uma rede de academias em Viena lança um aplicativo com IA que trata vários dados de seus alunos. Qual desses dados pertence às categorias especiais de dados pessoais do GDPR?

A. E-mail profissional no formato nome.sobrenome usado para enviar avisos sobre as aulas
B. Impressão digital usada para identificar de forma única cada aluno na catraca de entrada
C. Endereço IP e identificador de cookie usados para medir os acessos ao aplicativo da rede
D. Dados de localização do celular usados para sugerir ao aluno as unidades mais próximas

D10 · Domínio 4: IA ética

Um fornecedor de sistema de IA de risco elevado para um serviço público de emprego entrega uma interface que leitores de tela não conseguem usar e que exige visão perfeita para ler os resultados. Que requisito do HLEG e que obrigação do fornecedor na Lei da IA estão em jogo?

A. Bem-estar social e ambiental (impacto na sociedade); Art. 16(l), sobre consumo de energia
B. Robustez técnica e segurança (confiabilidade); Art. 15, sobre resiliência contra falhas de interface
C. Ação e supervisão humanas (controle humano); Art. 14, sobre interface para interromper o sistema
D. Diversidade, não discriminação e equidade (acessibilidade e desenho universal); Art. 16(l)

D11 · Domínio 4: IA ética

Uma empresa de saúde desenvolve um sistema de IA de risco elevado para apoio ao diagnóstico e quer usar as Orientações Éticas para uma IA de Confiança da Comissão como referência interna. Qual é o uso adequado dessas orientações?

A. Estruturar a governança interna com elas, cumprindo à parte os requisitos legais do AI Act
B. Substituir a verificação dos requisitos do AI Act pela autoavaliação baseada nas orientações
C. Tratar as orientações como norma harmonizada, que dá presunção de conformidade ao sistema
D. Restringir as orientações a projetos de pesquisa acadêmica, sem uso em ambiente industrial

D12 · Domínio 4: IA ética

Uma associação de defesa do consumidor da Grécia, que não foi afetada diretamente, suspeita que uma rede de supermercados usa um sistema de IA que viola a Lei da IA. Pelo Art. 85, qual via a associação tem?

A. Reclamar ao fornecedor, que encaminha a queixa à autoridade competente em até 15 dias
B. Apresentar reclamação à autoridade de fiscalização do mercado, como qualquer pessoa física ou jurídica
C. Reclamar só depois de provar que algum associado foi afetado por uma decisão do sistema
D. Apresentar reclamação ao Gabinete de IA, que é competente para queixas sobre sistemas de IA

01

CAPÍTULO 1

Domínio 1: Contexto da Lei da IA (AI Act)

Aqui eu preciso dominar o objetivo da Lei da IA, o seu âmbito (quem e o que fica dentro ou fora) e os papéis da cadeia: fornecedor, responsável pela implantação, importador, distribuidor e representante autorizado. O domínio pesa só 5% (2 questões por prova), mas é a base de todo o resto: sem identificar o papel e o âmbito, não acerto as obrigações do Domínio 2. As questões vêm em cenário curto, com uma empresa, um país e um uso, e pedem se a lei se aplica e quem é quem. Onde mais erro: trocar importador por distribuidor, achar que sede ou servidor fora da UE tira o sistema da lei e esquecer as exclusões (militar, pesquisa científica, uso pessoal).

Neste capítulo
16 tópicos-chave · 14 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Regulamento da UE (forma jurídica da Lei da IA)

Regulamento tem aplicação direta e uniforme em todos os Estados-Membros, sem lei nacional de transposição, ao contrário da diretiva. Por isso a Lei da IA cria as mesmas regras em todo o mercado europeu; aos países cabe designar autoridades e definir detalhes como o regime de sanções.

Objetivo da Lei da IA (Art. 1)

Melhorar o funcionamento do mercado interno e promover uma IA centrada no ser humano e confiável, com elevado nível de proteção da saúde, da segurança e dos direitos fundamentais da Carta, apoiando a inovação. O meio é graduar as obrigações pelo risco: práticas proibidas, risco elevado, deveres de transparência e risco mínimo.

Sistema de IA (Art. 3)

Sistema baseado em máquina, projetado para operar com níveis variados de autonomia, que pode se adaptar após a implantação e que infere, a partir das entradas, como gerar resultados (previsões, conteúdos, recomendações ou decisões). A definição é neutra quanto à técnica e não depende de onde roda; software de regras fixas definidas por pessoas fica fora.

Âmbito territorial (Art. 2(1))

A lei alcança fornecedores que colocam sistemas no mercado ou em serviço na UE, estejam na União ou num país terceiro; responsáveis pela implantação estabelecidos na UE; e fornecedores e responsáveis pela implantação de países terceiros quando o resultado do sistema é usado na UE. O local de treino, de operação ou dos servidores não define o âmbito.

Exclusão militar, de defesa e de segurança nacional (Art. 2(3))

Ficam fora os sistemas colocados no mercado, em serviço ou usados exclusivamente para fins militares, de defesa ou de segurança nacional, seja a entidade pública ou privada (considerando 24). Esse uso fica regido pelo direito internacional público. A exclusão depende da finalidade exclusiva, não da técnica nem de exportação.

Exclusão de pesquisa científica (Art. 2(6) e 2(8))

Sistemas e modelos, incluindo seus resultados, desenvolvidos e colocados em serviço para o único fim de pesquisa e desenvolvimento científico ficam fora. O Art. 2(8) também exclui pesquisa, teste e desenvolvimento antes da colocação no mercado, mas não os testes em condições reais. Publicar os resultados não coloca o modelo no mercado; oferecê-lo no mercado, sim.

Uso pessoal não profissional (Art. 3(4) e 2(10))

Quem usa IA numa atividade puramente pessoal e não profissional não tem as obrigações de responsável pela implantação. Compartilhar o resultado com a família não muda isso. O fornecedor do aplicativo, porém, continua com as suas obrigações, como marcar o conteúdo sintético (Art. 50(2)).

Código aberto (Art. 2(12))

Sistemas lançados sob licença livre e de código aberto ficam fora da Lei da IA, salvo se colocados no mercado ou em serviço como risco elevado, como prática do Art. 5 ou como sistema sujeito ao Art. 50. Número de usuários, gratuidade e local do repositório não são critérios.

Fornecedor

Quem desenvolve ou manda desenvolver um sistema de IA e o coloca no mercado ou em serviço com o seu próprio nome ou marca, como o fabricante estrangeiro que vende sob a sua marca. É o papel que concentra as obrigações de conformidade do sistema de risco elevado.

Responsável pela implantação (Art. 3(4))

Quem usa um sistema de IA sob a sua autoridade, exceto em atividade pessoal não profissional. Pode ser empresa privada ou autoridade pública; uma autoridade que usa o sistema de terceiro é responsável pela implantação, não fornecedora.

Importador (Art. 3(6)) e distribuidor (Art. 3(7))

Importador é a pessoa estabelecida na UE que coloca no mercado um sistema com nome ou marca de pessoa de país terceiro: é a primeira entrada na União. Distribuidor é quem, na cadeia, sem ser fornecedor nem importador, disponibiliza o sistema no mercado, como quem compra do importador e revende. Todos são operadores (Art. 3(8)), com obrigações próprias (Arts. 23 e 24).

Obrigações do importador (Art. 23)

Antes de colocar no mercado um sistema de risco elevado, o importador verifica se o fornecedor fez a avaliação de conformidade, elaborou a documentação técnica, aplicou a marcação CE, acompanhou o sistema da declaração UE de conformidade e das instruções de uso e nomeou representante autorizado. Se suspeitar de não conformidade, não coloca o sistema no mercado.

Representante autorizado (Art. 22)

O fornecedor estabelecido fora da UE nomeia, por mandato escrito e antes de disponibilizar o sistema de risco elevado, um representante estabelecido na União. Ele verifica a declaração UE de conformidade e a documentação técnica, mantém informações à disposição das autoridades por 10 anos, coopera com elas e, quando aplicável, faz o registro do Art. 49(1). Não se exige filial nem transferência de propriedade intelectual.

Mudança de papel na cadeia (Art. 25)

Distribuidor, importador, responsável pela implantação ou terceiro passa a ser considerado fornecedor de um sistema de risco elevado quando põe nele o seu nome ou marca, faz uma modificação substancial ou muda a finalidade de modo que ele se torne de risco elevado. Assume então as obrigações de fornecedor, como avaliação de conformidade e documentação.

Relação com GDPR e DSA (Art. 2(5) e 2(7))

A Lei da IA complementa o direito da UE: não afeta o GDPR nem as demais regras de proteção de dados (Art. 2(7)) e preserva as regras de responsabilidade dos prestadores intermediários do DSA (Art. 2(5)). Um mesmo sistema pode ter de cumprir as três normas ao mesmo tempo; a Lei da IA não é norma residual nem substituta.

Calendário de aplicação (Art. 113)

Publicação no Jornal Oficial em 12 de julho de 2024 e entrada em vigor em 1 de agosto de 2024. Disposições gerais, letramento em IA e práticas proibidas valem desde 2 de fevereiro de 2025; regras de modelos de finalidade geral, governança e sanções desde 2 de agosto de 2025; aplicação geral desde 2 de agosto de 2026. Duas proibições incluídas pelo Omnibus Digital valem a partir de 2 de dezembro de 2026.

Macetes para memorizar

Papéis da cadeia

Fornecedor FAZ, responsável pela implantação USA, importador TRAZ, distribuidor REPASSA, representante RESPONDE.

Âmbito territorial

Vale onde o sistema entra no mercado ou onde o resultado é usado, não onde o servidor está.

Exclusões do âmbito

Fora pela finalidade exclusiva: Militar (ou defesa e segurança nacional), Pesquisa científica e uso Pessoal não profissional. Código aberto fica fora só com ressalvas: volta se for risco elevado, Art. 5 ou Art. 50.

Calendário

Fev/25 proíbe, Ago/25 GPAI e multas, Ago/26 tudo, Dez/26 as duas proibições do Omnibus.

Art. 25

Pôs a marca, mexeu fundo ou mudou a finalidade: virou fornecedor.

Regulamento x diretiva

Regulamento Roda direto; Diretiva Depende de transposição.

Tabela de memorização: não confunda

Quando é...	...e quando é
Regulamento Aplica-se direto em todos os Estados-Membros, sem transposição: é a forma da Lei da IA.	**Diretiva** Precisa de lei nacional de transposição para produzir efeito.
Importador Estabelecido na UE e é o primeiro a colocar no mercado da União um sistema com marca de país terceiro.	**Distribuidor** Compra de quem já colocou o sistema no mercado e o revende ou disponibiliza, sem alterá-lo nem pôr sua marca.
Fornecedor Desenvolve ou manda desenvolver e coloca no mercado com seu nome ou marca; responde pela conformidade do sistema.	**Responsável pela implantação** Usa o sistema sob sua autoridade, em atividade profissional; a autoridade pública que usa sistema de terceiro está aqui.
Pesquisa científica exclusiva (Art. 2(6)) e testes antes do mercado (Art. 2(8)) Fora da Lei da IA enquanto a finalidade for só pesquisa e desenvolvimento.	**Testes em condições reais** Continuam dentro da lei: a exclusão do Art. 2(8) não os cobre.
Representante autorizado Nomeado por mandato escrito do fornecedor de fora da UE para responder perante as autoridades e guardar informações.	**Importador** Operador que coloca no mercado o sistema com marca estrangeira e verifica, antes, a conformidade feita pelo fornecedor.

Uso pessoal não profissional A pessoa física fica sem obrigações de responsável pela implantação (Art. 2(10)).	**Fornecedor do aplicativo usado** Mantém suas obrigações, como a marcação de conteúdo sintético do Art. 50(2).

Números que caem

Item	Valor
Publicação no Jornal Oficial	**12 de julho de 2024**
Entrada em vigor	**1 de agosto de 2024**
Proibições do Art. 5 e letramento em IA	**desde 2 de fevereiro de 2025**
Regras de modelos de finalidade geral, governança e sanções	**desde 2 de agosto de 2025**
Aplicação geral do regulamento	**2 de agosto de 2026**
Duas proibições incluídas pelo Omnibus Digital	**a partir de 2 de dezembro de 2026**
Guarda de informações pelo representante autorizado	**10 anos**
Peso do domínio	**5% (2 questões em 40)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** A Lei da IA precisa ser transposta por lei nacional em cada Estado-Membro.
Como não cair: É regulamento: aplica-se diretamente. Transposição é coisa de diretiva.

⚠ **Alerta de prova:** A lei vale só para órgãos da UE ou só funciona como recomendação.
Como não cair: Tem força obrigatória, com multas, e alcança fornecedores e responsáveis pela implantação privados e públicos.

⚠ **Alerta de prova:** A lei só se aplica a empresas com mais de 250 empregados.
Como não cair: Não há corte por número de empregados; PME têm apoio e proporcionalidade, não exclusão.

⚠ **Alerta de prova:** Sistema treinado e operado fora da Europa fica fora da lei.
Como não cair: Conta a colocação no mercado ou o uso do resultado na UE (Art. 2(1)), não o local de treino ou operação.

⚠ **Alerta de prova:** A lei só se aplica se a empresa abrir subsidiária ou filial na UE.
Como não cair: Estabelecimento na UE não é condição; o fornecedor de fora de sistema de risco elevado nomeia representante autorizado.

⚠ **Alerta de prova:** A lei só se aplica se os dados pessoais ficarem em servidores na UE.
Como não cair: Localização de servidores pode importar para o GDPR, não para o âmbito da Lei da IA.

⚠ **Alerta de prova:** Sistema militar de reconhecimento de alvos é prática proibida ou risco elevado.
Como não cair: Uso exclusivamente militar, de defesa ou de segurança nacional está fora do âmbito (Art. 2(3)), seja qual for a técnica.

⚠ **Alerta de prova:** Modelo de pesquisa de universidade pública deve cumprir risco elevado ou ser registrado na base da UE.
Como não cair: Ser pública não muda nada: a exclusão do Art. 2(6) depende da finalidade exclusiva de pesquisa; não há registro de modelos de pesquisa.

⚠ **Alerta de prova:** Publicar o resultado da pesquisa em revista científica traz o modelo para a lei.
Como não cair: Publicar não é colocar no mercado; a lei passa a valer quando o modelo for oferecido no mercado.

⚠ **Alerta de prova:** Compartilhar com parentes torna profissional o uso de IA generativa em casa.
Como não cair: Compartilhar com a família não muda a natureza pessoal; a exclusão do Art. 2(10) continua.

⚠ **Alerta de prova:** Duas empresas que vendem sistema de fora são ambas importadoras.
Como não cair: Só a primeira colocação no mercado da UE é importação; a revenda posterior é distribuição.

⚠ **Alerta de prova:** Quem fez modificação substancial e pôs sua marca continua responsável pela implantação ou vira distribuidor.
Como não cair: Art. 25: marca própria, modificação substancial ou mudança de finalidade tornam a empresa fornecedora.

⚠ **Alerta de prova:** A Lei da IA substitui o GDPR e o DSA, ou só se aplica quando nenhuma outra lei se aplica.
Como não cair: É complementar: Art. 2(7) preserva o GDPR, Art. 2(5) preserva o DSA, e as normas se aplicam juntas.

⚠ **Alerta de prova:** As proibições do Art. 5 valem desde 2 de agosto de 2026, ou desde a publicação em 12 de julho de 2024.
Como não cair: Proibições e letramento: 2 de fevereiro de 2025. 12/07/2024 é a publicação; 2/08/2026 é a aplicação geral.

Como cai na prova

📝 **Como cai:** Empresa de fora da UE (Brasil, Japão, Coreia) oferece sistema a clientes europeus e a pergunta é se a lei se aplica.
Como resolver: 1) Veja se há colocação no mercado ou uso do resultado na UE. 2) Ignore sede, local de treino e servidores. 3) Se for risco elevado, lembre do representante autorizado. 4) Descarte alternativas que exigem filial, dados na UE ou treino na UE.

📝 **Como cai:** Cadeia com duas ou três empresas em países diferentes e a pergunta é o papel de cada uma.
Como resolver: 1) Quem tem o nome ou a marca no produto é o fornecedor. 2) Quem faz a primeira entrada na UE de marca estrangeira é importador. 3) Quem revende depois é distribuidor. 4) Se alguém pôs marca própria ou modificou substancialmente, aplique o Art. 25.

📝 **Como cai:** Cenário de uso militar, de pesquisa ou pessoal e alternativas oferecendo risco elevado, proibido ou registro.
Como resolver: Verifique primeiro a exclusão do Art. 2 pela finalidade exclusiva; se a finalidade for exclusiva, a resposta é 'fora do âmbito'. Teste em condições reais e oferta no mercado puxam o sistema de volta.

📝 **Como cai:** Pergunta direta de data de aplicação.
Como resolver: Separe publicação (12/07/2024), vigor (01/08/2024), proibições (02/02/2025), GPAI e sanções (02/08/2025), geral (02/08/2026). As alternativas erradas usam as outras datas da mesma lista.

📝 **Como cai:** Pergunta sobre o objetivo da lei para explicar à diretoria.
Como resolver: Escolha a alternativa com regras baseadas em risco, IA confiável e centrada no ser humano e proteção de direitos fundamentais. Descarte as que falam em proibir IA generativa, substituir GDPR ou regular só defesa.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
empresa sediada fora da UE oferece o sistema online a clientes em Estados-Membros	**Lei da IA se aplica (Art. 2(1)); se for risco elevado, representante autorizado na UE (Art. 22)**

destinado exclusivamente às forças armadas, à defesa ou à segurança nacional	**fora do âmbito (Art. 2(3))**
apenas para o projeto de pesquisa científica, sem oferecer no mercado	**fora do âmbito (Art. 2(6))**
teste em condições reais, em vias públicas ou com pessoas reais	**dentro da lei: Art. 2(8) não exclui testes em condições reais**
pessoa usa em casa, sem fins profissionais	**sem obrigações de responsável pela implantação (Art. 2(10)); fornecedor mantém as suas**
primeira a colocar no mercado da UE sistema com a marca do fabricante estrangeiro	**importador (Art. 3(6))**
compra da empresa que trouxe o sistema e revende	**distribuidor (Art. 3(7))**
comprou sistema de risco elevado, modificou de forma substancial ou passou a vender com sua marca	**passa a ser fornecedor (Art. 25)**
software que executa regras fixas definidas por programadores	**não é sistema de IA: falta a inferência**
infere, a partir das entradas, como gerar previsões, conteúdos, recomendações ou decisões	**definição de sistema de IA do Art. 3**
qual a consequência de a lei ser um regulamento	**aplicação direta, sem transposição nacional**
como a lei se articula com GDPR e DSA	**complementar: Art. 2(7) e Art. 2(5)**
licença livre e de código aberto	**fora, salvo risco elevado, Art. 5 ou Art. 50 (Art. 2(12))**
desde quando valem as proibições	**2 de fevereiro de 2025 (Art. 113)**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- O âmbito é definido pela colocação no mercado, em serviço ou pelo uso do resultado na UE; sede, treino e servidores não importam.
- Exclusões: uso exclusivamente militar, de defesa ou de segurança nacional; pesquisa científica exclusiva; uso pessoal não profissional. Testes em condições reais continuam dentro.
- Importador faz a primeira entrada de marca estrangeira; distribuidor revende.
- Marca própria, modificação substancial ou nova finalidade de risco elevado transformam o operador em fornecedor (Art. 25).
- A Lei da IA soma-se ao GDPR e ao DSA; não substitui nenhum deles.

Essenciais para a prova (checklist)

- ☐ Sei explicar por que a Lei da IA, como regulamento, se aplica sem transposição.
- ☐ Sei descrever o objetivo do Art. 1 e a lógica baseada no risco.
- ☐ Sei reconhecer um sistema de IA pela inferência e descartar regras fixas.
- ☐ Sei aplicar o Art. 2(1) a fornecedores de países terceiros.
- ☐ Sei listar as exclusões do Art. 2 (militar, pesquisa, uso pessoal, código aberto com ressalvas).
- ☐ Sei distinguir fornecedor, responsável pela implantação, importador e distribuidor num cenário.
- ☐ Sei o que o importador verifica (Art. 23) e o que faz o representante autorizado (Art. 22).
- ☐ Sei quando um operador vira fornecedor pelo Art. 25.
- ☐ Sei as datas de 2024, 2025 e 2026 do calendário de aplicação.

Questões de revisão do capítulo

R1.1 · Domínio 1: Contexto da Lei da IA (AI Act)

Uma universidade desenvolve e coloca em serviço um modelo de IA apenas para seu projeto de pesquisa científica, sem oferecê-lo no mercado. Qual é a situação desse modelo perante o AI Act?

A. Está fora do AI Act, pois foi desenvolvido e colocado em serviço só para pesquisa científica
B. Deve cumprir os requisitos de risco elevado, por ter sido desenvolvido por uma instituição pública
C. Deve ser registrado na base de dados da UE antes do início da pesquisa científica na universidade
D. Fica sujeito ao AI Act assim que os resultados da pesquisa forem publicados em revista científica

R1.2 · Domínio 1: Contexto da Lei da IA (AI Act)

Uma empresa sediada no Brasil oferece, apenas online, um sistema de IA de triagem de currículos a empregadores estabelecidos em vários Estados-Membros da UE. O modelo é treinado e operado fora da Europa. Como o AI Act se aplica a essa situação?

A. Aplica-se, pois o sistema é colocado no mercado e usado na UE, mesmo com fornecedor de fora
B. Não se aplica, pois o regulamento alcança sistemas desenvolvidos e treinados dentro da UE
C. Só se aplica se a empresa abrir uma subsidiária em algum Estado-Membro para vender o sistema
D. Aplica-se só se os dados pessoais dos candidatos ficarem em servidores localizados na UE

R1.3 · Domínio 1: Contexto da Lei da IA (AI Act)

Segundo a definição do artigo 3 do AI Act, qual característica é central para que um software seja considerado um sistema de IA?

A. Utilizar obrigatoriamente redes neurais profundas
B. Inferir, a partir das entradas, como gerar resultados
C. Rodar em servidores de nuvem com alta capacidade de processamento
D. Executar regras fixas definidas por programadores

R1.4 · Domínio 1: Contexto da Lei da IA (AI Act)

Uma empresa europeia que desenvolve sistemas de IA quer explicar à diretoria o objetivo principal do AI Act. Qual descrição é a mais adequada?

A. Regular os sistemas de IA de órgãos públicos nas áreas de segurança e defesa nacional
B. Proibir o uso de IA generativa nos Estados-Membros até que uma agência europeia seja criada
C. Criar regras baseadas em risco para uma IA segura, transparente e que respeite direitos fundamentais
D. Substituir as legislações da UE sobre proteção de dados e direitos do consumidor por um código único

Respostas comentadas

R1.1. A) Está fora do AI Act, pois foi desenvolvido e colocado em serviço só para pesquisa científica

Por quê: O artigo 2(6) exclui do AI Act os sistemas e modelos de IA, incluindo seus resultados, desenvolvidos e colocados em serviço especificamente para o único fim de pesquisa e desenvolvimento científico. O artigo 2(8) também exclui atividades de pesquisa, teste e desenvolvimento anteriores à colocação no mercado, mas não os testes em condições reais. Se o modelo for depois oferecido no mercado, passa a se sujeitar às regras.

✗ B) Incorreta. Ser pública não muda a regra: a exclusão do artigo 2(6) depende da finalidade exclusiva de pesquisa.
✗ C) Incorreta. Não há registro de modelos de pesquisa; a base de dados da UE recebe sistemas de risco elevado colocados no mercado ou em serviço.
✗ D) Incorreta. Publicar resultados não coloca o modelo no mercado; a exclusão continua enquanto a finalidade for só pesquisa.

> **Dica de prova:** Só pesquisa científica: fora do AI Act. Teste em condições reais: dentro.

R1.2. A) Aplica-se, pois o sistema é colocado no mercado e usado na UE, mesmo com fornecedor de fora

Por quê: O artigo 2(1) aplica o AI Act a fornecedores que colocam no mercado ou em serviço sistemas de IA na UE, estejam estabelecidos na União ou num país terceiro, a responsáveis pela implantação estabelecidos na UE e a fornecedores e responsáveis pela implantação de países terceiros quando o resultado do sistema é usado na UE. Como a triagem de currículos está no Anexo III (emprego), o fornecedor brasileiro também precisará de representante autorizado na UE (artigo 22).

✗ B) Incorreta. O local de desenvolvimento ou treino não define o âmbito; importa a colocação no mercado, a colocação em serviço ou o uso do resultado na UE.
✗ C) Incorreta. Ter estabelecimento na UE não é condição: o artigo 2(1) alcança fornecedores de países terceiros que colocam sistemas no mercado da União.
✗ D) Incorreta. A localização dos servidores não define o âmbito do AI Act; ela pode importar para o GDPR, não para esta questão.

> **Dica de prova:** Âmbito territorial: vale o mercado e o uso na UE, não a sede do fornecedor.

R1.3. B) Inferir, a partir das entradas, como gerar resultados

Por quê: O AI Act define sistema de IA como um sistema baseado em máquina, projetado para operar com níveis variados de autonomia, que pode se adaptar após a implantação e que infere, a partir das entradas recebidas, como gerar resultados como previsões, conteúdos, recomendações ou decisões. A capacidade de inferência diferencia a IA de softwares baseados em regras fixas definidas por pessoas.

✗ A) Incorreta. A definição é neutra quanto à técnica usada.

✗ C) Incorreta. O local de execução não define um sistema de IA.

✗ D) Incorreta. Regras fixas definidas por pessoas ficam fora da definição.

> **Dica de prova:** Sistema de IA no AI Act: autonomia, possível adaptação e inferência.

R1.4. C) Criar regras baseadas em risco para uma IA segura, transparente e que respeite direitos fundamentais

Por quê: O artigo 1 do AI Act tem como finalidade melhorar o funcionamento do mercado interno e promover a adoção de uma IA centrada no ser humano e confiável, garantindo elevado nível de proteção da saúde, da segurança e dos direitos fundamentais da Carta e apoiando a inovação. Para isso, gradua as obrigações conforme o risco: práticas proibidas, sistemas de risco elevado, deveres de transparência e risco mínimo.

✗ A) Incorreta. O AI Act alcança setores públicos e privados, e os usos exclusivamente militares, de defesa e de segurança nacional ficam fora do seu âmbito.

✗ B) Incorreta. O AI Act não proíbe a IA generativa; cria deveres de transparência e regras para modelos de finalidade geral.

✗ D) Incorreta. O AI Act complementa o GDPR e as regras de consumo, que continuam aplicáveis; não os substitui.

> **Dica de prova:** Objetivo do AI Act: IA confiável e centrada no ser humano, com regras proporcionais ao risco.

02

CAPÍTULO 2 · 37,5% DA PROVA

Domínio 2: Lei da IA detalhada

É o coração da prova: 37,5% do peso e 15 questões em 40. Preciso classificar qualquer sistema na categoria certa (proibido, risco elevado, transparência, mínimo), saber os requisitos do risco elevado (Arts. 9 a 15), quem faz o quê na cadeia (fornecedor, responsável pela implantação, importador, distribuidor), o regime dos modelos GPAI, a governança (Gabinete de IA, Comité IA, fórum, painel, autoridades nacionais), incidentes e multas. As questões são cenários que citam o artigo e pedem a consequência exata. Onde mais erro: misturar prazos e tetos do GDPR com os da Lei da IA, esquecer que PME pagam o menor valor e trocar o órgão competente (EDPS, Comissão, autoridade nacional).

Neste capítulo
18 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Abordagem baseada no risco

Quanto maior o risco, mais obrigações: risco inaceitável é proibido (Art. 5); risco elevado cumpre requisitos e avaliação de conformidade (Capítulo III); certos sistemas têm deveres de transparência (Art. 50); o restante é risco mínimo, sem obrigações específicas, com códigos de conduta voluntários (Art. 95). Obrigações gerais, como o letramento em IA do Art. 4, valem para todos.

Práticas proibidas (Art. 5)

Técnicas subliminares, manipuladoras ou enganosas que distorcem decisões e causam dano significativo (alínea a); exploração de vulnerabilidades por idade, deficiência ou situação social ou econômica (alínea b); pontuação social por entes públicos e privados; previsão de crimes só por perfil ou traços de personalidade; raspagem não direcionada de rostos da internet ou de CFTV; reconhecimento de emoções no trabalho e no ensino; categorização biométrica para inferir atributos sensíveis (alínea g); identificação biométrica remota em tempo real pela polícia em espaços públicos (alínea h), salvo exceções. Consentimento, aviso ou dados públicos não tornam a prática lícita.

Classificação de risco elevado (Art. 6)

Duas vias: o sistema é produto, ou componente de segurança de produto, da legislação de harmonização do Anexo I sujeito a avaliação por terceiros (Art. 6(1)); ou o uso está no Anexo III. Pela versão consolidada, IA só para assistência, otimização ou conveniência não é componente de segurança (Art. 6(1a)), salvo se sua falha puder pôr em perigo a saúde e a segurança (Art. 6(1b)). O Anexo III é alterado por atos delegados da Comissão (Art. 7).

Derrogação do Art. 6(3) e reclassificação (Art. 80)

Sistema do Anexo III pode não ser de risco elevado se não representa risco significativo, por exemplo ao executar tarefa processual restrita, melhorar resultado de atividade humana já concluída ou fazer tarefa preparatória; a exceção nunca vale com perfilagem. O fornecedor documenta a avaliação e registra o sistema (Art. 49(2)). Se a autoridade de fiscalização concluir que é risco elevado e que a classificação foi feita para contornar os requisitos, exige conformidade e pode multar (Art. 80(7)).

Finalidade pretendida e uso indevido previsível (Art. 3(12) e 3(13))

A finalidade pretendida é definida pelo fornecedor nas instruções, materiais promocionais e documentação técnica, e orienta a classificação. O uso indevido razoavelmente previsível decorre de comportamento humano previsível e entra na gestão de riscos do próprio fornecedor (Art. 9(2)(b)). O uso real diverso dos clientes não redefine a finalidade.

Gestão de riscos (Art. 9)

Processo iterativo e contínuo em todo o ciclo de vida, com revisão sistemática regular, que inclui riscos vindos do acompanhamento pós-comercialização (Art. 9(2)(c)). Ordem das medidas (Art. 9(5)): eliminar ou reduzir pelo projeto, depois mitigar e controlar o que resta, por fim informar e formar; o risco residual tem de ser julgado aceitável. O Art. 9(9) manda considerar impacto adverso em menores de 18 anos e outros grupos vulneráveis.

Dados e governança de dados (Art. 10)

O Art. 10(2) lista práticas como origem e finalidade original da coleta, preparação (anotação, rotulagem, limpeza), suposições, disponibilidade e adequação, exame e mitigação de vieses e lacunas. O Art. 10(3) pede conjuntos de treino, validação e teste pertinentes, suficientemente representativos e, na medida do possível, isentos de erros e completos; não exige perfeição, anonimização nem cotas. O Art. 10(4) exige refletir o contexto geográfico, contextual, comportamental ou funcional de uso.

Documentação técnica, conservação e logs (Arts. 11, 12 e 18)

A documentação técnica (Anexo IV) é feita antes da colocação no mercado e mantida atualizada; PME e SMC podem usar o formulário simplificado da Comissão, sem dispensa. O fornecedor guarda documentação técnica, do sistema de gestão da qualidade e declaração UE por 10 anos (Art. 18). Para identificação biométrica remota do Anexo III 1(a), os logs registram no mínimo período de uso, base de referência, dados que deram correspondência e quem verificou (Art. 12(3)).

Exatidão, robustez e cibersegurança (Art. 15)

Sistemas que continuam aprendendo devem eliminar ou reduzir ciclos de feedback enviesados (Art. 15(4)); aprender após o lançamento não é proibido. O Art. 15(5) exige resiliência contra envenenamento de dados (treino adulterado), envenenamento de modelo (componente pré-treinado), exemplos adversariais ou evasão (entrada feita para causar erro), ataques de confidencialidade e falhas do modelo.

Obrigações do fornecedor e sistema de gestão da qualidade (Arts. 16, 17, 20 e 21)

O fornecedor cumpre os requisitos, indica nome, marca e contato no sistema ou, se não der, na embalagem ou documentação (Art. 16(b)), mantém sistema de gestão da qualidade proporcional ao porte que inclui gestão de riscos, pós-comercialização e incidentes (Art. 17), faz avaliação, declaração UE, marcação CE e registro, cumpre acessibilidade. Não conformidade: corrigir, retirar, desativar ou recolher e avisar a cadeia (Art. 20(1)); havendo risco, investigar e informar a autoridade (Art. 20(2)). A pedido fundamentado, entrega documentação e acesso aos logs, com confidencialidade (Arts. 21 e 78).

Obrigações do responsável pela implantação (Art. 26)

Usar conforme as instruções (26(1)); atribuir a supervisão a pessoas com competência, formação, autoridade e apoio (26(2)); garantir dados de entrada pertinentes e representativos, quando os controla (26(4)); monitorar e, se houver risco, informar fornecedor ou distribuidor e autoridade e suspender o uso (26(5)); em incidente grave, avisar primeiro o fornecedor; guardar logs por no mínimo 6 meses (26(6)); informar trabalhadores (26(7)); autoridade pública não usa sistema não registrado (26(8)); usar as instruções do Art. 13 na DPIA (26(9)).

Avaliação de conformidade, declaração, CE e registro (Arts. 43, 47, 48 e 49)

Anexo III pontos 2 a 8: controle interno pelo fornecedor (Anexo VI). Ponto 1 (biometria): pode exigir organismo notificado (Anexo VII) quando não se aplicam normas harmonizadas ou especificações comuns. Produtos do Anexo I, Seção A: procedimento setorial com os requisitos da Lei da IA dentro (Art. 43(3)). Concluída a avaliação: declaração UE (Art. 47), marcação CE afixada pelo fornecedor (Art. 48) e registro na base da UE antes do mercado para o Anexo III, exceto o ponto 2, registrado em nível nacional. Modificação substancial exige nova avaliação (Art. 43(4)).

Modelo GPAI e sistema de IA de finalidade geral (Arts. 3(63), 3(66) e 53)

Modelo GPAI é o modelo com generalidade significativa, capaz de ampla gama de tarefas e integrável em sistemas a jusante; o sistema de IA de finalidade geral é o produto construído sobre ele. Obrigações do Art. 53(1): documentação técnica para Gabinete de IA e autoridades (a), informações aos integradores (b, Anexo XII), política de direitos autorais que respeita o opt-out de mineração de textos e dados da Diretiva 2019/790 (c) e resumo público do conteúdo de treino segundo modelo do Gabinete de IA (d). Código aberto sem risco sistêmico fica isento só de (a) e (b) (Art. 53(2)).

GPAI com risco sistêmico (Arts. 51, 52 e 55)

Presume-se capacidade de elevado impacto quando o cômputo acumulado de treino supera 10^25 FLOPs; a Comissão também pode designar por outros critérios, inclusive após alerta do painel científico. O fornecedor notifica a Comissão em até duas semanas após atingir ou saber que atingirá o limiar (Art. 52(1)). Deveres extras (Art. 55): avaliar o modelo com testes adversariais, mitigar riscos sistêmicos, comunicar incidentes graves ao Gabinete de IA e garantir cibersegurança. Risco sistêmico não é prática proibida.

Código de práticas de GPAI (Arts. 53(4) e 56)

Instrumento voluntário publicado em julho de 2025, com capítulos de transparência, direitos autorais e segurança para modelos com risco sistêmico. Serve para demonstrar cumprimento dos Arts. 53 e 55 até haver normas harmonizadas. Quem não adere nem segue norma harmonizada demonstra meios alternativos adequados, avaliados pela Comissão; não há declaração UE, CE nem organismo notificado para GPAI.

Governança (Arts. 64 a 70 e 74)

Gabinete de IA: parte da Comissão, coordena a aplicação harmonizada e tem competência exclusiva sobre fornecedores de modelos GPAI. Comité IA: um representante por Estado-Membro, aconselha Comissão e Estados. Fórum consultivo (Art. 67): partes interessadas (indústria, startups, PME, sociedade civil, academia), mandatos de dois anos. Painel científico (Art. 68): peritos independentes que emitem alertas qualificados sobre risco sistêmico. Cada Estado designa ao menos uma autoridade notificadora e uma de fiscalização do mercado, e uma destas como ponto único de contato notificado à Comissão (Art. 70).

Incidente grave e notificação (Arts. 3(49) e 73)

Incidente grave leva, direta ou indiretamente, a morte ou dano grave à saúde, perturbação grave e irreversível de infraestrutura crítica, violação de obrigações que protegem direitos fundamentais ou dano grave à propriedade ou ao ambiente. Prazos do fornecedor: até 15 dias (regra geral), até 10 dias (morte), até 2 dias (infração generalizada ou infraestrutura crítica). Depois de notificar, investiga e corrige sem alterar o sistema de forma que prejudique a análise das causas antes de avisar as autoridades (Art. 73(6)).

Sandbox, testes em condições reais e apoio a PME (Arts. 57, 60 e 62)

Sandbox: ambiente controlado das autoridades nacionais para desenvolver e testar com orientação; não dispensa avaliação de conformidade e a responsabilidade civil continua, mas não há multa administrativa se o plano e a orientação forem seguidos de boa-fé (Art. 57(12)). Teste real fora do sandbox: plano aprovado pela autoridade de fiscalização (tácito em 30 dias se o direito nacional prever), registro, até 6 meses prorrogáveis por mais 6, consentimento informado (Art. 61). PME e startups: acesso prioritário ao sandbox, sensibilização, canais de orientação e taxas de avaliação de conformidade reduzidas pelo porte, não gratuitas (Art. 62).

Macetes para memorizar

Multas do Art. 99

35-7 proíbe, 15-3 descumpre, 7,5-1 mente. Grande paga o MAIOR, PME paga o MENOR.

Multas fora do Art. 99

Órgão da UE: EDPS 1,5 mi ou 750 mil. GPAI: Comissão 3% ou 15 mi.

Prazos de incidente grave

15 geral, 10 morte, 2 crítico. 72 horas é GDPR.

Ordem do Art. 9(5)

EMI: Elimina pelo projeto, Mitiga o resto, Informa e forma por último.

Dados do Art. 10(3)

PRIC: Pertinentes, Representativos, Isentos de erros e Completos, na medida do possível.

Logs de biometria remota (Art. 12(3))

Quando usou, contra qual base, o que deu correspondência e quem conferiu.

Obrigações do Art. 53(1)

Autoridade recebe Documentação; integrador recebe Informação; todos respeitam Direitos autorais; público recebe o Resumo do treino.

Guarda

Papel do fornecedor: 10 anos. Log do responsável pela implantação: 6 meses no mínimo.

Tabela de memorização: não confunda

Quando é...	...e quando é
Modelo GPAI (Art. 3(63)) O motor: o modelo treinado, licenciado a outros desenvolvedores.	**Sistema de IA de finalidade geral (Art. 3(66))** O produto construído sobre o modelo, como o assistente de chat lançado ao público.
Identificação biométrica remota Compara a pessoa com uma lista ou base para descobrir quem é: risco elevado (Anexo III 1(a)); proibida só em tempo real pela polícia em espaço público.	**Verificação biométrica 1 para 1** Confirma que a pessoa é quem diz ser (desbloqueio, abertura de conta): fora do Anexo III, segue o GDPR.
Controle interno (Anexo VI) Regra para o Anexo III pontos 2 a 8, como emprego e crédito.	**Organismo notificado (Anexo VII ou procedimento setorial)** Biometria do ponto 1 sem normas harmonizadas ou especificações comuns, e produtos do Anexo I com avaliação por terceiros.
Teto pelo maior valor Empresas em geral: vale o maior entre valor fixo e percentual do faturamento.	**Teto pelo menor valor** PME e startups (Art. 99(6)) e, nos tetos dos parágrafos 4 e 5, SMC: vale o menor.

Art. 20(1) Não conformidade: corrigir, retirar, desativar ou recolher e informar distribuidores e, se aplicável, responsáveis pela implantação, representante e importadores.	**Art. 20(2)** O sistema apresenta risco (Art. 79(1)): investigar as causas e informar a autoridade de fiscalização do mercado e, se for o caso, o organismo notificado.
Fórum consultivo (Art. 67) Representa partes interessadas e aconselha Comité IA e Comissão.	**Painel científico (Art. 68)** Peritos independentes de fornecedores que alertam o Gabinete de IA sobre risco sistêmico.
Envenenamento de dados Adulteram o conjunto de treino para induzir erros.	**Exemplo adversarial** Uma entrada criada para enganar o modelo durante o uso. Ambos ficam no Art. 15(5).

Números que caem

Item	Valor
Multa por práticas proibidas (Art. 99(3))	**até 35 milhões de euros ou 7% do faturamento anual mundial**
Multa por obrigações de operadores, organismos notificados e Art. 50 (Art. 99(4))	**até 15 milhões de euros ou 3%**
Multa por informação incorreta, incompleta ou enganosa (Art. 99(5))	**até 7,5 milhões de euros ou 1%**
Multas da EDPS a órgãos da União (Art. 100)	**até 1,5 milhão de euros (Art. 5) e até 750 mil euros (demais)**
Multas da Comissão a fornecedores de GPAI (Art. 101)	**até 3% ou 15 milhões de euros, o maior**
Exemplo de PME com faturamento de 10 milhões infringindo o Art. 26	**teto de 300 mil euros (3%, menor que 15 milhões)**
Notificação de incidente grave (Art. 73)	**15 dias (geral), 10 dias (morte), 2 dias (infraestrutura crítica ou infração generalizada)**
Conservação da documentação do fornecedor (Art. 18)	**10 anos**
Conservação dos logs pelo responsável pela implantação (Art. 26(6))	**no mínimo 6 meses**
Limiar de presunção de risco sistêmico (Art. 51)	**mais de 10^25 FLOPs de cômputo de treino**
Notificação à Comissão do limiar de GPAI (Art. 52(1))	**até duas semanas**
Teste em condições reais fora do sandbox (Art. 60)	**até 6 meses, prorrogáveis por mais 6; aprovação tácita após 30 dias quando o direito nacional prevê**
Mandato do fórum consultivo	**2 anos, prorrogáveis**

Código de práticas de GPAI	**publicado em julho de 2025**
Diretrizes da Comissão sobre práticas proibidas e definição de sistema de IA	**fevereiro de 2025**
Nova Diretiva de Responsabilidade por Produtos Defeituosos	**em vigor desde 8 de dezembro de 2024; vale para produtos colocados no mercado a partir de 9 de dezembro de 2026**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Modelo GPAI com risco sistêmico deve ser retirado do mercado por ser prática proibida.
Como não cair: É permitido, com obrigações adicionais do Art. 55; não está no Art. 5.

⚠ **Alerta de prova:** Entregar manual aos integradores transfere a gestão de risco do modelo GPAI.
Como não cair: Informar integradores (Art. 53) não substitui os deveres próprios do Art. 55.

⚠ **Alerta de prova:** Ao expandir para outro país é preciso nova marcação CE ou nova avaliação de conformidade em cada Estado-Membro.
Como não cair: A marcação CE é afixada pelo fornecedor e vale na União; o ponto é adequar os dados ao novo contexto (Art. 10(4)).

⚠ **Alerta de prova:** Incidente grave deve ser notificado em 72 horas.
Como não cair: 72 horas é violação de dados do GDPR. Lei da IA: 15 dias, 10 em caso de morte, 2 para infraestrutura crítica ou infração generalizada.

⚠ **Alerta de prova:** O teto das multas por práticas proibidas é 20 milhões ou 4%.
Como não cair: 20 milhões ou 4% é o GDPR. Práticas proibidas: 35 milhões ou 7%.

⚠ **Alerta de prova:** PME paga até 15 milhões, porque vale o maior valor, ou tem teto especial de 1,5 milhão.
Como não cair: Para PME vale o menor (Art. 99(6)); 1,5 milhão é o teto da EDPS para órgãos da UE.

⚠ **Alerta de prova:** Gabinete de IA, Comissão ou autoridade nacional multam agência da União.
Como não cair: Órgãos da União são multados pela EDPS (Art. 100). A Comissão multa fornecedores de GPAI (Art. 101).

⚠ **Alerta de prova:** Participar de sandbox isenta de responsabilidade civil ou dispensa a avaliação de conformidade.
Como não cair: Danos a terceiros continuam a ser responsabilidade do participante; o sandbox só evita multa se houver boa-fé e respeito ao plano.

⚠ **Alerta de prova:** A gestão de riscos termina com o relatório antes do lançamento ou só é refeita com modificação substancial.
Como não cair: É processo contínuo e iterativo em todo o ciclo de vida, alimentado pelo pós-comercialização.

⚠ **Alerta de prova:** A ordem do Art. 9(5) começa por informar e formar o responsável pela implantação.
Como não cair: Primeiro eliminar ou reduzir pelo projeto, depois mitigar e controlar, por último informar e formar.

⚠ **Alerta de prova:** Uso indevido razoavelmente previsível é problema do responsável pela implantação.
Como não cair: O Art. 9(2)(b) manda o próprio fornecedor avaliar esses riscos.

⚠ **Alerta de prova:** Na derrogação do Art. 6(3) o sistema sai da lei e dispensa documentar e registrar.
Como não cair: A avaliação é documentada e o registro continua (Art. 49(2)); com perfilagem não há derrogação.

⚠ **Alerta de prova:** O responsável pela implantação avisa primeiro a autoridade de fiscalização ou a de proteção de dados em caso de incidente grave.
Como não cair: Art. 26(5): primeiro o fornecedor; depois importador ou distribuidor e autoridades de fiscalização do mercado.

⚠ **Alerta de prova:** Fornecedor de GPAI que negligenciou pedido de documentos responde pelo teto de 1% ou 7,5 milhões, aplicado pela autoridade nacional.
Como não cair: GPAI tem teto único de 3% ou 15 milhões, o maior, aplicado pela Comissão (Art. 101).

Como cai na prova

📝 **Como cai:** Cenário descreve um sistema e pede como a Lei da IA o classifica.
Como resolver: 1) Teste o Art. 5 (proibido?). 2) Produto ou componente de segurança do Anexo I com avaliação por terceiros? 3) Uso listado no Anexo III? Se sim, veja a derrogação do Art. 6(3) (sem perfilagem). 4) Interage com pessoas ou gera conteúdo? Art. 50. 5) Senão, risco mínimo. Transparência ou consentimento nunca salvam uma prática proibida.

📝 **Como cai:** Infração descrita e alternativas com vários tetos de multa.
Como resolver: 1) Identifique o tipo: proibição (35 mi/7%), obrigação de operador ou transparência (15 mi/3%), informação enganosa (7,5 mi/1%). 2) Veja quem é o infrator: órgão da UE vai à EDPS, GPAI à Comissão. 3) Veja o porte: PME pega o menor, empresa grande o maior. 4) Se houver faturamento, calcule o percentual.

📝 **Como cai:** Incidente ou risco detectado e pergunta sobre prazo ou ordem de comunicação.
Como resolver: Separe quem detectou. Fornecedor: Art. 73 (15/10/2 dias) e Art. 20. Responsável pela implantação: avisa primeiro o fornecedor, depois importador ou distribuidor e autoridade; se o risco vem do uso conforme, suspende. Descarte 72 horas e o Gabinete de IA na cadeia.

📝 **Como cai:** Pergunta 'que obrigação o artigo X impõe a Y' com alternativas trocando os papéis.
Como resolver: Lembre a divisão: fornecedor fabrica a conformidade (documentação, avaliação, declaração, CE, registro, gestão de riscos); responsável pela implantação usa conforme instruções, supervisiona, controla dados de entrada, guarda logs e avisa; distribuidor confere CE, declaração e instruções. Alternativa que dá ao responsável pela implantação tarefa de fornecedor está errada.

📝 **Como cai:** Pergunta sobre qual órgão faz algo (aconselhar, alertar, multar, fiscalizar).
Como resolver: Gabinete de IA = Comissão e GPAI; Comité IA = Estados-Membros; fórum = partes interessadas; painel = peritos independentes; autoridade notificadora = organismos de avaliação; autoridade de fiscalização do mercado = sistemas no mercado e ponto único de contato.

📝 **Como cai:** Cenário de GPAI com pergunta sobre obrigação, isenção de código aberto ou prova de conformidade.
Como resolver: Diferencie modelo e sistema; aplique o Art. 53(1) a todos; código aberto sem risco sistêmico só se livra de documentação e informação aos integradores; com risco sistêmico perde a isenção e soma o Art. 55; prova de conformidade via código de práticas, norma harmonizada ou meios alternativos avaliados pela Comissão.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
coleta não direcionada de imagens faciais da internet ou de câmeras	**prática proibida (Art. 5)**
prever crimes só com perfil ou traços de personalidade	**proibido; se apoiar avaliação humana baseada em fatos objetivos, é risco elevado**
compara rostos gravados, dias depois, com uma lista, uso privado	**identificação biométrica remota a posteriori: risco elevado (Anexo III 1(a))**

modelo treinado com dados de um país será usado em outros	**Art. 10(4): contexto geográfico, comportamental e funcional**
registros adulterados inseridos no conjunto de treino	**envenenamento de dados, Art. 15(5)**
sistema continua aprendendo e o viés se realimenta	**ciclos de feedback, Art. 15(4)**
cômputo de treino acima de 10^25 FLOPs	**presunção de risco sistêmico; notificar a Comissão em até duas semanas**
fornecedor de GPAI não aderiu ao código de práticas	**meios alternativos adequados avaliados pela Comissão (Art. 53(4))**
editora reservou direitos contra mineração de textos e dados	**política de direitos autorais do Art. 53(1)(c) e Art. 4(3) da Diretiva 2019/790**
funcionária quer denunciar violação do empregador	**Art. 87 e Diretiva (UE) 2019/1937**
agência ou órgão da União violou a lei	**EDPS: até 1,5 milhão (Art. 5) ou 750 mil (demais infrações)**
relatório incompleto ou enganoso entregue à autoridade	**até 7,5 milhões ou 1% (Art. 99(5))**
perturbação grave e irreversível em rede de eletricidade ou outra infraestrutura crítica	**notificação imediata e no máximo em 2 dias (Art. 73(3))**
autoridade pública constata que o sistema do Anexo III não está registrado	**não usa e informa fornecedor ou distribuidor (Art. 26(8))**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- A classificação parte da finalidade pretendida definida pelo fornecedor; aviso, consentimento ou dados públicos não tiram uma prática do Art. 5.
- Fornecedor fabrica a conformidade; responsável pela implantação usa conforme as instruções, supervisiona, guarda logs e avisa.
- Multas: 35/7, 15/3, 7,5/1; grande paga o maior, PME o menor; EDPS para órgãos da UE, Comissão para GPAI.
- Incidente grave: 15, 10 ou 2 dias; 72 horas é do GDPR.
- GPAI: Art. 53 para todos, Art. 55 para risco sistêmico (10^25 FLOPs); código aberto só ganha isenção parcial e a perde com risco sistêmico.

Essenciais para a prova (checklist)

- ☐ Sei listar as práticas proibidas do Art. 5 e suas ressalvas (médico ou segurança, exceções policiais).
- ☐ Sei aplicar as duas vias do Art. 6 e a derrogação do Art. 6(3).
- ☐ Sei a ordem do Art. 9(5) e o caráter contínuo da gestão de riscos.

- ☐ Sei os critérios de dados do Art. 10(2), 10(3) e 10(4).
- ☐ Sei diferenciar envenenamento de dados, envenenamento de modelo e exemplo adversarial.
- ☐ Sei as obrigações do Art. 26 para o responsável pela implantação, inclusive a ordem de comunicação em incidente grave.
- ☐ Sei quando há controle interno e quando entra organismo notificado.
- ☐ Sei as quatro obrigações do Art. 53(1), a isenção do código aberto e os deveres do Art. 55.
- ☐ Sei os tetos de multa dos Arts. 99, 100 e 101 e a regra do menor para PME.
- ☐ Sei os papéis do Gabinete de IA, Comité IA, fórum consultivo, painel científico e autoridades nacionais.

Questões de revisão do capítulo

R2.1 · Domínio 2: Lei da IA detalhada

Uma comunidade de desenvolvedores publica um sistema de IA sob licença livre e de código aberto. Em qual das situações a seguir a Lei da IA continua a se aplicar a esse sistema?

A. Quando passar a ter mais de mil usuários ativos em Estados-Membros da União
B. Quando for colocado no mercado ou em serviço como sistema de IA de risco elevado
C. Quando for distribuído de forma gratuita, sem monetização direta pelos seus autores
D. Quando o repositório do código estiver hospedado em servidores fora da União

R2.2 · Domínio 2: Lei da IA detalhada

Qual órgão criado pelo AI Act reúne representantes dos Estados-Membros para aconselhar a Comissão e apoiar a aplicação coerente do regulamento?

A. Comité Europeu para a Inteligência Artificial
B. Comité Europeu para a Proteção de Dados
C. Agência da UE para a Cibersegurança (ENISA)
D. Tribunal de Justiça da União Europeia

R2.3 · Domínio 2: Lei da IA detalhada

Uma autoridade pública vai usar um sistema de identificação biométrica remota do Anexo III, ponto 1(a). Que informações os registros automáticos (logs) desse sistema devem permitir gravar, no mínimo?

A. Nome de cada pessoa filmada, localização das câmeras e imagens integrais de cada sessão de uso
B. Período de cada uso, versão do modelo, taxa de acurácia obtida e custo operacional de cada consulta
C. Base de referência consultada, consentimento das pessoas identificadas e parecer do encarregado de dados
D. Período de cada uso, base de referência, dados com correspondência e quem verificou os resultados

R2.4 · Domínio 2: Lei da IA detalhada

Uma empresa treinou um grande modelo de linguagem, capaz de executar ampla gama de tarefas, e o licencia a outros desenvolvedores. Ela também lança, para o público, um assistente de chat baseado nesse modelo, que serve a várias finalidades. Como a Lei da IA classifica esses dois elementos?

A. Ambos são modelos GPAI, já que a Lei da IA não diferencia modelo de IA e sistema de IA nesse caso
B. O modelo é um sistema de IA de finalidade geral, e o assistente é um modelo integrado a ele
C. O modelo é um modelo GPAI, e o assistente baseado nele é um sistema de IA de finalidade geral
D. O assistente é um modelo GPAI, e o modelo licenciado é um componente de sistema de risco elevado

Respostas comentadas

R2.1. B) Quando for colocado no mercado ou em serviço como sistema de IA de risco elevado

Por quê: O Art. 2(12) determina que a Lei da IA não se aplica a sistemas de IA lançados sob licenças livres e de código aberto, salvo se forem colocados no mercado ou em serviço como sistemas de risco elevado ou como sistema que se enquadra no Art. 5 (práticas proibidas) ou no Art. 50 (obrigações de transparência).

✗ A) Incorreta. O Art. 2(12) não usa número de usuários como critério; as exceções são risco elevado, prática proibida e obrigações do Art. 50.

✗ C) Incorreta. A gratuidade é característica comum do código aberto e não traz o sistema de volta ao âmbito da lei.

✗ D) Incorreta. O local de hospedagem do código não é critério do Art. 2(12); o que conta é o enquadramento como risco elevado, Art. 5 ou Art. 50.

> **Dica de prova:** Código aberto fica fora da Lei da IA, exceto se for risco elevado, prática proibida ou sujeito ao Art. 50 (Art. 2(12)).

R2.2. A) Comité Europeu para a Inteligência Artificial

Por quê: O AI Act cria o Comité Europeu para a Inteligência Artificial (Comité IA), formado por um representante de cada Estado-Membro, para aconselhar e assistir a Comissão e os Estados-Membros na aplicação coerente do regulamento (artigos 65 e 66). Ele atua com o Gabinete de IA, com um fórum consultivo de partes interessadas e com um painel científico de peritos independentes.

✗ B) Incorreta. O Comité Europeu para a Proteção de Dados atua no âmbito do GDPR.

✗ C) Incorreta. A ENISA é a agência europeia de cibersegurança.

✗ D) Incorreta. O Tribunal de Justiça interpreta o direito da UE, sem papel consultivo.

> **Dica de prova:** Comité IA: representantes dos Estados-Membros. Gabinete de IA: parte da Comissão.

R2.3. D) Período de cada uso, base de referência, dados com correspondência e quem verificou os resultados

Por quê: Para os sistemas do ponto 1(a) do Anexo III, o Art. 12(3) exige que os logs registrem, no mínimo: (a) o período de cada utilização, com data e hora de início e fim; (b) a base de dados de referência usada na verificação; (c) os dados de entrada que levaram a uma correspondência; (d) a identificação das pessoas físicas envolvidas na verificação dos resultados (Art. 14(5)).

✗ A) Incorreta. O Art. 12(3) não exige registrar o nome de cada pessoa filmada nem imagens integrais; lista um conteúdo mínimo diferente.

✗ B) Incorreta. Versão do modelo, acurácia e custo não estão no mínimo do Art. 12(3), que foca no uso, na base de referência, nas correspondências e na verificação humana.

✗ C) Incorreta. Consentimento e parecer do encarregado não constam do Art. 12(3); faltam ainda o período de uso e a identificação de quem verificou os resultados.

> **Dica de prova:** Logs de identificação biométrica remota: quando usou, contra qual base, o que deu correspondência e quem verificou.

R2.4. C) O modelo é um modelo GPAI, e o assistente baseado nele é um sistema de IA de finalidade geral

Por quê: O Art. 3(63) define modelo de IA de finalidade geral (GPAI) como modelo que apresenta generalidade significativa, é capaz de executar com competência ampla gama de tarefas distintas e pode ser integrado em diversos sistemas ou aplicações a jusante. O Art. 3(66) define sistema de IA de finalidade geral como o sistema de IA baseado em um modelo GPAI, com capacidade de servir a várias finalidades, para uso direto ou integração em outros sistemas.

✗ A) Incorreta. A Lei da IA distingue modelo GPAI (Art. 3(63)) de sistema de IA de finalidade geral (Art. 3(66)).

✗ B) Incorreta. Os papéis estão invertidos: o modelo é o modelo GPAI, e o sistema construído sobre ele é o sistema de IA de finalidade geral.

✗ D) Incorreta. O assistente é um sistema de IA construído sobre o modelo; e licenciar o modelo não o torna, por si, componente de sistema de risco elevado.

> **Dica de prova:** Modelo GPAI = o motor (Art. 3(63)); sistema de IA de finalidade geral = o produto construído sobre ele (Art. 3(66)).

03

CAPÍTULO 3 · 12,5% DA PROVA

Domínio 3: IA confiável

Este domínio vale 12,5% (5 questões): 7,5% de privacidade e proteção de dados e 5% de transparência e rastreabilidade. Preciso aplicar os princípios do GDPR a cenários de IA (minimização, exatidão, limitação da conservação, finalidade, segurança, responsabilidade), separar pseudonimização de anonimização e conhecer DPIA, DPO, decisões automatizadas, violações de dados e transferências. Do lado da Lei da IA, caem o Art. 13 (transparência para o responsável pela implantação), o Art. 50 (chatbots, conteúdo sintético, deepfakes, emoções), os logs do Art. 12 e a base de dados do Art. 71. Onde mais erro: escolher o princípio do GDPR vizinho e trocar quem tem o dever no Art. 50 (fornecedor ou responsável pela implantação).

Neste capítulo

17 tópicos-chave · 14 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Limitação da conservação (GDPR Art. 5(1)(e))

Dados pessoais são guardados pelo menor tempo necessário para a finalidade, com prazos para apagar ou revisar. Cifrar, atualizar ou registrar o prazo na política não justifica uma guarda desproporcional. Exceção: guarda mais longa para arquivo de interesse público ou pesquisa, com medidas como anonimização ou pseudonimização.

Exatidão (GDPR Art. 5(1)(d))

Dados exatos e atualizados conforme a finalidade, com retificação ou eliminação sem demora dos inexatos. O titular pode pedir retificação (Art. 16), atendida em princípio em até 1 mês. Em IA, um dado errado na entrada ou no treino gera resultado injusto para a pessoa.

Minimização (GDPR Art. 5(1)(c))

Dados adequados, pertinentes e limitados ao necessário para a finalidade. Em IA, afeta a escolha de atributos: ganho de acurácia não justifica atributo desnecessário, pseudonimizar não autoriza coletar o irrelevante e consentimento atrelado a dado desnecessário não é livre. Dados anônimos são preferíveis quando viável.

Integridade e confidencialidade (GDPR Art. 5(1)(f) e Art. 32)

Segurança adequada ao risco contra acesso não autorizado, tratamento ilícito e perda, destruição ou dano acidentais. Medidas típicas: pseudonimização, cifragem, capacidade de restaurar a disponibilidade após incidente e testes regulares das medidas. Servidor sem controle de acesso e sem backup viola este princípio.

Limitação da finalidade

Dados coletados para uma finalidade só podem ser tratados para outra compatível. Reaproveitar dados antigos para treinar IA exige rever base legal e finalidade, minimizar, informar os titulares e, se houver risco elevado (como monitoramento sistemático de trabalhadores), fazer DPIA.

Responsabilidade (accountability, GDPR Art. 5(2) e Art. 24)

O controlador cumpre os princípios e tem de conseguir demonstrar isso a qualquer momento, não só após uma violação. Registros das atividades, DPIA e documentação das decisões servem a essa prova; códigos de conduta (Art. 40) e certificações (Art. 42) são voluntários e só ajudam. O operador age em nome do controlador e não assume essa demonstração.

Categorias especiais de dados (GDPR Art. 9)

Origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos para identificar uma pessoa de forma única, saúde e vida ou orientação sexual. O tratamento é proibido salvo hipóteses como consentimento explícito ou interesse público relevante. IP, cookie, localização e e-mail profissional são pessoais, mas não sensíveis.

Pseudonimização x anonimização

Dado pseudonimizado (nomes trocados por códigos, tabela guardada à parte) continua pessoal, pois pode ser reatribuído com informação adicional; o GDPR se aplica. Só a anonimização irreversível, em que a pessoa não é mais identificável, tira o dado do GDPR. Para o EDPB, o anonimato de um modelo de IA é avaliado caso a caso.

Proteção desde a concepção e por padrão (GDPR Art. 25)

By design: medidas técnicas e organizacionais desde as primeiras fases do projeto, como pseudonimização e cifragem. By default: a configuração inicial trata só o necessário, pelo menor prazo, com acesso restrito a quem precisa. Vale para todo controlador, independentemente de DPIA.

DPIA e DPO (GDPR Arts. 35 e 37 a 39)

DPIA é obrigatória pelo menos para avaliação sistemática e extensa com perfilagem, dados sensíveis em larga escala e monitoramento sistemático de áreas públicas em larga escala; é feita antes e, se o risco residual for alto, há consulta prévia (Art. 36). DPO é obrigatório para autoridades públicas (exceto tribunais na função jurisdicional) e quando a atividade principal é monitoramento ou perfilagem em larga escala ou dados sensíveis em larga escala.

Decisão exclusivamente automatizada (GDPR Art. 22)

O titular tem direito de não ficar sujeito a decisão só automatizada com efeitos jurídicos ou similarmente significativos, como recusa de crédito on-line. Exceções: necessidade para o contrato, lei com salvaguardas ou consentimento explícito; em todas, valem intervenção humana, ponto de vista e contestação. O Art. 86 da Lei da IA não substitui o Art. 22.

Violação de dados e transferências (GDPR Arts. 33, 34 e 45)

Violação, inclusive indisponibilidade por ransomware, é notificada à autoridade em até 72 horas, salvo improbabilidade de risco; alto risco exige avisar também os titulares. Transferência para país com decisão de adequação (por exemplo Brasil, Japão, Reino Unido, Suíça e EUA pelo Data Privacy Framework) não exige salvaguarda adicional; sem adequação, usam-se cláusulas contratuais-padrão ou regras corporativas vinculativas (estas, dentro de grupo).

Parecer 28/2024 do EDPB e Art. 4a da Lei da IA

O EDPB admite o interesse legítimo para desenvolver modelos de IA, com teste de três etapas: interesse legítimo, necessidade estrita e ponderação com os direitos dos titulares; dados públicos são só um critério. O Art. 4a (versão consolidada) permite tratar categorias especiais para detectar e corrigir vieses só se dados sintéticos ou anonimizados não bastarem, sem repasse a terceiros e com eliminação após a correção.

Dados pessoais no sandbox (Art. 59)

Reuso de dados coletados para outra finalidade só para sistemas de interesse público relevante (saúde pública, ambiente, energia, transporte, administração pública), com condições cumulativas: necessidade, ambiente funcionalmente separado e protegido, sem compartilhamento fora do sandbox, sem decisões sobre os titulares, eliminação ao final, logs e resumo público do projeto.

Transparência para o responsável pela implantação (Art. 13)

O sistema de risco elevado deve funcionar de forma suficientemente transparente para o responsável pela implantação interpretar e usar o resultado (Art. 13(1)). O fornecedor entrega instruções de uso com identidade, finalidade, exatidão e robustez, limitações, riscos previsíveis, medidas de supervisão e manutenção; não código-fonte, pesos ou dados de treino.

Obrigações de transparência do Art. 50

50(1), fornecedor: sistema que interage com pessoas informa que é IA, salvo se óbvio ou se for uso penal autorizado por lei (a ressalva não vale para canal público de denúncia). 50(2), fornecedor: saídas sintéticas marcadas em formato legível por máquina, salvo edição padrão sem mudança substancial. 50(3), responsável pela implantação: informar expostos a reconhecimento de emoções ou categorização biométrica. 50(4), responsável pela implantação: divulgar deepfakes e textos de interesse público, salvo revisão humana com responsabilidade editorial. 50(5): informação clara, distinguível, acessível e no máximo na primeira interação.

Rastreabilidade: logs e base de dados da UE (Arts. 12 e 71)

Os logs automáticos ao longo da vida útil permitem identificar riscos ou modificações substanciais, apoiar o pós-comercialização e o monitoramento pelo responsável pela implantação. A base de dados da UE, mantida pela Comissão como controladora, é pública por regra e legível por máquina; ficam restritos a seção não pública do Art. 49(4) e os registros de testes em condições reais. Ela registra sistemas de risco elevado, não modelos GPAI nem decisões individuais.

Macetes para memorizar

💡 Princípios do GDPR no cenário

Errado = Exatidão; Tempo = Conservação; Quantidade = Minimização; Acesso ou perda = Segurança; Novo uso = Finalidade; Não consigo provar = Responsabilidade.

💡 By design x by default

Design é o que se constrói no projeto; Default é como o sistema sai da fábrica.

💡 Pseudônimo

Pseudônimo é apelido: quem tem a tabela sabe quem é.

💡 Prazos de dados

72 horas para violação, 1 mês para responder ao titular.

Quem faz o quê no Art. 50

Parágrafos 1 e 2 são do Fornecedor (Faz o sistema); 3 e 4 são de quem implanta (Informa o público); 5 diz Como e Quando.

Exceções do Art. 50(4)

Deepfake artístico: avisa sem estragar. Texto de notícia: dispensa se um editor assina.

Tabela de memorização: não confunda

Quando é...	...e quando é
Pseudonimização Ainda dá para reidentificar com informação adicional: dado pessoal, GDPR se aplica; é medida de segurança e de by design.	**Anonimização** Irreversível, a pessoa não é mais identificável: fora do GDPR.
Proteção desde a concepção (by design) Medidas embutidas no projeto, como pseudonimizar e cifrar.	**Proteção por padrão (by default)** Configuração inicial mais protetora: só o necessário, pelo menor prazo, acesso restrito de fábrica.
Violação de dados (GDPR) Controlador notifica a autoridade de proteção de dados em até 72 horas.	**Incidente grave (Lei da IA)** Fornecedor notifica a autoridade de fiscalização do mercado em até 15 dias (regra geral), 10 ou 2 dias.
Art. 50(1) e 50(2): deveres do fornecedor Projetar o chatbot para avisar que é IA e marcar saídas sintéticas de forma legível por máquina.	**Art. 50(3) e 50(4): deveres do responsável pela implantação** Informar quem é exposto a reconhecimento de emoções e divulgar deepfakes e textos de interesse público.
Transparência do Art. 13 da Lei da IA Fornecedor informa o responsável pela implantação por instruções de uso (exatidão, limitações, supervisão).	**Transparência do GDPR (Arts. 12 a 14)** Controlador informa o titular: finalidades, base legal, prazo, direitos e a existência de decisão automatizada com a lógica e as consequências; dados diretos, no momento da coleta.
Minimização Quais e quantos dados tratar.	**Limitação da conservação** Por quanto tempo guardar.

Números que caem

Item	Valor
Notificação de violação de dados à autoridade (GDPR)	**até 72 horas**
Resposta a pedido de titular, como retificação	**em princípio, até 1 mês**
Informar titular quando os dados vêm de outra fonte	**até um mês ou no primeiro contato**
Parecer do EDPB sobre modelos de IA	**Parecer 28/2024 (dezembro de 2024)**
Teste do interesse legítimo para IA	**3 etapas**

Peso do domínio	**12,5% (3.1: 7,5%; 3.2: 5%)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** Cifrar os currículos torna proporcional a guarda por dez anos.
Como não cair: Cifragem é segurança; o prazo continua limitado pela finalidade (limitação da conservação).

⚠ **Alerta de prova:** Dado inexato pode ficar até o fim do prazo de retenção ou ser resolvido com novo consentimento.
Como não cair: Exatidão exige retificar ou apagar sem demora; prazo de guarda e consentimento não corrigem dado errado.

⚠ **Alerta de prova:** Pseudonimizar todos os atributos permite usar o conjunto completo.
Como não cair: Pseudonimizado continua pessoal; a minimização corta o atributo desnecessário, como a origem racial.

⚠ **Alerta de prova:** Trocar nomes por códigos e guardar a tabela no hospital é anonimização.
Como não cair: É pseudonimização: a reidentificação ainda é possível.

⚠ **Alerta de prova:** Consentimento explícito dispensa as salvaguardas do Art. 22 do GDPR.
Como não cair: Consentimento só autoriza a decisão automatizada; intervenção humana, ponto de vista e contestação continuam.

⚠ **Alerta de prova:** A violação por ransomware em hospital segue o prazo de 2 ou 15 dias.
Como não cair: Esses prazos são do Art. 73 da Lei da IA; o GDPR fixa 72 horas.

⚠ **Alerta de prova:** Para o Brasil é preciso usar cláusulas contratuais-padrão ou regras corporativas vinculativas.
Como não cair: O Brasil tem decisão de adequação; regras corporativas vinculativas servem a transferências dentro de um grupo.

⚠ **Alerta de prova:** Modelo treinado é anônimo por definição, ou dados públicos dispensam a ponderação.
Como não cair: Anonimato do modelo é avaliado caso a caso, e dado público é só um critério da expectativa razoável.

⚠ **Alerta de prova:** Para corrigir vieses com dados de origem étnica basta autorização do Gabinete de IA, e os dados podem ir a auditor externo.
Como não cair: O Art. 4a não prevê autorização; proíbe repasse a terceiros e manda apagar após a correção.

⚠ **Alerta de prova:** Obra satírica com deepfake fica isenta de divulgação, ou precisa de aviso permanente em cada cena.
Como não cair: A divulgação continua, mas de modo adequado que não prejudique a fruição da obra.

⚠ **Alerta de prova:** Notícia gerada por IA e revisada por editor responsável precisa ser rotulada.
Como não cair: O Art. 50(4) dispensa quando há revisão humana ou controle editorial com responsabilidade editorial.

⚠ **Alerta de prova:** Chatbot de denúncia da polícia fica fora do Art. 50(1) por ser uso penal autorizado.
Como não cair: A exceção penal não vale para sistemas disponíveis ao público para denunciar infrações.

⚠ **Alerta de prova:** Quem informa os visitantes sobre reconhecimento de emoções é o fornecedor, ou basta cumprir o GDPR.
Como não cair: Art. 50(3): o responsável pela implantação informa; o GDPR soma-se, não substitui.

⚠ **Alerta de prova:** Avisar que é IA por e-mail depois da ligação, ou na política de privacidade, cumpre a transparência.
Como não cair: Art. 50(5): de forma clara e distinguível, no máximo na primeira interação.

Como cai na prova

📝 **Como cai:** Cenário de empresa europeia tratando dados para IA e pergunta 'qual princípio do GDPR está em jogo'.
Como resolver: Ache o verbo do problema: guardar demais (conservação), dado errado (exatidão), dado sobrando (minimização), exposição ou perda (integridade e confidencialidade), novo uso (finalidade), falta de prova (responsabilidade). As erradas trazem o princípio vizinho com uma medida que parece boa.

📝 **Como cai:** Lista de quatro dados ou quatro organizações para achar o dado sensível, quem precisa de DPO ou DPIA.
Como resolver: Use os exemplos de 'não obrigatório': médico de família ou de bairro, pequeno escritório, loja que só executa o contrato. Procure larga escala, perfilagem sistemática ou biometria para identificação única.

📝 **Como cai:** Cenário de transparência do Art. 50 pedindo se o dever se aplica e quem o cumpre.
Como resolver: 1) Identifique o parágrafo: interação (1), conteúdo sintético (2), emoções ou biometria (3), deepfake ou texto (4). 2) Defina o titular do dever. 3) Teste as exceções: óbvio pelo contexto, uso penal autorizado (com a ressalva da denúncia), edição padrão, obra artística, revisão editorial.

📝 **Como cai:** Pergunta que mistura GDPR e Lei da IA (prazos, explicação, avaliações).
Como resolver: Separe os regimes: 72 horas e Art. 22 são GDPR; 15 dias, Art. 86 e Art. 13 são Lei da IA. Um não substitui o outro.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
guardar dados por prazo longo para treinar modelo futuro	**limitação da conservação**
dado sobre a pessoa está errado ou foi declarado indevido	**exatidão: retificar ou apagar sem demora**
escolha de atributos do modelo, incluindo dado que não serve à finalidade	**minimização**
servidor sem controle de acesso ou sem cópia de segurança	**integridade e confidencialidade (Art. 32)**
dados coletados há anos, agora usados para treinar IA	**limitação da finalidade, revisão da base legal, informar titulares e DPIA**
cumpre o GDPR mas não tem registros das avaliações	**responsabilidade: cumprir e demonstrar**
impressão digital para identificar de forma única	**dado biométrico sensível (Art. 9)**
nomes trocados por códigos, tabela guardada pelo hospital	**pseudonimização: continua dado pessoal**
empréstimo on-line aprovado ou recusado sem análise humana	**Art. 22 do GDPR: intervenção humana, ponto de vista e contestação**
atividade principal é traçar perfis com IA	**DPO obrigatório; DPIA para perfilagem sistemática e extensa**
médicos não entendem as pontuações do sistema de risco elevado	**Art. 13(1): transparência para o responsável pela implantação**
corretor que ajusta ortografia sem mudar o sentido	**exceção à marcação legível por máquina do Art. 50(2)**
reconstruir o que o sistema fez após um incidente	**rastreabilidade pelos logs do Art. 12**

jornalista consulta a base de dados da UE	**Art. 71: pública por regra, com seção não pública e testes reais restritos**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Pseudonimizado continua dado pessoal; só a anonimização irreversível sai do GDPR.
- 72 horas é violação de dados no GDPR; incidente grave da Lei da IA tem outros prazos.
- Art. 50: 1 e 2 são do fornecedor, 3 e 4 do responsável pela implantação, 5 define forma e momento (primeira interação).
- Responsabilidade é cumprir e conseguir demonstrar; código de conduta ajuda, mas é voluntário.
- Art. 13 é transparência do fornecedor para o responsável pela implantação; explicação à pessoa afetada é o Art. 86.

Essenciais para a prova (checklist)

- ☐ Sei identificar o princípio do GDPR violado em um cenário de IA.
- ☐ Sei listar as categorias especiais do Art. 9 do GDPR e reconhecer dados pessoais comuns.
- ☐ Sei diferenciar pseudonimização e anonimização.
- ☐ Sei separar proteção desde a concepção e por padrão.
- ☐ Sei quando DPIA e DPO são obrigatórios.
- ☐ Sei as salvaguardas do Art. 22 do GDPR.
- ☐ Sei o prazo de 72 horas e a lógica das decisões de adequação.
- ☐ Sei as condições do Art. 4a e do Art. 59 para dados pessoais em IA.
- ☐ Sei quem cumpre cada parágrafo do Art. 50 e suas exceções.
- ☐ Sei para que servem os logs do Art. 12 e o que é público na base do Art. 71.

Questões de revisão do capítulo

R3.1 · Domínio 3: IA confiável

A autoridade de proteção de dados pede a uma seguradora belga que comprove a conformidade do tratamento feito por seu sistema de IA de subscrição. A seguradora responde que cumpre o GDPR, mas não tem registros das avaliações feitas. Qual afirmação descreve o princípio em jogo?

A. O controlador só precisa demonstrar a conformidade depois de uma violação de dados notificada à autoridade
B. O operador que hospeda o modelo é quem demonstra a conformidade, pois guarda os registros técnicos do tratamento
C. O controlador responde pelo cumprimento dos princípios e deve ser capaz de demonstrá-lo quando solicitado
D. O controlador cumpre o princípio ao aderir a um código de conduta aprovado, que é obrigatório no setor de seguros

R3.2 · Domínio 3: IA confiável

Que obrigação o AI Act impõe aos fornecedores de sistemas de IA que geram áudio, imagem, vídeo ou texto sintéticos?

A. Limitar a geração a conteúdos destinados ao uso interno das empresas
B. Marcar as saídas em formato legível por máquina como geradas por IA
C. Submeter cada conteúdo gerado à aprovação da autoridade nacional
D. Registrar cada conteúdo gerado em uma base de dados pública europeia

R3.3 · Domínio 3: IA confiável

Pelo AI Act, o que o fornecedor de um sistema de IA de risco elevado deve entregar aos responsáveis pela implantação para que eles o usem corretamente?

A. A lista atualizada de clientes que já utilizam o sistema
B. Instruções de uso com finalidade, desempenho e limitações
C. Uma cópia integral dos dados pessoais usados no treino do modelo
D. O código-fonte completo do modelo e seus pesos treinados

R3.4 · Domínio 3: IA confiável

Um hospital da Bélgica entrega a uma empresa de IA um conjunto de prontuários em que os nomes foram trocados por códigos. O hospital guarda a tabela que liga cada código ao paciente. Como o GDPR trata esse conjunto nas mãos da empresa?

A. Deixam de ser dados pessoais, pois a tabela de correspondência fica com o hospital, e não com a empresa
B. Continuam dados pessoais, pois a pseudonimização ainda permite reidentificar os pacientes
C. Continuam dados pessoais só até o fim do treino, quando o modelo resultante passa a ser anônimo
D. Deixam de ser dados pessoais, pois a troca de nomes por códigos equivale a uma anonimização

Respostas comentadas

R3.1. C) O controlador responde pelo cumprimento dos princípios e deve ser capaz de demonstrá-lo quando solicitado

Por quê: O princípio da responsabilidade (accountability), Art. 5(2) e Art. 24 do GDPR, é pedra angular do regulamento: o controlador cumpre os princípios e demonstra o cumprimento. Registros das atividades de tratamento, DPIA e documentação das decisões servem a essa demonstração; códigos de conduta (Art. 40) e certificações (Art. 42) são voluntários e ajudam a prová-la.

✗ A) Incorreta. O dever de demonstrar a conformidade é permanente e não depende de uma violação de dados ter ocorrido.
✗ B) Incorreta. O operador trata dados em nome do controlador, segundo instruções documentadas; a demonstração do cumprimento dos princípios cabe ao controlador.
✗ D) Incorreta. Códigos de conduta e certificações são instrumentos voluntários que ajudam a demonstrar a conformidade, mas não são obrigatórios nem substituem o cumprimento.

> **Dica de prova:** Responsabilidade = cumprir E conseguir demonstrar. Código de conduta ajuda, mas é voluntário.

R3.2. B) Marcar as saídas em formato legível por máquina como geradas por IA

Por quê: O artigo 50(2) exige que fornecedores de sistemas de IA que geram áudio, imagem, vídeo ou texto sintéticos marquem as saídas em formato legível por máquina e detectável como geradas ou manipuladas artificialmente, com soluções técnicas eficazes e interoperáveis, como marcas d'água ou metadados. Há exceções para funções de edição de apoio que não alteram substancialmente o conteúdo.

✗ A) Incorreta. A lei não restringe a geração ao uso interno.
✗ C) Incorreta. Não há aprovação prévia de conteúdos pela autoridade.
✗ D) Incorreta. Conteúdos gerados não são registrados em base pública.

> **Dica de prova:** Fornecedor de IA generativa: saídas marcadas como geradas por IA, legíveis por máquina.

R3.3. B) Instruções de uso com finalidade, desempenho e limitações

Por quê: O artigo 13 exige que sistemas de risco elevado sejam suficientemente transparentes para que os responsáveis pela implantação interpretem e usem os resultados de forma adequada. Para isso, o fornecedor entrega instruções de uso com sua identidade, finalidade prevista, nível de exatidão e robustez, limitações conhecidas, riscos previsíveis, medidas de supervisão humana e manutenção necessária.

✗ A) Incorreta. Lista de clientes não ajuda a usar o sistema e não é exigida.

✗ C) Incorreta. Entregar dados pessoais de treino violaria a proteção de dados.

✗ D) Incorreta. A lei não exige entregar código-fonte ou pesos ao responsável pela implantação.

> **Dica de prova:** Transparência para o responsável pela implantação: instruções de uso claras e completas.

R3.4. B) Continuam dados pessoais, pois a pseudonimização ainda permite reidentificar os pacientes

Por quê: Pelo Art. 4(1) e (5) e pelo Considerando 26 do GDPR, dados pseudonimizados continuam dados pessoais, pois podem ser atribuídos a uma pessoa com informação adicional. Só dados tornados anônimos de forma irreversível, em que a pessoa não é mais identificável, ficam fora do GDPR. A pseudonimização é uma medida de segurança e de proteção desde a concepção.

✗ A) Incorreta. Para a Comissão, dado pseudonimizado que pode ser usado para reidentificar a pessoa continua sendo dado pessoal; guardar a tabela em outro lugar é uma salvaguarda, e não anonimização.

✗ C) Incorreta. O fim do treino não muda a natureza do conjunto, e, para o EDPB, o anonimato de um modelo é avaliado caso a caso, conforme a probabilidade de identificar pessoas ou extrair seus dados.

✗ D) Incorreta. Trocar nomes por códigos é pseudonimização; para haver anonimização, a pessoa não pode mais ser identificada e o processo tem de ser irreversível.

> **Dica de prova:** Pseudonimizado = ainda pessoal (GDPR se aplica). Anonimizado de forma irreversível = fora do GDPR.

04

CAPÍTULO 4 · 10% DA PROVA

Domínio 4: IA ética

Vale 10% (4 questões): princípios e diretrizes éticas e direitos humanos. Preciso conhecer as Orientações Éticas do HLEG (quatro princípios, sete requisitos, tensões entre princípios, HITL/HOTL/HIC, ALTAI), os Princípios da OCDE e, na Lei da IA, a supervisão humana do Art. 14, a avaliação de impacto sobre os direitos fundamentais do Art. 27 e os direitos das pessoas (informação do Art. 26(11), reclamação do Art. 85, explicação do Art. 86). As questões trazem cenários e pedem o princípio afetado ou a regra exata do artigo. Onde mais erro: confundir os princípios do HLEG entre si, trocar 14(3)(a) por 14(3)(b) e esquecer quem está obrigado à avaliação de impacto.

Neste capítulo
16 tópicos-chave · 14 pegadinhas · 6 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Orientações Éticas para uma IA de Confiança (HLEG, 2019)

Documento do grupo de peritos de alto nível da Comissão, sem força de lei. O considerando 27 da Lei da IA reconhece seus sete princípios como base para IA confiável e para códigos de conduta voluntários. Podem estruturar a governança interna, mas não substituem requisitos legais nem dão presunção de conformidade; valem para todos os setores.

Quatro princípios éticos do HLEG

Respeito pela autonomia humana (a IA não subordina, coage, engana, manipula nem condiciona; amplia capacidades e preserva escolha real); prevenção de danos (não causar nem agravar danos físicos, mentais ou sociais, com atenção a vulneráveis); equidade (dimensão substantiva: distribuição justa de benefícios e custos; dimensão processual: contestar e obter reparação); explicabilidade (processos transparentes e decisões explicáveis a quem é afetado).

Sete requisitos de IA confiável (HLEG)

Ação e supervisão humanas; robustez técnica e segurança; privacidade e governança de dados; transparência; diversidade, não discriminação e equidade; bem-estar social e ambiental; responsabilização. Sigilo sobre a lógica, autonomia plena e retorno financeiro não são requisitos.

Tensões entre princípios (HLEG, seção 2.3)

Não há hierarquia fixa: o exemplo é o policiamento preditivo, que opõe prevenção de danos e autonomia. Pede deliberação responsável, reflexão fundamentada em evidências, trade-off explicitamente reconhecido, avaliado e documentado, com revisão contínua. Sem trade-off aceitável, o sistema não segue naquela forma; a dignidade humana é absoluta e não entra em ponderação.

HITL, HOTL e HIC

Human-in-the-loop: intervenção em cada ciclo de decisão, muitas vezes inviável. Human-on-the-loop: intervenção no ciclo de projeto e monitoramento da operação. Human-in-command: supervisão da atividade global e decisão sobre quando e como usar, inclusive não usar ou anular. Quanto menos supervisão humana, mais testes e governança rigorosa.

ALTAI

Assessment List for Trustworthy AI, de 17/07/2020, do HLEG: lista de autoavaliação que traduz os sete requisitos em passos concretos, em PDF e ferramenta web. Não é norma harmonizada, não certifica e não é o questionário de avaliação de impacto do Gabinete de IA.

Princípios da OCDE para IA

De 2019, atualizados em maio de 2024. Cinco princípios baseados em valores: crescimento inclusivo, desenvolvimento sustentável e bem-estar; direitos humanos e valores democráticos (com equidade e privacidade); transparência e explicabilidade; robustez, segurança e proteção; responsabilização. Cinco recomendações a governos: P&D, ecossistema inclusivo, governança interoperável, capacidade humana e mercado de trabalho, cooperação internacional. A UE usa a definição de sistema de IA da OCDE.

Supervisão humana efetiva (Art. 14)

Sistemas de risco elevado são projetados para que pessoas capacitadas entendam capacidades e limites, percebam o viés de automação, interpretem os resultados e possam não usar, anular, reverter ou interromper o sistema. Assinar decisões sem acesso à informação é supervisão formal, não efetiva; controle remoto do fornecedor ou pesquisa de satisfação não servem.

Medidas de supervisão do Art. 14(3)

Proporcionais aos riscos, à autonomia e ao contexto, de dois tipos: (a) identificadas e integradas no sistema pelo fornecedor; (b) identificadas pelo fornecedor para o responsável pela implantação aplicar. As duas são definidas antes da colocação no mercado ou em serviço e descritas nas instruções de uso (Art. 13(3)(d)).

Capacidades do Art. 14(4) e dupla verificação do Art. 14(5)

O supervisor deve entender e monitorar o sistema, estar ciente do viés de automação (alínea b), interpretar o resultado, decidir não usar ou anular, e intervir ou interromper com botão de parada que leve a estado seguro (alínea e). Para identificação biométrica remota do Anexo III 1(a), nenhuma ação sem verificação separada por pelo menos duas pessoas competentes, salvo em aplicação da lei, migração, fronteiras ou asilo quando o direito a considerar desproporcional.

Quem faz a avaliação de impacto sobre os direitos fundamentais (Art. 27(1))

Antes de implantar sistema de risco elevado do Art. 6(2): organismos de direito público, entidades privadas que prestam serviços públicos e responsáveis pela implantação de sistemas de crédito (Anexo III 5(b)) e de seguros de vida e de saúde (5(c)). Sistemas do ponto 2 do Anexo III (infraestrutura crítica) ficam de fora.

Conteúdo e ciclo da avaliação de impacto (Art. 27)

Conteúdo: processos de uso, período e frequência, categorias de pessoas afetadas, riscos específicos (com as informações do Art. 13), medidas de supervisão humana e medidas se os riscos se materializarem, com governança e reclamações. Vale para o primeiro uso e é atualizada quando um elemento muda (27(2)), sem prazo fixo; os resultados são notificados à autoridade de fiscalização do mercado com o modelo do Gabinete de IA (27(3) e 27(5)). Pode remeter à DPIA ou incluir partes dela (27(4)).

Direitos das pessoas: Arts. 26(11), 85 e 86

Art. 26(11): quem implanta sistema do Anexo III que decide ou ajuda a decidir sobre pessoas as informa de que estão sujeitas a ele, mesmo que a IA só auxilie. Art. 85: qualquer pessoa física ou jurídica com motivos pode reclamar à autoridade de fiscalização do mercado, sem precisar ser afetada. Art. 86: a pessoa afetada por decisão com efeitos jurídicos ou impacto significativo obtém do responsável pela implantação explicação clara do papel da IA e dos principais elementos da decisão; não inclui código-fonte nem indenização automática.

Discriminação indireta

Critério aparentemente neutro (como interrupção de carreira acima de dois anos) que prejudica de forma desproporcional certos grupos. Vir de dados históricos não o torna aceitável; pede revisão de variáveis e rótulos, medição do impacto e salvaguardas. Em recrutamento (Anexo III ponto 4), o Art. 10 exige exame de vieses nos dados.

Acessibilidade e desenho universal

Fazem parte do requisito de diversidade, não discriminação e equidade do HLEG: sistemas utilizáveis por todos, independentemente de idade, gênero ou capacidades. Na Lei da IA, o Art. 16(l) exige do fornecedor de risco elevado os requisitos de acessibilidade das Diretivas 2016/2102 e 2019/882.

Usuários vulneráveis em contexto emocional

Prevenção de danos pede detectar sinais de vulnerabilidade e encaminhar a apoio humano ou recursos de ajuda. Esconder que é IA viola a transparência e o Art. 50(1); respostas impessoais ou limite de horário não protegem quem está em crise.

Macetes para memorizar

💡 Quatro princípios do HLEG

APEE: Autonomia, Prevenção de danos, Equidade, Explicabilidade.

💡 Sete requisitos do HLEG

Começa no humano (ação e supervisão humanas) e termina na prestação de contas (responsabilização); no meio, R-P-T-E-B: Robustez, Privacidade, Transparência, Equidade, Bem-estar.

💡 HITL, HOTL, HIC

IN the loop = em cada decisão; ON the loop = de cima, no projeto e no monitoramento; IN command = no comando, decide se usa.

💡 Quem faz a avaliação do Art. 27

Público, privado que presta serviço público, Crédito e Corpo (vida e saúde). Infraestrutura fica fora.

💡 Arts. 85 e 86

85 = Qualquer um reclama; 86 = só o afetado pede explicação.

💡 Art. 14(5)

Biometria remota: dois olhos humanos antes de agir.

Tabela de memorização: não confunda

Quando é...	...e quando é
Human-on-the-loop (HOTL) Analistas acompanham a operação e ajustam regras e limiares no ciclo de projeto, sem aprovar cada alerta.	**Human-in-the-loop (HITL)** Uma pessoa intervém em cada ciclo de decisão do sistema.
Human-in-command (HIC) Supervisão da atividade global e decisão de se, quando e como usar o sistema.	**Human-on-the-loop (HOTL)** Monitoramento da operação com intervenção no projeto.
Reclamação (Art. 85) Qualquer pessoa física ou jurídica, mesmo não afetada, reclama à autoridade de fiscalização do mercado.	**Explicação (Art. 86)** Só a pessoa afetada por decisão de sistema do Anexo III pede explicação ao responsável pela implantação.
Avaliação de impacto sobre os direitos fundamentais (Art. 27) Obrigação da Lei da IA para certos responsáveis pela implantação, notificada à autoridade de fiscalização do mercado.	**DPIA (Art. 35 do GDPR)** Obrigação do GDPR para tratamento de alto risco; pode ser citada ou ter partes incluídas na avaliação do Art. 27, sem substituí-la.
Art. 14(3)(a) Medida que o fornecedor embute no sistema, como tela com grau de confiança.	**Art. 14(3)(b)** Medida que o fornecedor indica para o responsável pela implantação aplicar, como dupla revisão humana.
Respeito pela autonomia humana A IA tira a escolha humana, manipula ou condiciona pessoas (operador sem margem de decisão).	**Prevenção de danos** Risco de dano físico, mental ou social, dignidade, segurança e robustez, atenção a vulneráveis.
Princípios da OCDE baseados em valores Crescimento inclusivo, direitos humanos, transparência e explicabilidade, robustez e segurança, responsabilização.	**Recomendações da OCDE aos governos** Investir em P&D, ecossistema inclusivo, governança interoperável, capacidade humana, cooperação internacional.

Números que caem

Item	Valor
Orientações Éticas do HLEG	**2019**
ALTAI	**17/07/2020**
Princípios da OCDE para IA	**2019, atualizados em maio de 2024**
Princípios e requisitos do HLEG	**4 princípios e 7 requisitos**
Princípios da OCDE	**5 princípios baseados em valores e 5 recomendações**
Verificação separada na biometria remota (Art. 14(5))	**pelo menos duas pessoas**
Peso do domínio	**10% (4.1: 5%; 4.2: 5%)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** O botão de parada resolve a confiança excessiva dos radiologistas na IA.
Como não cair: O risco é o viés de automação (Art. 14(4)(b)); o botão de parada serve para interromper com segurança.

⚠ **Alerta de prova:** Toda identificação de risco elevado exige verificação por duas pessoas, ou só abaixo de um limiar de confiança.
Como não cair: A dupla verificação é só para identificação biométrica remota do Anexo III 1(a) e vale para qualquer correspondência usada como base de ação.

⚠ **Alerta de prova:** Concessionária privada de água com componente de segurança deve fazer avaliação de impacto sobre direitos fundamentais.
Como não cair: Infraestrutura crítica (ponto 2 do Anexo III) fica fora do Art. 27.

⚠ **Alerta de prova:** Seguradora privada não precisa da avaliação de impacto por não ser pública.
Como não cair: Crédito (5(b)) e seguros de vida e saúde (5(c)) estão expressamente obrigados, mesmo privados.

⚠ **Alerta de prova:** A avaliação de impacto é revista a cada ano, ou nunca mais depois do primeiro uso.
Como não cair: Não há prazo fixo: atualiza-se quando um elemento muda, como pessoas afetadas ou frequência.

⚠ **Alerta de prova:** A avaliação de impacto vai ao fornecedor, é publicada na base da UE ou enviada à autoridade de dados em 72 horas.
Como não cair: Os resultados são notificados à autoridade de fiscalização do mercado com o modelo do Gabinete de IA.

⚠ **Alerta de prova:** A DPIA substitui a avaliação de impacto, ou não pode ser aproveitada.
Como não cair: Art. 27(4): remete-se à DPIA ou incluem-se partes dela; as duas se complementam.

⚠ **Alerta de prova:** Para reclamar pelo Art. 85 a associação precisa provar que algum associado foi afetado, ou deve reclamar ao Gabinete de IA.
Como não cair: Qualquer pessoa com motivos reclama, sem ser afetada, à autoridade de fiscalização do mercado.

⚠ **Alerta de prova:** O Art. 26(11) exige consentimento dos estudantes ou só vale para decisão exclusivamente automatizada.
Como não cair: Exige informar, e vale também quando a IA só auxilia a decisão.

⚠ **Alerta de prova:** O HLEG tem hierarquia fixa em que a prevenção de danos vence, ou a dignidade pode ceder ao benefício coletivo.
Como não cair: Não há hierarquia: pondera-se e documenta-se; a dignidade humana não entra em ponderação.

⚠ **Alerta de prova:** Seguir as Orientações do HLEG dá presunção de conformidade ou substitui os requisitos da Lei da IA.
Como não cair: São voluntárias; presunção só vem de normas harmonizadas publicadas no Jornal Oficial.

⚠ **Alerta de prova:** A ALTAI é lista da OCDE, norma harmonizada ou o questionário do Art. 27.
Como não cair: É a autoavaliação do HLEG de 2020 baseada nos sete requisitos.

⚠ **Alerta de prova:** Critério tirado de dados históricos é objetivo e pode ser mantido se explicado ou trocado por regras fixas.
Como não cair: Critério neutro com efeito desproporcional é discriminação indireta; explicar ou trocar a técnica não corrige.

⚠ **Alerta de prova:** Investir em P&D ou capacitar a força de trabalho são princípios de valores da OCDE.
Como não cair: São recomendações aos formuladores de políticas; transparência e explicabilidade é princípio de valor.

Como cai na prova

📝 **Como cai:** Cenário ético e pergunta 'qual princípio do HLEG é afetado'.
Como resolver: Identifique o problema central: sem escolha ou manipulação (autonomia), dano ou vulnerabilidade (prevenção de danos), tratamento desigual ou falta de contestação (equidade), opacidade (explicabilidade). As erradas descrevem corretamente outro princípio que não é o ponto do caso.

📝 **Como cai:** Lista de quatro responsáveis pela implantação para achar quem NÃO faz a avaliação de impacto.
Como resolver: Marque os obrigados: público, privado em serviço público, crédito, seguros de vida e saúde. A sobra costuma ser infraestrutura crítica.

📝 **Como cai:** Cenário de supervisão humana com alternativas citando 14(3), 14(4), 14(5) e 13(3).
Como resolver: Pergunte: é sobre projeto da medida (14(3)), capacidade do supervisor (14(4)) ou biometria remota (14(5))? Métricas de acurácia nas instruções são 13(3), não supervisão.

📝 **Como cai:** Pessoa ou entidade quer agir contra um sistema e a pergunta é a via correta.
Como resolver: Afetado por decisão do Anexo III: explicação (Art. 86) perante o responsável pela implantação. Qualquer um com motivos: reclamação (Art. 85) à autoridade de fiscalização. Informação prévia: Art. 26(11). Retirar do mercado é medida de autoridade, não direito individual.

📝 **Como cai:** Uso das Orientações do HLEG, ALTAI ou OCDE em empresa sujeita à Lei da IA.
Como resolver: São referências voluntárias: servem à governança e à autoavaliação, sem presunção de conformidade e sem substituir requisitos legais.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
profissionais aceitam quase sempre a sugestão da IA sem examinar	**viés de automação, Art. 14(4)(b)**
identificação biométrica remota aponta uma correspondência antes de barrar alguém	**verificação separada por pelo menos duas pessoas (Art. 14(5))**
fornecedor embute tela de confiança e recomenda dupla revisão ao cliente	**Art. 14(3)(a) e 14(3)(b)**
analistas não aprovam cada alerta, mas monitoram e ajustam limiares	**human-on-the-loop**
IA define cada movimento do operador, sem margem de escolha	**respeito pela autonomia humana**
contestar decisões e obter reparação	**equidade, dimensão processual**
policiamento preditivo opõe prevenção de danos e autonomia	**tensão entre princípios: ponderar, documentar, revisar**
interface inacessível a leitores de tela	**diversidade, não discriminação e equidade (HLEG) + Art. 16(l)**
ferramenta prática para verificar os sete requisitos passo a passo	**ALTAI**
banco ou seguradora de vida e saúde vai implantar sistema de risco elevado	**avaliação de impacto sobre os direitos fundamentais (Art. 27)**
avaliação de impacto concluída, qual o próximo passo	**notificar a autoridade de fiscalização do mercado com o modelo preenchido**
crédito negado por sistema de risco elevado, pessoa quer entender	**direito à explicação (Art. 86)**

associação não afetada suspeita de infração	**reclamação à autoridade de fiscalização do mercado (Art. 85)**
critério neutro afeta de forma desproporcional cuidadores	**discriminação indireta: rever variáveis e mitigar**

🎯 Se você lembrar de só uma coisa deste capítulo...

- HLEG: 4 princípios (autonomia, prevenção de danos, equidade, explicabilidade) e 7 requisitos; voluntários e sem presunção de conformidade.
- Avaliação de impacto do Art. 27: público, privado em serviço público, crédito e seguros de vida e saúde; infraestrutura crítica fora; notificada à autoridade de fiscalização do mercado.
- Art. 14(5): duas pessoas só na identificação biométrica remota do Anexo III 1(a).
- Art. 85 qualquer um reclama; Art. 86 o afetado pede explicação; Art. 26(11) informa mesmo se a IA só auxilia.

Essenciais para a prova (checklist)

- ☐ Sei os quatro princípios éticos do HLEG e as duas dimensões da equidade.
- ☐ Sei listar os sete requisitos de IA confiável.
- ☐ Sei como o HLEG trata tensões entre princípios.
- ☐ Sei diferenciar HITL, HOTL e HIC.
- ☐ Sei o que é a ALTAI e o que ela não é.
- ☐ Sei separar princípios e recomendações da OCDE.
- ☐ Sei as medidas e capacidades dos Arts. 14(3), 14(4) e 14(5).
- ☐ Sei quem faz, o que contém e quando se atualiza a avaliação do Art. 27.
- ☐ Sei distinguir os direitos dos Arts. 26(11), 85 e 86.

Questões de revisão do capítulo

R4.1 · Domínio 4: IA ética

Um sistema de IA de risco elevado é usado para apoiar a concessão de benefícios sociais. Segundo o AI Act, o que a supervisão humana exigida para esse tipo de sistema deve permitir?

A. Que um servidor assine cada decisão, mesmo sem acesso às informações usadas pelo sistema
B. Que pessoas capacitadas entendam os resultados e possam interromper ou anular o sistema
C. Que o fornecedor acompanhe remotamente o uso e altere as decisões tomadas pelo órgão
D. Que os cidadãos afetados avaliem o sistema por meio de uma pesquisa anual de satisfação

R4.2 · Domínio 4: IA ética

Nas Orientações Éticas para uma IA de Confiança do grupo de peritos de alto nível (HLEG), o princípio da prevenção de danos está mais diretamente associado a qual preocupação?

A. Assegurar que as pessoas possam contestar decisões e obter reparação efetiva
B. Evitar que a IA cause ou agrave danos físicos, mentais ou sociais a pessoas
C. Permitir que as pessoas entendam como o sistema chegou a uma decisão
D. Distribuir de forma justa e igual os benefícios e os custos dos sistemas de IA

R4.3 · Domínio 4: IA ética

Uma organização usa redes neurais profundas num sistema de IA de risco elevado e discute como tratar a explicabilidade. Qual abordagem está alinhada ao conceito de IA confiável?

A. Limitar a explicabilidade a logs e documentação de código, sem pensar em quem receberá a explicação
B. Vetar modelos complexos e usar árvores de decisão simples, mesmo com grande perda de acurácia
C. Substituir as explicações por métricas de desempenho, como precisão e recall, após testes extensos
D. Adaptar o grau de explicação ao risco, ao contexto e ao público, com documentação e técnicas pós-hoc

R4.4 · Domínio 4: IA ética

Uma empresa de segurança de um estádio na Holanda usa, conforme a lei nacional, um sistema de identificação biométrica remota (Anexo III, ponto 1(a)) para identificar torcedores banidos. O sistema aponta uma correspondência na entrada. Pelo Art. 14(5) da Lei da IA, o que é necessário antes de barrar a pessoa?

A. Confirmação por uma pessoa competente, desde que o sistema registre o período de cada uso
B. Autorização prévia de autoridade judiciária para cada identificação feita pelo sistema no estádio
C. Verificação por duas pessoas quando a confiança da correspondência ficar abaixo do limiar fixado
D. Verificação e confirmação separadas da identificação por pelo menos duas pessoas competentes

Respostas comentadas

R4.1. B) Que pessoas capacitadas entendam os resultados e possam interromper ou anular o sistema

Por quê: O artigo 14 do AI Act exige que sistemas de risco elevado sejam projetados para supervisão humana efetiva. As pessoas designadas devem ter competência e autoridade para entender capacidades e limites do sistema, perceber o viés de automação, interpretar os resultados e decidir não usá-los, anulá-los ou interromper o sistema.

✗ A) Incorreta. Assinar sem entender é supervisão formal, não efetiva.
✗ C) Incorreta. A supervisão cabe a quem usa o sistema, não a um controle remoto do fornecedor.
✗ D) Incorreta. Pesquisa de satisfação não permite intervir nas decisões.

Dica de prova: Supervisão humana efetiva: entender, poder intervir e parar.

R4.2. B) Evitar que a IA cause ou agrave danos físicos, mentais ou sociais a pessoas

Por quê: As Orientações Éticas do HLEG (2019) partem de quatro princípios: respeito pela autonomia humana, prevenção de danos, equidade e explicabilidade. A prevenção de danos exige que os sistemas de IA não causem nem agravem danos e protejam a dignidade humana e a integridade física e mental, o que inclui ambientes seguros, robustez técnica e atenção a pessoas vulneráveis e a assimetrias de poder.

✗ A) Incorreta. Contestar decisões e obter reparação é a dimensão processual do princípio da equidade.
✗ C) Incorreta. Entender como o sistema decide é o princípio da explicabilidade.
✗ D) Incorreta. A distribuição justa de benefícios e custos é a dimensão substantiva do princípio da equidade.

Dica de prova: Quatro princípios do HLEG: autonomia humana, prevenção de danos, equidade e explicabilidade.

R4.3. D) Adaptar o grau de explicação ao risco, ao contexto e ao público, com documentação e técnicas pós-hoc

Por quê: Nas Orientações do HLEG, o princípio da explicabilidade pede processos transparentes e decisões explicáveis, na medida do possível, a quem é afetado. Quando o modelo é uma caixa-preta, outras medidas de explicabilidade podem ser exigidas, como rastreabilidade, auditabilidade e comunicação transparente sobre as capacidades do sistema, e o grau de explicação depende do contexto e da gravidade das consequências de um resultado errado.

✗ A) Incorreta. A explicação deve servir às pessoas envolvidas, como usuários, afetados e auditores, e não só à equipe técnica.
✗ B) Incorreta. IA confiável não proíbe modelos complexos; pede explicações e controles adequados ao risco.
✗ C) Incorreta. Métricas de desempenho não explicam decisões nem permitem contestá-las.

Dica de prova: Explicabilidade: explicar para quem, para quê e quanto, conforme o risco.

R4.4. D) Verificação e confirmação separadas da identificação por pelo menos duas pessoas competentes

Por quê: O Art. 14(5) acrescenta, para identificação biométrica remota do Anexo III 1(a), que nenhuma ação ou decisão seja tomada com base na identificação sem verificação e confirmação separadas por pelo menos duas pessoas com competência, formação e autoridade necessárias. A exigência não se aplica a usos de aplicação da lei, migração, controle de fronteiras ou asilo quando o direito da UE ou nacional a considerar desproporcional.

✗ A) Incorreta. O registro do período de cada uso é exigência de logs (Art. 12(3)) e não substitui a verificação por duas pessoas.

✗ B) Incorreta. A autorização prévia judicial ou administrativa é exigida para identificação biométrica remota em tempo real pela polícia (Art. 5), e não para este caso.

✗ C) Incorreta. O Art. 14(5) não condiciona a dupla verificação a um limiar de confiança: ela vale para qualquer identificação usada como base de ação.

> **Dica de prova:** Identificação biométrica remota (Anexo III 1(a)): duas pessoas confirmam antes de agir (Art. 14(5)).

05

CAPÍTULO 5 · 15% DA PROVA

Domínio 5: Lei da IA na prática

Vale 15% (6 questões): 2,5% de setor público (decisões públicas, acusação de crimes, eleições) e 12,5% de setor privado (finanças e seguros, saúde, emprego e educação, condução autônoma, publicidade e turismo). Aqui eu aplico a classificação do Domínio 2 a casos reais: o que está no Anexo III, o que entra pelo Anexo I e o que fica fora. O raciocínio é sempre pela finalidade pretendida, sistema a sistema, nunca pelo setor ou pelo tipo de empresa. Onde mais erro: achar que todo uso em finanças ou saúde é risco elevado, esquecer as exceções expressas (fraude, verificação 1 para 1, logística de campanha, fadiga) e achar que revisão humana ou aviso muda a classificação.

Neste capítulo
17 tópicos-chave · 14 pegadinhas · 7 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Reconhecimento de emoções (Art. 5(1)(f) e Anexo III 1(c))

Proibido no local de trabalho e em instituições de ensino, salvo razões médicas ou de segurança (o considerando 44 cita uso terapêutico). Quando não é proibido, é risco elevado pelo Anexo III 1(c), e quem implanta informa as pessoas expostas (Art. 50(3)). Aviso prévio, consentimento ou ausência de decisão automatizada não afastam a proibição.

Fadiga e dor não são emoções

O Art. 3(39) define reconhecimento de emoções como inferir emoções ou intenções a partir de dados biométricos; o considerando 18 exclui estados físicos como dor ou fadiga e cita detecção de fadiga de motoristas e pilotos. Esse sistema não cai na proibição, mas segue sujeito ao GDPR.

Infraestrutura crítica (Anexo III ponto 2)

Componentes de segurança na gestão e operação de infraestrutura digital crítica, tráfego rodoviário e fornecimento de água, gás, aquecimento ou eletricidade, como controle de semáforos. O risco é à vida e à saúde, mesmo sem dados pessoais. Registro em nível nacional (Art. 49(5)).

Educação (Anexo III ponto 3)

Risco elevado para acesso ou admissão, avaliação de resultados de aprendizagem, definição do nível de educação que a pessoa poderá acessar (3(c)) e monitoramento e detecção de comportamento proibido em provas, como cola (3(d)). A decisão final do professor não muda a classificação; monitorar a prova não é proibido, só o reconhecimento de emoções.

Emprego (Anexo III ponto 4)

4(a): recrutamento e triagem de currículos. 4(b): decisões sobre condições de trabalho, promoção ou cessação, atribuição de tarefas com base em comportamento ou características e monitoramento e avaliação de desempenho. O empregador informa trabalhadores e representantes antes do uso (Art. 26(7)). Uso interno não isenta.

Serviços essenciais (Anexo III ponto 5)

5(a): autoridades avaliando elegibilidade a benefícios e serviços públicos e concedendo, reduzindo, revogando ou recuperando benefícios. 5(b): solvabilidade e pontuação de crédito de pessoas físicas, seja quem for o usuário, exceto detecção de fraude financeira. 5(c): avaliação de risco e precificação de seguros de vida e de saúde de pessoas físicas. 5(d): avaliar e classificar chamadas de emergência, priorizar despacho de polícia, bombeiros e socorro e triagem de pacientes.

Migração, asilo e fronteiras (Anexo III ponto 7)

Inclui polígrafos e ferramentas semelhantes, avaliação de riscos de quem entra no território e, no 7(c), auxílio no exame de pedidos de asilo, visto e residência, inclusive confiabilidade das provas. Não é segurança nacional excluída. Registro em seção não pública da base da UE (Art. 49(4)).

Justiça e processos democráticos (Anexo III ponto 8)

8(a): IA usada por autoridade judiciária, ou em seu nome, para pesquisar e interpretar fatos e o direito e aplicá-lo a casos concretos (por exemplo, recomendar penas). Ferramenta de minutas para advogados não entra. 8(b): sistemas destinados a influenciar o resultado de eleição ou referendo ou o voto; ferramentas administrativas e logísticas de campanha, sem exposição direta dos eleitores, ficam fora.

Dispositivo médico com IA (Anexo I)

Software que é dispositivo médico sujeito a organismo notificado é risco elevado pelo Art. 6(1), não pelo Anexo III. A avaliação é única, no procedimento do regulamento setorial com os requisitos da Lei da IA dentro (Art. 43(3)). Incidentes: pelo Art. 73(10), a Lei da IA só cobre violação de direitos fundamentais; dano à saúde segue a vigilância dos Regulamentos 2017/745 e 2017/746. Aplicativo de bem-estar sem finalidade médica não é dispositivo nem risco elevado.

Veículos e condução automatizada (Anexo I, Seção B)

Pelo Art. 2(2) da versão consolidada, aplicam-se diretamente só o Art. 6(1), o Art. 60a e os Arts. 102 a 112, que levam os requisitos à homologação setorial. O Art. 60a, incluído pelo Omnibus Digital, permite aos Estados-Membros autorizar testes em condições reais fora de sandbox, com quadros de teste nacionais ou conjuntos.

Componente de segurança (Art. 6(1a) e 6(1b))

IA só para assistência ao usuário, otimização, eficiência, automação, conveniência ou controle de qualidade não é componente de segurança, como assistente de voz que escolhe músicas. Se a falha puder pôr em perigo a saúde e a segurança, é componente de segurança.

Setor financeiro na prática (Arts. 17(4) e 74(6))

Para instituições financeiras reguladas, a autoridade de fiscalização do mercado é o supervisor financeiro nacional, quando o sistema está ligado diretamente aos serviços financeiros. O banco fornecedor cumpre o sistema de gestão da qualidade pelas regras de governança financeira, exceto gestão de riscos, pós-comercialização e notificação de incidentes. Recomendação de investimentos não está no ponto 5.

Deepfake (Art. 3(60) e Art. 50(4))

Imagem, áudio ou vídeo gerado ou manipulado por IA que se assemelha a pessoas, objetos, locais, entidades ou eventos existentes e pareceria autêntico. Uma praia real em condições inexistentes é deepfake. Quem divulga informa que é artificial; publicidade não tem exceção, só obras evidentemente artísticas, satíricas ou ficcionais têm divulgação limitada.

Publicidade e precificação

Publicidade lícita personalizada não é, por si, manipulação proibida (considerando 29); segmentação de campanhas e descontos não é risco elevado. Precificação personalizada não está no Anexo III, mas é proibida se explorar vulnerabilidades por idade, deficiência ou situação social ou econômica com dano significativo (Art. 5(1)(b)). Perfilagem segue o GDPR.

DSA e anúncios

Plataformas online, incluindo viagens e hospedagem, não podem mostrar anúncios baseados em perfilagem a menores nem usar dados sensíveis, e devem rotular anúncios informando quem paga e por que o usuário os vê. A Lei da IA não substitui o DSA (Art. 2(5)); aceite dos pais não afasta a proibição.

Identificação biométrica remota em tempo real pela polícia

Proibida em regra em espaços acessíveis ao público. Exceções estritas: busca direcionada de vítimas de sequestro, tráfico ou exploração sexual e de desaparecidos; prevenção de ameaça iminente, como ataque terrorista; localização de suspeitos de crimes graves. Exige autorização prévia de autoridade judicial ou administrativa independente.

Classificação sistema a sistema

Num mesmo grupo empresarial, cada sistema é classificado pela sua finalidade: triagem de currículos é risco elevado, chatbot tem dever de transparência e IA generativa para rascunhos internos não publicados não tem deveres específicos (a marcação das saídas é do fornecedor do gerador).

Macetes para memorizar

💡 Pontos do Anexo III citados na prova

1 Biometria, 2 Infraestrutura, 3 Educação, 4 Emprego, 5 Serviços essenciais, 7 Migração, 8 Justiça e democracia.

💡 Finanças no Anexo III

Crédito e Corpo: crédito de pessoa física e seguros de vida e de saúde. Fraude, investimento e outros seguros ficam fora.

💡 Emoções

Escola e Empresa proíbem; Saúde e Segurança salvam; no resto é risco elevado.

💡 Fadiga

Fadiga e dor são do corpo, não do coração.

💡 Deepfake

POLEE: Pessoas, Objetos, Locais, Entidades, Eventos.

💡 Saúde

Diagnóstico entra pela porta do Anexo I; emergência e benefício, pela porta do Anexo III.

💡 Veículos

Carro: a Lei da IA chega pela homologação, não pela montadora aplicando todo o Capítulo III.

Tabela de memorização: não confunda

Quando é...	...e quando é

Reconhecimento de emoções no trabalho ou no ensino Proibido, salvo razões médicas ou de segurança.	**Reconhecimento de emoções em outros contextos (como estações de metrô)** Risco elevado (Anexo III 1(c)), com informação às pessoas expostas.
Avaliação de crédito de pessoa física (5(b)) Risco elevado, mesmo em varejista que não é banco.	**Detecção de fraude financeira** Exceção expressa do 5(b); continua sujeita às regras gerais da lei e ao GDPR.
Seguros de vida e de saúde Risco elevado (5(c)) e avaliação de impacto sobre os direitos fundamentais.	**Seguros de automóvel, patrimonial e de viagem** Fora do Anexo III.
Diagnóstico por dispositivo médico Entra pelo Anexo I e Art. 6(1), com avaliação no procedimento setorial.	**Saúde no Anexo III** Triagem de emergência e elegibilidade a serviços públicos, incluindo cuidados de saúde.
Influenciar o voto (8(b)) Risco elevado: mensagens dirigidas a eleitores para mudar o voto.	**Organizar a logística da campanha** Fora do risco elevado: ferramentas administrativas sem exposição direta dos eleitores.
Apoio a juízes (8(a)) Risco elevado: autoridade judiciária interpretando e aplicando o direito.	**Minutas de contratos revisadas por advogados** Fora do risco elevado, com transparência e letramento em IA.
Publicidade personalizada lícita Prática comercial legítima, sujeita ao GDPR e às regras de consumo.	**Manipulação ou exploração de vulnerabilidades** Proibida pelo Art. 5(1)(a) ou (b) quando distorce o comportamento e causa dano significativo.

Números que caem

Item	Valor
Peso do domínio	**15% (5.1 setor público: 2,5%; 5.2 setor privado: 12,5%)**
Regulamentos de dispositivos médicos citados no Art. 73(10)	**2017/745 e 2017/746**
Artigos aplicáveis a veículos do Anexo I, Seção B (Art. 2(2))	**Art. 6(1), Art. 60a e Arts. 102 a 112**

Alertas de prova (pegadinhas)

> ⚠ **Alerta de prova:** Com revisão médica ou decisão final humana, o sistema deixa de ser risco elevado.
> **Como não cair:** A classificação segue a finalidade pretendida; revisão humana não a altera.

⚠ **Alerta de prova:** Software de diagnóstico é risco elevado pelo Anexo III por ser de saúde.
Como não cair: Dispositivo médico entra pelo Anexo I (Art. 6(1)); o Anexo III cobre triagem de emergência e elegibilidade.

⚠ **Alerta de prova:** Controle de semáforos é risco mínimo por não tratar dados pessoais, ou fica fora por ser municipal.
Como não cair: É componente de segurança do tráfego rodoviário (Anexo III ponto 2).

⚠ **Alerta de prova:** Classificar consumidores para descontos é risco elevado ou perfilagem proibida.
Como não cair: Marketing não está no ponto 5; a perfilagem segue o GDPR.

⚠ **Alerta de prova:** IA em campanhas eleitorais é proibida, ou é risco mínimo porque o voto é do eleitor.
Como não cair: Influenciar o voto é risco elevado (8(b)); logística de campanha fica fora.

⚠ **Alerta de prova:** Antifraude entra no 5(b) por usar dados financeiros ou sai de toda a Lei da IA.
Como não cair: É exceção expressa do 5(b), mas proibições e letramento em IA continuam valendo.

⚠ **Alerta de prova:** Deepfake só existe com rosto ou voz de pessoa real.
Como não cair: Locais, objetos, entidades e eventos reais também contam (Art. 3(60)).

⚠ **Alerta de prova:** Monitorar desempenho de trabalhadores por câmeras é prática proibida.
Como não cair: É risco elevado (4(b)); a proibição no trabalho é só para reconhecimento de emoções.

⚠ **Alerta de prova:** Reconhecimento de emoções em espaço público é sempre proibido.
Como não cair: A proibição vale no trabalho e no ensino; nos demais contextos é risco elevado.

⚠ **Alerta de prova:** Banco com IA de crédito é fiscalizado pelo Gabinete de IA ou pela autoridade de dados.
Como não cair: O supervisor financeiro nacional é a autoridade de fiscalização do mercado (Art. 74(6)).

⚠ **Alerta de prova:** Teste de veículo em vias públicas está fora da lei por ser atividade de teste, ou depende do Gabinete de IA.
Como não cair: Art. 2(8) não exclui testes reais; o Art. 60a deixa a autorização com os Estados-Membros.

⚠ **Alerta de prova:** Dispositivo médico com IA notifica todo incidente grave pela Lei da IA em 15 dias.
Como não cair: Art. 73(10): pela Lei da IA só violação de direitos fundamentais; dano à saúde vai pelo regime médico.

⚠ **Alerta de prova:** Asilo e fronteiras são segurança nacional e ficam fora da lei.
Como não cair: Migração, asilo e fronteiras são área expressa do Anexo III ponto 7.

⚠ **Alerta de prova:** Todo assistente no painel do carro é componente de segurança.
Como não cair: Conveniência não é componente de segurança; só se a falha puder pôr pessoas em perigo.

Como cai na prova

📝 **Como cai:** Cenário setorial (banco, hospital, escola, prefeitura) e alternativas proibido, risco elevado, limitado ou mínimo.
Como resolver: 1) Esqueça o setor e pegue a finalidade exata. 2) Confira se há exceção expressa (fraude, fadiga, verificação 1 para 1, logística de campanha, razão médica). 3) Ache o ponto do Anexo III ou a via do Anexo I. 4) Descarte alternativas que mudam a classificação por aviso, consentimento ou revisão humana.

📝 **Como cai:** Pergunta 'esse uso está no ponto X do Anexo III?' com alternativas que generalizam.
Como resolver: O Anexo III lista finalidades específicas, não setores inteiros. 'Qualquer sistema usado por instituição financeira' ou 'todo uso corporativo' está errado.

📝 **Como cai:** Cenário com vários sistemas do mesmo grupo e pergunta pelo enquadramento de cada um.
Como resolver: Classifique um por um: Anexo III para o que decide sobre pessoas, Art. 50 para o que conversa ou gera conteúdo publicado, nada específico para uso interno sem publicação.

📝 **Como cai:** Produto regulado (dispositivo médico, veículo) e pergunta sobre avaliação, incidente ou artigos aplicáveis.
Como resolver: Lembre a integração: avaliação única no procedimento setorial (Art. 43(3)); incidente de saúde pelo regime médico (Art. 73(10)); veículos só com Arts. 6(1), 60a e 102 a 112.

📝 **Como cai:** Publicidade, turismo ou preço personalizado e alternativas citando Anexo III, Art. 5 e DSA.
Como resolver: Publicidade não está no Anexo III; verifique se há manipulação ou exploração de vulnerabilidade com dano significativo (Art. 5); deepfake pede divulgação; anúncios a menores vão pelo DSA.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em

reconhecimento de emoções para uso terapêutico de aluno	**não proibido (razão médica); risco elevado (1(c))**
detecta fadiga de motoristas para evitar acidentes	**não é reconhecimento de emoções (considerando 18)**
semáforos, água, gás, eletricidade como componente de segurança	**Anexo III ponto 2, registro nacional**
definir em que nível de curso o aluno poderá se matricular	**Anexo III 3(c)**
monitorar alunos pela câmera em provas online	**Anexo III 3(d)**
câmeras avaliam produtividade individual de trabalhadores	**Anexo III 4(b) e informar trabalhadores (Art. 26(7))**
decidir se o cliente pode pagar em parcelas pela capacidade de pagamento	**crédito de pessoa física, 5(b), mesmo sem ser banco**
priorizar ambulâncias, bombeiros e polícia em chamadas	**Anexo III 5(d)**
propor redução ou revogação de benefícios sociais	**Anexo III 5(a) e avaliação de impacto (Art. 27)**
recomendar penas a juízes	**Anexo III 8(a)**
mensagens personalizadas para mudar o voto de indecisos	**Anexo III 8(b)**
vídeo realista de lugar real em condições inexistentes	**deepfake: divulgar que é artificial**
anúncios personalizados para adolescentes em plataforma de viagens	**DSA proíbe anúncios baseados em perfilagem a menores**
preço personalizado por perfil socioeconômico inferido	**verificar exploração de vulnerabilidades (Art. 5(1)(b))**

🎯 Se você lembrar de só uma coisa deste capítulo...

- Classifica-se pela finalidade pretendida de cada sistema, não pelo setor nem pelo tipo de empresa.
- Exceções expressas: detecção de fraude (5(b)), verificação 1 para 1, logística de campanha (8(b)), fadiga e dor, razão médica ou de segurança nas emoções.
- Finanças no Anexo III: crédito de pessoa física e seguros de vida e de saúde.
- Dispositivo médico e veículos entram pelo Anexo I e se integram à legislação setorial.

Essenciais para a prova (checklist)

- ☐ Sei quando o reconhecimento de emoções é proibido e quando é risco elevado.
- ☐ Sei por que detecção de fadiga não é reconhecimento de emoções.

- ☐ Sei os casos dos pontos 2, 3, 4, 5, 7 e 8 do Anexo III com exemplos.
- ☐ Sei as exceções de fraude financeira e de logística de campanha.
- ☐ Sei como dispositivos médicos e veículos se relacionam com a Lei da IA.
- ☐ Sei quem fiscaliza IA de risco elevado em banco regulado.
- ☐ Sei definir deepfake e o dever de divulgação, inclusive em publicidade.
- ☐ Sei separar publicidade lícita, manipulação proibida e as regras do DSA para menores.
- ☐ Sei as exceções para identificação biométrica remota em tempo real pela polícia.

Questões de revisão do capítulo

R5.1 · Domínio 5: Lei da IA na prática

Uma empresa desenvolve um software de IA que analisa exames de imagem para apoiar diagnósticos. Pelo regulamento de dispositivos médicos, ele é dispositivo médico e precisa de avaliação de conformidade por organismo notificado. Como o AI Act o classifica?

A. Risco limitado, pois o médico revisa o resultado antes de qualquer decisão clínica
B. Fora do AI Act, pois dispositivos médicos são regulados só pela legislação de saúde
C. Risco elevado, pelo Anexo III, por estar ligado a serviços de saúde e de emergência
D. Risco elevado, pelo artigo 6(1), como produto abrangido pela legislação do Anexo I

R5.2 · Domínio 5: Lei da IA na prática

Uma prefeitura implanta um sistema de IA que controla em tempo real os semáforos de cruzamentos movimentados e funciona como componente de segurança da gestão do tráfego. Como o AI Act classifica o sistema?

A. Risco mínimo, por apenas otimizar o fluxo de veículos, sem tratar dados pessoais
B. Prática proibida, por permitir o monitoramento contínuo dos motoristas da cidade
C. Risco elevado, como componente de segurança da gestão do tráfego rodoviário
D. Fora do AI Act, por se tratar de infraestrutura pública operada por um município

R5.3 · Domínio 5: Lei da IA na prática

Uma empresa de marketing digital em Lisboa usa IA para classificar consumidores em valor comercial alto, médio ou baixo e, com isso, definir campanhas e descontos. O uso não envolve crédito, seguros, emprego ou serviços públicos. Como esse sistema tende a ser tratado?

A. Risco elevado, por perfilar consumidores com impacto no acesso a descontos comerciais
B. Fora do risco elevado, mas a perfilagem deve cumprir o GDPR, com base legal e transparência
C. Modelo de IA de finalidade geral, por classificar usuários, sujeito às obrigações de GPAI
D. Prática proibida, pois o AI Act vedaria a perfilagem comportamental para fins comerciais

R5.4 · Domínio 5: Lei da IA na prática

Uma consultoria política oferece a partidos um sistema de IA que gera e direciona mensagens personalizadas a eleitores indecisos para mudar seu voto numa eleição nacional. Como o AI Act classifica esse sistema?

A. Prática proibida, pois o AI Act veda qualquer uso de IA em campanhas eleitorais
B. Risco elevado, por se destinar a influenciar o resultado da eleição ou o voto
C. Risco mínimo, pois a decisão final de votar continua sendo de cada eleitor
D. Risco limitado, bastando rotular as mensagens como geradas por inteligência artificial

Respostas comentadas

R5.1. D) Risco elevado, pelo artigo 6(1), como produto abrangido pela legislação do Anexo I
Por quê: O artigo 6(1) considera de risco elevado o sistema de IA que é ele próprio um produto, ou componente de segurança de um produto, abrangido pela legislação de harmonização do Anexo I, como o regulamento de dispositivos médicos, desde que esse produto deva passar por avaliação de conformidade por terceiros. Nesse caso, os requisitos do AI Act são avaliados dentro do procedimento do regulamento setorial (artigo 43(3)).

✗ A) Incorreta. A revisão médica não muda a classificação definida pelo artigo 6(1).
✗ B) Incorreta. O AI Act se soma à legislação de dispositivos médicos, que está listada no Anexo I.
✗ C) Incorreta. Na saúde, o Anexo III cobre a triagem de emergência e a elegibilidade a serviços públicos; o diagnóstico por dispositivo médico entra pela via do Anexo I.

> **Dica de prova:** Dispositivo médico com organismo notificado: risco elevado pelo artigo 6(1).

R5.2. C) Risco elevado, como componente de segurança da gestão do tráfego rodoviário
Por quê: O Anexo III, ponto 2, considera de risco elevado os sistemas de IA destinados a ser usados como componentes de segurança na gestão e operação de infraestrutura digital crítica, do tráfego rodoviário e do fornecimento de água, gás, aquecimento ou eletricidade, porque falhas podem pôr em risco a vida e a saúde de muitas pessoas. Esses sistemas são registrados em nível nacional, e não na base de dados da UE (artigo 49(5)).

✗ A) Incorreta. O risco aqui é à segurança física das pessoas; a ausência de dados pessoais não afasta o Anexo III.
✗ B) Incorreta. Controlar semáforos não é prática proibida; o caso é de infraestrutura crítica.
✗ D) Incorreta. O AI Act alcança autoridades públicas, e a infraestrutura crítica é área expressa do Anexo III.

> **Dica de prova:** Componente de segurança no tráfego rodoviário: Anexo III, ponto 2.

R5.3. B) Fora do risco elevado, mas a perfilagem deve cumprir o GDPR, com base legal e transparência

Por quê: O Anexo III lista como risco elevado o acesso a serviços essenciais, como avaliação de crédito e precificação de seguros de vida e saúde, e não a segmentação de campanhas e descontos. Assim, o sistema tende a ficar fora do risco elevado. Ainda assim, a perfilagem é tratamento de dados pessoais: exige base legal, transparência, respeito ao direito de oposição ao marketing direto e, quando cabível, DPIA.

✗ A) Incorreta. Descontos de marketing não estão entre os serviços essenciais do Anexo III.

✗ C) Incorreta. GPAI é um modelo de uso amplo, não um sistema de segmentação específico.

✗ D) Incorreta. O AI Act não proíbe a perfilagem comercial em geral.

> **Dica de prova:** Marketing e descontos não são risco elevado; crédito e seguros de vida e saúde são.

R5.4. B) Risco elevado, por se destinar a influenciar o resultado da eleição ou o voto

Por quê: O Anexo III, ponto 8(b), considera de risco elevado os sistemas de IA destinados a influenciar o resultado de uma eleição ou referendo ou o comportamento de voto das pessoas. Ficam de fora as ferramentas a cujos resultados as pessoas não são diretamente expostas, como as usadas para organizar, otimizar ou estruturar campanhas do ponto de vista administrativo ou logístico. O risco aqui é para os processos democráticos.

✗ A) Incorreta. O AI Act não proíbe a IA em campanhas; ferramentas administrativas e logísticas, sem exposição direta dos eleitores, ficam inclusive fora do risco elevado.

✗ C) Incorreta. A classificação depende da finalidade pretendida, que aqui é influenciar o voto, hipótese listada no Anexo III.

✗ D) Incorreta. Rotular conteúdo não basta: o Anexo III, ponto 8(b), torna de risco elevado os sistemas destinados a influenciar eleições.

> **Dica de prova:** Influenciar o voto: Anexo III, ponto 8(b). Logística de campanha: fora.

06

CAPÍTULO 6 · 20% DA PROVA

Domínio 6: Diretrizes para apoiar a conformidade

Vale 20% (8 questões): 5% de normas europeias (CEN/CLC/TR 18115) e 15% de normas internacionais (ISO/IEC 42001, NIST AI RMF, ISO/IEC 23894, ISO/IEC TR 24368). O apêndice da Lei da IA só ajuda nos Arts. 40 e 41; as normas ISO/IEC, CEN/CLC e NIST não estão nele, então preciso decorar estrutura: cláusulas e anexos da 42001, funções e perfis do NIST, processo e anexos da 23894, temas e revisão ética do TR 24368, além de normas harmonizadas e especificações comuns (Arts. 40 e 41). As questões pedem a natureza do documento (requisito, orientação, relatório técnico), onde fica cada conteúdo e se gera presunção de conformidade. Onde mais erro: achar que norma ISO ou relatório técnico dá presunção, trocar anexos de normas diferentes e confundir as funções do NIST AI RMF com as do NIST Cybersecurity Framework.

Neste capítulo

17 tópicos-chave · 14 pegadinhas · 8 macetes · 14 gatilhos · 4 questões comentadas

Tópicos-chave

Normas harmonizadas (Art. 40)

Quem segue normas harmonizadas com referência publicada no Jornal Oficial, nos termos do Regulamento (UE) 1025/2012, presume-se conforme com os requisitos cobertos. A Comissão emite pedidos de normalização e o CEN e o CENELEC elaboram as normas no JTC 21. A aplicação continua voluntária: outro referencial é possível, sem presunção, e a norma não dispensa avaliação de conformidade, registro nem reclassifica o risco.

Especificações comuns (Art. 41)

Se o pedido de normalização não foi aceito, as normas atrasaram, são insuficientes (inclusive quanto a direitos fundamentais) e não há referência publicada nem esperada, a Comissão adota especificações comuns por ato de execução, após consultar o fórum consultivo. Quem as segue tem presunção (41(3)); quem não segue justifica solução técnica de nível ao menos equivalente (41(5)). São revogadas quando a norma harmonizada é publicada.

Pedido de normalização ao CEN e ao CENELEC

Dez áreas-chave para risco elevado: gestão de riscos; governança e qualidade dos conjuntos de dados; manutenção de registros; transparência; supervisão humana; exatidão; robustez; cibersegurança; gestão da qualidade; avaliação da conformidade. Letramento em IA, sandbox, avaliação de impacto, marcação de conteúdo sintético, códigos de conduta, direitos autorais e pontuação social não estão entre elas.

CEN/CLC/TR 18115:2024

Relatório técnico do CEN/CLC/JTC 21 com visão geral de normas de IA focadas em dados e ciclo de vida dos dados. Declara três áreas: governança de dados, qualidade de dados e propriedades de conjuntos que permitam avaliação imparcial e testes. Mapeia ligações entre normas e regulamentos para criar linguagem comum e cultura de qualidade, apoiando o Art. 10; não fixa limiares, não é certificável e não gera presunção.

ISO/IEC 42001 (sistema de gestão de IA)

Especifica requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de IA; por isso é auditável e certificável. Aplica-se a qualquer organização que fornece ou usa produtos ou serviços com IA, de qualquer porte, tipo e natureza, sem exigir certificação prévia em outra norma. Segue a estrutura harmonizada das normas de gestão e o ciclo PDCA; sua única referência normativa é a ISO/IEC 22989.

Cláusulas da ISO/IEC 42001

5 Liderança: 5.1 comprometimento, 5.2 política de IA, 5.3 papéis. 6 Planejamento: 6.1.2 avaliação de riscos, 6.1.3 tratamento, 6.1.4 avaliação de impacto do sistema de IA, 6.3 planejamento de mudanças. 7 Suporte: recursos, competência, conscientização, comunicação, informação documentada (7.5.3). 8 Operação: 8.2 riscos, 8.3 tratamento, 8.4 impacto. 9 Avaliação de desempenho: 9.1 monitoramento, 9.2 auditoria interna, 9.3 análise crítica pela direção. 10 Melhoria: 10.1 melhoria contínua, 10.2 não conformidade e ação corretiva.

Anexos e declaração de aplicabilidade da ISO/IEC 42001

Anexo A (normativo): objetivos de controle e controles de referência. Anexo B (normativo): orientação de implementação dos controles. Anexo C (informativo): potenciais objetivos organizacionais e fontes de risco. Anexo D (informativo): uso do sistema de gestão em domínios ou setores. A declaração de aplicabilidade lista os controles do Anexo A necessários, indica se estão implementados e justifica inclusões e exclusões.

Por que a IA pede gestão própria (introdução da 42001)

Decisões automáticas às vezes não transparentes e não explicáveis, uso de aprendizado de máquina em vez de lógica codificada por humanos e aprendizado contínuo, que muda o comportamento durante o uso. A norma não proíbe aprendizado contínuo nem certifica versões de modelo; pede salvaguardas adequadas. A avaliação de impacto da 42001 tem orientação específica na ISO/IEC 42005.

ISO/IEC 23894 (orientação sobre gestão de riscos de IA)

Documento de orientação (guidance), com recomendações e não requisitos; não é auditável como a 42001 e não gera presunção de conformidade. Ajuda organizações que desenvolvem, produzem, implantam ou usam IA a integrar a gestão de riscos às atividades ligadas à IA, inclusive quem só usa IA de terceiros. É personalizável a qualquer organização e contexto e deve ser usada com a ISO 31000:2018, espelhando sua estrutura.

Estrutura e anexos da ISO/IEC 23894

Cláusula 4 princípios (abordagem integrada, estruturada e abrangente, todos os níveis, sistema inteiro, riscos com consequências positivas ou negativas); 5 estrutura; 6 processo: 6.2 comunicação e consulta, 6.3 escopo, contexto e critérios, 6.4 avaliação de riscos (identificação, análise e avaliação), 6.5 tratamento, 6.6 monitoramento e análise crítica, 6.7 registro e relato. Anexos informativos: A objetivos, B fontes de risco, C exemplo de mapeamento entre processos de risco e ciclo de vida.

NIST AI RMF 1.0

Framework voluntário, que preserva direitos, não setorial e independente do caso de uso, para organizações de todo porte. Pode ser usado ao lado da Lei da IA, mas não é norma harmonizada, não é obrigatório nem para fornecedores do governo dos EUA e não gera presunção. O Apêndice B explica riscos novos ou ampliados da IA frente ao software tradicional: dados defasados ou não representativos, deriva, opacidade, incerteza de modelos pré-treinados, padrões de teste imaturos e manutenção mais frequente.

Funções do Núcleo do NIST AI RMF

GOVERN: transversal, cultiva cultura de riscos, políticas e responsabilidades, permeia as outras três durante todo o ciclo de vida. MAP: estabelece o contexto (finalidades, usuários, leis, impactos) e permite a decisão inicial go/no-go. MEASURE: métricas e ferramentas quantitativas, qualitativas ou mistas, testes antes e durante a operação e TEVV documentado. MANAGE: prioriza riscos, aloca recursos e responde (mitigar, transferir, evitar ou aceitar), com planos de resposta e recuperação.

Perfis, Playbook e NIST AI 600-1

Seção 6: perfis de caso de uso (contexto específico, como contratação), perfis temporais (Perfil Atual x Perfil Alvo, cuja comparação revela lacunas e gera plano priorizado) e perfis intersetoriais. O Playbook traz ações sugeridas e voluntárias por subcategoria; não é checklist nem sequência obrigatória. O NIST AI 600-1 (26/07/2024) é o perfil intersetorial de IA generativa, voluntário.

Características de IA confiável do NIST

Válida e confiável; segura; protegida e resiliente; responsável e transparente; explicável e interpretável; com privacidade reforçada; justa, com viés nocivo gerenciado. Na figura, válida e confiável é a base (condição necessária) e responsável e transparente é uma caixa vertical que se relaciona com todas.

ISO/IEC TR 24368:2022

Relatório técnico com visão geral de alto nível das preocupações éticas e sociais da IA, sem defender nenhum sistema de valores e sem requisitos certificáveis. Destina-se a tecnólogos, reguladores, grupos de interesse e sociedade em geral. Cita fontes de preocupação como coleta não autorizada de dados pessoais, dados de treino enviesados, decisões opacas e falta de rastreabilidade; complementa a ISO/IEC 22989 e a 42001 e mapeia normas sobre o tema.

Conteúdo do TR 24368

Cláusula 4: estruturas éticas como ética das virtudes, utilitarismo e deontologia, sem escolher uma. Cláusula 6: 14 temas-chave, como responsabilização, equidade e não discriminação, transparência e explicabilidade, privacidade, controle humano, sustentabilidade ambiental e práticas trabalhistas. Cláusula 7: alinhar processos a princípios e estrutura de revisão ética em cinco passos: identificar a questão, levantar os fatos, avaliar alternativas, decidir e agir, agir e refletir.

Omnibus Digital e normas

Segundo o FAQ do AI Act Service Desk, o atraso das normas e de outras ferramentas de apoio dificultava a implementação; por isso a aplicação das regras de risco elevado foi vinculada à disponibilidade desse apoio, com período de transição e limite máximo de adiamento. A data não fica a critério de cada Estado-Membro.

Macetes para memorizar

💡 Anexos da 42001

A de Ação (controles), B de Bula (como implementar), C de Causas (objetivos e fontes de risco), D de Domínios (setores).

💡 Anexos da 23894

A Alvos (objetivos), B Bases de risco (fontes), C Ciclo de vida. Todos informativos.

Natureza dos documentos

42001 Exige (requisitos), 23894 Orienta (guidance), TR Informa (relatório técnico), NIST Sugere (voluntário). Só o Jornal Oficial dá presunção.

Funções do NIST AI RMF

GOVERN governa tudo o tempo todo; MAP mapeia o contexto; MEASURE mede; MANAGE maneja e responde.

Respostas em MANAGE

MTEA: Mitigar, Transferir, Evitar, Aceitar.

Revisão ética do TR 24368

Questão, Fatos, Alternativas, Decisão, Reflexão.

TR 18115

Três D: Dados governados, Dados de qualidade, Datasets com propriedades para teste imparcial.

Cláusulas 9 e 10 da 42001

9 Checa (monitoramento, auditoria, análise crítica); 10 Age (melhoria e ação corretiva).

Tabela de memorização: não confunda

Quando é...	...e quando é
ISO/IEC 42001 Requisitos de sistema de gestão de IA, auditáveis e certificáveis.	**ISO/IEC 23894** Orientação (guidance) para integrar a gestão de riscos de IA, usada com a ISO 31000; não se audita conformidade contra ela.
Norma harmonizada (Art. 40) Elaborada por CEN e CENELEC a pedido da Comissão; presunção quando a referência é publicada no Jornal Oficial.	**Especificação comum (Art. 41)** Ato de execução da Comissão quando não há norma harmonizada adequada; também dá presunção e é revogada quando a norma sai.
CEN/CLC/JTC 21 Comitê europeu de IA: TR 18115 e normas harmonizadas da Lei da IA.	**ISO/IEC JTC 1/SC 42** Subcomitê internacional: ISO/IEC 42001 e 23894.
NIST AI RMF (GOVERN, MAP, MEASURE, MANAGE) Funções do Núcleo de gestão de riscos de IA.	**NIST Cybersecurity Framework (identificar, proteger, detectar, responder) e PDCA da ISO** Funções de cibersegurança do NIST; PDCA é o ciclo das normas ISO de sistema de gestão, como a 42001.
MAP Antes da decisão go/no-go: contexto, finalidades, usuários, leis, impactos.	**MEASURE** Testes, métricas de exatidão, viés e robustez, benchmarks e TEVV documentado.
Anexo A da 42001 Normativo: objetivos de controle e controles de referência (base da declaração de aplicabilidade).	**Anexo C da 42001** Informativo: potenciais objetivos organizacionais e fontes de risco.

Perfis temporais Comparar Perfil Atual e Perfil Alvo para achar lacunas.	**Perfis de caso de uso** Aplicar funções e subcategorias a um contexto específico, como contratação.

Números que caem

Item	Valor
Regulamento de normalização europeia	**Regulamento (UE) 1025/2012**
Áreas do pedido de normalização ao CEN e ao CENELEC	**10**
CEN/CLC/TR 18115	**publicado em 2024; JTC 21 criado em 2021**
ISO 31000 usada com a 23894	**ISO 31000:2018**
NIST AI 600-1 (perfil de IA generativa)	**26 de julho de 2024**
Funções do Núcleo do NIST AI RMF	**4**
Temas-chave da cláusula 6 do TR 24368	**14**
Passos da revisão ética do TR 24368	**5**
Peso do domínio	**20% (6.1: 5%; 6.2: 15%)**

Alertas de prova (pegadinhas)

⚠ **Alerta de prova:** A ISO/IEC 23894 garante presunção de conformidade com o Art. 9 por ser norma ISO/IEC publicada.
Como não cair: Presunção só vem de norma harmonizada com referência no Jornal Oficial ou de especificação comum.

⚠ **Alerta de prova:** O TR 18115 é norma harmonizada, especificação comum ou norma certificável de gestão de dados.
Como não cair: É relatório técnico informativo do CEN e do CENELEC; não gera presunção nem fixa limiares.

⚠ **Alerta de prova:** O auditor pode auditar a conformidade com a 23894 como faz com a 42001.
Como não cair: A 23894 é orientação, sem requisitos auditáveis; só a 42001 especifica requisitos.

⚠ **Alerta de prova:** A 23894 dispensa ou substitui a ISO 31000 ou a converte em requisitos certificáveis.
Como não cair: É usada em conjunto com a ISO 31000:2018, espelhando sua estrutura e somando orientação de IA.

⚠ **Alerta de prova:** A 42001 só vale para quem desenvolve modelos próprios, para risco elevado da Lei da IA ou para quem já tem 27001.
Como não cair: Vale para qualquer organização que fornece ou usa IA, sem certificação prévia.

⚠ **Alerta de prova:** A política de IA fica no Planejamento (6) ou no Suporte (7).
Como não cair: Política de IA é 5.2, na cláusula de Liderança.

⚠ **Alerta de prova:** Auditoria interna está na cláusula 8 ou 7, e ação corretiva na 9.
Como não cair: Auditoria interna é 9.2 (Avaliação de desempenho); ação corretiva é 10.2 (Melhoria).

⚠ **Alerta de prova:** Fontes de risco da 42001 estão no Anexo A ou no Anexo D; o Anexo A da 23894 é normativo.
Como não cair: 42001: fontes de risco no Anexo C, setores no D. 23894: todos os anexos são informativos (A objetivos, B fontes, C ciclo de vida).

⚠ **Alerta de prova:** A referência normativa da 42001 é a ISO 31000.
Como não cair: A única referência normativa da 42001 é a ISO/IEC 22989; a ISO 31000 é ligada à 23894.

⚠ **Alerta de prova:** GOVERN é executada uma vez no início ou por último, depois de MANAGE.
Como não cair: GOVERN é transversal e contínua, permeando as outras três.

⚠ **Alerta de prova:** As opções de resposta ao risco ficam em MEASURE ou são identificar, proteger, detectar e responder.
Como não cair: Em MANAGE: mitigar, transferir, evitar ou aceitar.

⚠ **Alerta de prova:** O Playbook é checklist obrigatório ou versão certificável do AI RMF.
Como não cair: São ações sugeridas e voluntárias; adota-se o que se aplica.

⚠ **Alerta de prova:** O TR 24368 adota o utilitarismo ou define código de ética único.
Como não cair: Apresenta várias estruturas éticas sem defender um sistema de valores.

⚠ **Alerta de prova:** Sem norma harmonizada, a Comissão torna a ISO/IEC 42001 obrigatória por ato delegado ou o Comité IA dá presunção a normas nacionais.
Como não cair: A alternativa são especificações comuns por ato de execução (Art. 41).

Como cai na prova

📝 **Como cai:** Empresa quer usar uma norma como prova de conformidade com a Lei da IA.
Como resolver: Pergunte: é norma harmonizada com referência no Jornal Oficial ou especificação comum? Se não (ISO/IEC, TR, NIST, HLEG), apoia mas não gera presunção. Mesmo com presunção, avaliação de conformidade e registro continuam.

📝 **Como cai:** Pergunta 'em qual cláusula ou anexo está X' na 42001 ou na 23894.
Como resolver: Lembre as âncoras: 42001 política 5.2, riscos 6.1.2, impacto 6.1.4 e 8.4, auditoria 9.2, ação corretiva 10.2; anexos A controles, B implementação, C fontes, D setores. 23894: princípios 4, estrutura 5, processo 6 (6.4 avaliação), anexos A, B, C informativos.

📝 **Como cai:** Cenário de atividade de gestão de riscos e pergunta qual função do NIST AI RMF.
Como resolver: Contexto e go/no-go = MAP; testes e métricas = MEASURE; priorizar e responder = MANAGE; políticas, papéis e cultura contínuos = GOVERN. Descarte funções do CSF e PDCA.

📝 **Como cai:** Pergunta sobre a natureza ou o público de um documento (TR 24368, TR 18115, Playbook, ALTAI).
Como resolver: Relatório técnico e Playbook não têm requisitos nem certificação; TR 24368 não defende sistema de valores e serve a público amplo; TR 18115 conecta normas de dados.

📝 **Como cai:** Pergunta sobre quem elabora normas ou qual regulamento rege a publicação.
Como resolver: Regulamento (UE) 1025/2012, CEN e CENELEC (JTC 21), referência no Jornal Oficial. Gabinete de IA, Comité IA, ENISA e autoridades de dados não elaboram normas harmonizadas.

Gatilhos do enunciado

Se o enunciado trouxer...	Pense em
governança de dados alinhada ao Art. 10, documento europeu de 2024	**CEN/CLC/TR 18115**
sem norma harmonizada publicada nem esperada	**especificações comuns por ato de execução (Art. 41)**
fornecedor não segue a especificação comum e usa solução própria	**justificar solução de nível ao menos equivalente (Art. 41(5))**
integrar a 42001 com 27001 e 9001 sem estrutura paralela	**estrutura harmonizada das normas de gestão**
documento que justifica inclusão e exclusão de controles	**declaração de aplicabilidade (Anexo A da 42001)**
como o sistema de IA pode afetar pessoas, grupos e sociedade, na 42001	**avaliação de impacto do sistema de IA (6.1.4 e 8.4)**
ciclo de melhoria contínua de norma ISO de gestão	**PDCA**

decisão go/no-go antes de desenvolver	**MAP**
métricas de exatidão, viés e robustez e resultados de TEVV	**MEASURE**
Perfil Atual comparado ao Perfil Alvo	**perfis temporais (seção 6 do AI RMF)**
documento do NIST para riscos de IA generativa	**NIST AI 600-1**
característica do NIST que é a base de todas	**válida e confiável**
identificação, análise e avaliação de riscos na 23894	**6.4 avaliação de riscos**
revisão ética em etapas, logo após identificar a questão	**levantar os fatos (TR 24368, 7.2)**

🎯 **Se você lembrar de só uma coisa deste capítulo...**

- Presunção de conformidade só com norma harmonizada referenciada no Jornal Oficial ou especificação comum; ISO/IEC, TR, NIST e HLEG apoiam, mas não presumem.
- 42001 = requisitos auditáveis (anexos A e B normativos); 23894 = orientação com a ISO 31000 (anexos informativos).
- NIST AI RMF: GOVERN transversal, MAP contexto, MEASURE testes, MANAGE resposta; voluntário e não setorial.
- TR 18115 é de dados (Art. 10); TR 24368 é de ética e não defende sistema de valores.

Essenciais para a prova (checklist)

- ☐ Sei explicar o efeito das normas harmonizadas (Art. 40) e quando entram especificações comuns (Art. 41).
- ☐ Sei as dez áreas do pedido de normalização.
- ☐ Sei as três áreas e a natureza do CEN/CLC/TR 18115.
- ☐ Sei localizar política, riscos, impacto, auditoria e ação corretiva nas cláusulas da 42001.
- ☐ Sei o conteúdo e a natureza dos anexos A a D da 42001 e a declaração de aplicabilidade.
- ☐ Sei a relação da 23894 com a ISO 31000 e as etapas 6.2 a 6.7.
- ☐ Sei as quatro funções do NIST AI RMF e as opções de resposta de MANAGE.
- ☐ Sei o que são perfis temporais, Playbook e NIST AI 600-1.
- ☐ Sei as características de IA confiável do NIST e qual é a base.
- ☐ Sei o escopo, o público, os temas e a revisão ética do TR 24368.

Questões de revisão do capítulo

R6.1 · Domínio 6: Diretrizes para apoiar a conformidade

Durante a auditoria interna do sistema de gestão de IA de uma seguradora, constata-se que um novo sistema entrou em produção sem a avaliação de impacto prevista. A organização registra a constatação e decide a ação corretiva. Em quais cláusulas da ISO/IEC 42001 estão essas duas etapas?

A. Auditoria interna na cláusula 6 (Planejamento); não conformidade e ação corretiva na cláusula 8 (Operação)
B. Auditoria interna na cláusula 8 (Operação); não conformidade e ação corretiva na cláusula 9 (Avaliação de desempenho)
C. Auditoria interna na cláusula 7 (Suporte); não conformidade e ação corretiva na cláusula 10 (Melhoria)
D. Auditoria interna na cláusula 9 (Avaliação de desempenho); não conformidade e ação corretiva na 10 (Melhoria)

R6.2 · Domínio 6: Diretrizes para apoiar a conformidade

Uma cooperativa de crédito baixa o Playbook do NIST AI RMF, e o auditor interno propõe exigir que cada ação sugerida seja cumprida, uma a uma, como lista de verificação de conformidade. O que o NIST afirma sobre o Playbook?

A. É a versão certificável do AI RMF, usada por auditores para emitir parecer de conformidade
B. Substitui as quatro funções do Núcleo por um roteiro único e ordenado de implementação
C. É a lista oficial de controles obrigatórios, que deve ser cumprida por inteiro para aplicar o AI RMF
D. Traz ações sugeridas e voluntárias por subcategoria, sem ser checklist nem sequência de passos

R6.3 · Domínio 6: Diretrizes para apoiar a conformidade

Suponha que nenhuma organização europeia de normalização aceite o pedido da Comissão para certo requisito de sistemas de IA de risco elevado e que não haja referência de norma harmonizada publicada nem esperada no Jornal Oficial em prazo razoável. Que instrumento a Lei da IA prevê para essa situação?

A. Código de práticas voluntário elaborado pelo Gabinete de IA com os fornecedores do setor
B. Ato de execução da Comissão com especificações comuns, após consulta ao fórum consultivo
C. Diretriz do Comité IA que concede presunção de conformidade a normas nacionais escolhidas
D. Ato delegado que torna obrigatória a ISO/IEC 42001 para os fornecedores de risco elevado

R6.4 · Domínio 6: Diretrizes para apoiar a conformidade

A ISO/IEC 42001 adota a estrutura comum das normas de sistemas de gestão ISO. Qual ciclo de melhoria contínua orienta esse sistema de gestão de IA?

A. Coletar, Treinar, Validar e Implantar
B. Definir, Medir, Analisar, Melhorar e Controlar
C. Planejar, Fazer, Checar e Agir (PDCA)
D. Identificar, Proteger, Detectar e Responder

Respostas comentadas

R6.1. D) Auditoria interna na cláusula 9 (Avaliação de desempenho); não conformidade e ação corretiva na 10 (Melhoria)

Por quê: Pelo sumário da ISO/IEC 42001, a cláusula 9 (Avaliação de desempenho) reúne 9.1 Monitoramento, medição, análise e avaliação, 9.2 Auditoria interna e 9.3 Análise crítica pela direção. A cláusula 10 (Melhoria) reúne 10.1 Melhoria contínua e 10.2 Não conformidade e ação corretiva.

✗ A) Incorreta. A cláusula 6 trata de planejamento, e a ação corretiva não fica na cláusula 8.
✗ B) Incorreta. A cláusula 8 trata da operação (planejamento e controle, riscos e impacto), e a ação corretiva não fica na cláusula 9.
✗ C) Incorreta. A cláusula 7 trata de recursos, competência, conscientização, comunicação e informação documentada, não de auditoria.

> **Dica de prova:** Checar = cláusula 9 (auditoria, análise crítica). Agir = cláusula 10 (ação corretiva).

R6.2. D) Traz ações sugeridas e voluntárias por subcategoria, sem ser checklist nem sequência de passos

Por quê: O NIST AI RMF Playbook é um recurso complementar que traz ações sugeridas, alinhadas a cada subcategoria das quatro funções do Núcleo, para alcançar os resultados do AI RMF. O NIST afirma que ele não é uma lista de verificação nem um conjunto de passos a seguir por inteiro: as sugestões são voluntárias, e a organização adota quantas se aplicarem ao seu setor, caso de uso ou interesse.

✗ A) Incorreta. O AI RMF e o Playbook são voluntários e não são esquemas de certificação.
✗ B) Incorreta. O Playbook se alinha às subcategorias das quatro funções do Núcleo; ele não as substitui por um roteiro ordenado.
✗ C) Incorreta. O NIST diz que o Playbook não é checklist nem conjunto de passos a seguir por inteiro; a organização usa as sugestões que se aplicam ao seu caso.

> **Dica de prova:** Playbook do NIST: sugestões voluntárias, não checklist.

R6.3. B) Ato de execução da Comissão com especificações comuns, após consulta ao fórum consultivo

Por quê: Pelo Art. 41(1), a Comissão pode adotar, por atos de execução (procedimento de exame do Art. 98(2)), especificações comuns para os requisitos do Capítulo III, Seção 2, quando o pedido de normalização não foi aceito, as normas não foram entregues no prazo, tratam de forma insuficiente os direitos fundamentais ou não cumprem o pedido, e não há referência publicada nem esperada. Ao redigi-las, consulta o fórum consultivo do Art. 67. Quando a norma harmonizada for publicada, o ato é revogado (Art. 41(4)).

✗ A) Incorreta. Códigos de práticas são instrumentos dos modelos de IA de finalidade geral (Art. 56), e não o substituto de normas harmonizadas para risco elevado.

✗ C) Incorreta. O Comité IA não concede presunção de conformidade; a presunção vem de normas harmonizadas publicadas ou de especificações comuns.

✗ D) Incorreta. A Lei da IA não torna obrigatória uma norma ISO/IEC por ato delegado; a alternativa prevista são especificações comuns por ato de execução.

> **Dica de prova:** Sem norma harmonizada: especificações comuns por ato de execução (Art. 41).

R6.4. C) Planejar, Fazer, Checar e Agir (PDCA)

Por quê: Como as demais normas de sistemas de gestão ISO, a ISO/IEC 42001 segue o ciclo PDCA: planejar (contexto, riscos e objetivos), fazer (operação e controles), checar (monitoramento, auditoria interna e análise crítica) e agir (correções e melhoria contínua). DMAIC vem do Seis Sigma, e Identificar, Proteger, Detectar e Responder vem do NIST Cybersecurity Framework.

✗ A) Incorreta. Essas são etapas técnicas do ciclo de vida de modelos.

✗ B) Incorreta. DMAIC é a metodologia do Seis Sigma.

✗ D) Incorreta. Essas são funções do NIST Cybersecurity Framework.

> **Dica de prova:** Norma de sistema de gestão ISO: pense em PDCA.

DIA DA PROVA

Estratégia de prova

São 40 questões de múltipla escolha em 90 minutos, com aprovação em 26 acertos (65%), e o texto da Lei da IA vem como apêndice no exame digital; não há anotações nem equipamentos eletrônicos. O nível é Bloom 2 a 4, então quase tudo vem em cenário curto (uma empresa, um país, um sistema) pedindo a classificação, o papel, a obrigação ou a consequência exata de um artigo. As alternativas erradas são plausíveis: trazem o artigo vizinho, o prazo ou o teto de outro regime (72 horas e 20 milhões ou 4% do GDPR), o órgão errado (Gabinete de IA no lugar da autoridade nacional ou da EDPS) ou os papéis invertidos. Normas e frameworks (ISO/IEC, NIST, HLEG, GDPR) caem com a mesma precisão, mas não estão no apêndice. A prova usa os termos da Lei da IA (AI Act), mesmo quando o PL 2338/2023 brasileiro tem nomes parecidos.

Como responder

✓ Distribua o tempo: 90 minutos para 40 questões dá pouco mais de 2 minutos cada; marque e pule as de cálculo de multa ou de artigo que exigem consulta e volte no fim.

✓ Use o apêndice da Lei da IA para conferir, não para estudar na hora: saiba de cor onde estão o Art. 5 (proibições), Art. 6 e Anexos I e III (classificação), Art. 26 (responsável pela implantação), Art. 27 (avaliação de impacto), Art. 50 (transparência), Art. 73 (incidentes) e Arts. 99 a 101 (multas).

✓ Priorize o Domínio 2 (15 questões por prova) e o Domínio 6 (8 questões): juntos são mais da metade da nota, e no 6 as normas ISO/IEC, CEN/CLC e NIST não estão no apêndice (só os Arts. 40 e 41 da Lei da IA estão).

✓ Em todo cenário, identifique primeiro o papel (fornecedor, responsável pela implantação, importador, distribuidor, autoridade) e só depois a obrigação.

✓ Para classificar, siga sempre a mesma ordem: Art. 5, Anexo I, Anexo III com a derrogação do Art. 6(3), Art. 50 e, por fim, risco mínimo.

✓ Desconfie de alternativas absolutas ('todo', 'qualquer', 'sempre', 'dispensa', 'isenta') e das que resolvem uma proibição com aviso, consentimento ou revisão humana.

✓ Quando a alternativa traz um número, pergunte de qual regime ele é: 72 horas e 20 milhões ou 4% são GDPR; 15, 10 e 2 dias e 35, 15 e 7,5 milhões são Lei da IA.

✓ Os termos podem aparecer como 'propósito geral' ou 'finalidade geral' para GPAI, e 'Gabinete de IA' para AI Office: trate como sinônimos.

Erros que derrubam candidatos

✗ Aplicar prazos e tetos do GDPR a incidentes e multas da Lei da IA.

✗ Esquecer que PME e startups pagam o menor entre valor fixo e percentual, e grandes empresas o maior.

✗ Classificar pelo setor ou pelo tipo de empresa em vez da finalidade pretendida de cada sistema.

✗ Dar ao responsável pela implantação obrigações do fornecedor (documentação técnica, avaliação de conformidade, marcação CE) ou o contrário.

✗ Achar que ISO/IEC 42001, ISO/IEC 23894, TR 18115, NIST AI RMF ou Orientações do HLEG geram presunção de conformidade.

✗ Trocar órgãos: Gabinete de IA, Comité IA, fórum consultivo, painel científico, EDPS e autoridades nacionais têm papéis distintos.

✗ Confundir DPIA do GDPR com avaliação de impacto sobre os direitos fundamentais do Art. 27, achando que uma substitui a outra.

Na semana da prova

- ☐ Faça simulados cronometrando 90 minutos e revise cada erro localizando o artigo da Lei da IA ou a cláusula da norma correspondente.
- ☐ Monte uma folha mental de números: multas (35/7, 15/3, 7,5/1, EDPS e Comissão), prazos (15/10/2 dias, 2 semanas, 6 meses, 10 anos, 72 horas) e o limiar de 10^25 FLOPs.
- ☐ Repasse o índice da Lei da IA até localizar em segundos os artigos-chave e os pontos do Anexo III.
- ☐ Revise o Domínio 6 por estrutura: cláusulas e anexos da 42001, processo e anexos da 23894, funções e perfis do NIST, temas e passos do TR 24368.
- ☐ Na véspera, revise só as seções 'lembrar' e 'pegadinhas' de cada capítulo e descanse.

REVISÃO FINAL

Folha de cola

Leia na véspera e na manhã da prova: os gatilhos e as pegadinhas mais importantes de cada domínio.

1. Domínio 1: Contexto da Lei da IA (AI Act)

‣ empresa sediada fora da UE oferece o sistema online a clientes em Estados-Membros → **Lei da IA se aplica (Art. 2(1)); se for risco elevado, representante autorizado na UE (Art. 22)**

‣ destinado exclusivamente às forças armadas, à defesa ou à segurança nacional → **fora do âmbito (Art. 2(3))**

‣ apenas para o projeto de pesquisa científica, sem oferecer no mercado → **fora do âmbito (Art. 2(6))**

‣ teste em condições reais, em vias públicas ou com pessoas reais → **dentro da lei: Art. 2(8) não exclui testes em condições reais**

‣ pessoa usa em casa, sem fins profissionais → **sem obrigações de responsável pela implantação (Art. 2(10)); fornecedor mantém as suas**

⚠ É regulamento: aplica-se diretamente. Transposição é coisa de diretiva.

⚠ Tem força obrigatória, com multas, e alcança fornecedores e responsáveis pela implantação privados e públicos.

⚠ Não há corte por número de empregados; PME têm apoio e proporcionalidade, não exclusão.

2. Domínio 2: Lei da IA detalhada

‣ coleta não direcionada de imagens faciais da internet ou de câmeras → **prática proibida (Art. 5)**

‣ prever crimes só com perfil ou traços de personalidade → **proibido; se apoiar avaliação humana baseada em fatos objetivos, é risco elevado**

‣ compara rostos gravados, dias depois, com uma lista, uso privado → **identificação biométrica remota a posteriori: risco elevado (Anexo III 1(a))**

‣ modelo treinado com dados de um país será usado em outros → **Art. 10(4): contexto geográfico, comportamental e funcional**

‣ registros adulterados inseridos no conjunto de treino → **envenenamento de dados, Art. 15(5)**

⚠ É permitido, com obrigações adicionais do Art. 55; não está no Art. 5.

⚠ Informar integradores (Art. 53) não substitui os deveres próprios do Art. 55.

⚠ A marcação CE é afixada pelo fornecedor e vale na União; o ponto é adequar os dados ao novo contexto (Art. 10(4)).

3. Domínio 3: IA confiável

‣ guardar dados por prazo longo para treinar modelo futuro → **limitação da conservação**

‣ dado sobre a pessoa está errado ou foi declarado indevido → **exatidão: retificar ou apagar sem demora**

‣ escolha de atributos do modelo, incluindo dado que não serve à finalidade → **minimização**

‣ servidor sem controle de acesso ou sem cópia de segurança → **integridade e confidencialidade (Art. 32)**

‣ dados coletados há anos, agora usados para treinar IA → **limitação da finalidade, revisão da base legal, informar titulares e DPIA**

⚠ Cifragem é segurança; o prazo continua limitado pela finalidade (limitação da conservação).

⚠ Exatidão exige retificar ou apagar sem demora; prazo de guarda e consentimento não corrigem dado errado.

⚠ Pseudonimizado continua pessoal; a minimização corta o atributo desnecessário, como a origem racial.

4. Domínio 4: IA ética

‣ profissionais aceitam quase sempre a sugestão da IA sem examinar → **viés de automação, Art. 14(4)(b)**

‣ identificação biométrica remota aponta uma correspondência antes de barrar alguém → **verificação separada por pelo menos duas pessoas (Art. 14(5))**

‣ fornecedor embute tela de confiança e recomenda dupla revisão ao cliente → **Art. 14(3)(a) e 14(3)(b)**

‣ analistas não aprovam cada alerta, mas monitoram e ajustam limiares → **human-on-the-loop**

‣ IA define cada movimento do operador, sem margem de escolha → **respeito pela autonomia humana**

⚠ O risco é o viés de automação (Art. 14(4)(b)); o botão de parada serve para interromper com segurança.

⚠ A dupla verificação é só para identificação biométrica remota do Anexo III 1(a) e vale para qualquer correspondência usada como base de ação.

⚠ Infraestrutura crítica (ponto 2 do Anexo III) fica fora do Art. 27.

5. Domínio 5: Lei da IA na prática

‣ reconhecimento de emoções para uso terapêutico de aluno → **não proibido (razão médica); risco elevado (1(c))**

‣ detecta fadiga de motoristas para evitar acidentes → **não é reconhecimento de emoções (considerando 18)**

‣ semáforos, água, gás, eletricidade como componente de segurança → **Anexo III ponto 2, registro nacional**

‣ definir em que nível de curso o aluno poderá se matricular → **Anexo III 3(c)**

‣ monitorar alunos pela câmera em provas online → **Anexo III 3(d)**

⚠ A classificação segue a finalidade pretendida; revisão humana não a altera.

⚠ Dispositivo médico entra pelo Anexo I (Art. 6(1)); o Anexo III cobre triagem de emergência e elegibilidade.

⚠ É componente de segurança do tráfego rodoviário (Anexo III ponto 2).

6. Domínio 6: Diretrizes para apoiar a conformidade

‣ governança de dados alinhada ao Art. 10, documento europeu de 2024 → **CEN/CLC/TR 18115**

‣ sem norma harmonizada publicada nem esperada → **especificações comuns por ato de execução (Art. 41)**

‣ fornecedor não segue a especificação comum e usa solução própria → **justificar solução de nível ao menos equivalente (Art. 41(5))**

‣ integrar a 42001 com 27001 e 9001 sem estrutura paralela → **estrutura harmonizada das normas de gestão**

‣ documento que justifica inclusão e exclusão de controles → **declaração de aplicabilidade (Anexo A da 42001)**

⚠ Presunção só vem de norma harmonizada com referência no Jornal Oficial ou de especificação comum.

⚠ É relatório técnico informativo do CEN e do CENELEC; não gera presunção nem fixa limiares.

⚠ A 23894 é orientação, sem requisitos auditáveis; só a 42001 especifica requisitos.

GABARITO

Respostas do diagnóstico

D1. D) Avaliação de conformidade, documentação, marcação CE e representante → revise o capítulo 1

Por quê: Pelo artigo 23, antes de colocar no mercado um sistema de risco elevado, o importador deve verificar que o fornecedor realizou a avaliação de conformidade, elaborou a documentação técnica, aplicou a marcação CE, acompanhou o sistema da declaração UE de conformidade e das instruções de uso e nomeou um representante autorizado. Se suspeitar de não conformidade, não deve colocar o sistema no mercado.

✗ A) Incorreta. A lei não exige dados de treino coletados na UE.

✗ B) Incorreta. Filial na UE não é exigida; basta o representante autorizado.

✗ C) Incorreta. Não há exigência de auditoria acadêmica do código.

> **Dica de prova:** Importador: confira avaliação, documentação, CE e representante antes de vender.

D2. C) A portuguesa é importadora e a espanhola é distribuidora → revise o capítulo 1

Por quê: O artigo 3(6) define importador como a pessoa estabelecida na UE que coloca no mercado um sistema de IA com nome ou marca de pessoa estabelecida num país terceiro. O artigo 3(7) define distribuidor como a pessoa da cadeia de abastecimento, que não seja o fornecedor nem o importador, que disponibiliza o sistema no mercado da União. Todos são operadores (artigo 3(8)), cada um com obrigações próprias (artigos 23 e 24).

✗ A) Incorreta. Só quem coloca o sistema pela primeira vez no mercado da UE é importador; a revenda posterior é distribuição.

✗ B) Incorreta. Os papéis estão invertidos: a primeira colocação no mercado da UE de sistema com marca estrangeira é feita pelo importador.

✗ D) Incorreta. Fornecedor é quem desenvolve ou manda desenvolver e coloca no mercado com seu próprio nome ou marca, como o fabricante coreano.

> **Dica de prova:** Importador: primeira entrada na UE com marca estrangeira. Distribuidor: revende.

D3. D) Não se aplica, pois sistemas de uso exclusivamente militar estão fora do âmbito → revise o capítulo 1

Por quê: O artigo 2(3) exclui do AI Act os sistemas de IA colocados no mercado, colocados em serviço ou usados, com ou sem modificação, exclusivamente para fins militares, de defesa ou de segurança nacional, seja qual for o tipo de entidade que realiza essas atividades, pública ou privada (considerando 24). O uso de IA militar, inclusive de força letal, fica regido pelo direito internacional público.

✗ A) Incorreta. A exportação não muda a exclusão; o que importa é a finalidade exclusivamente militar.

✗ B) Incorreta. O artigo 5 não trata de usos militares, que estão fora do âmbito do regulamento.

✗ C) Incorreta. Sistemas usados exclusivamente para fins militares, de defesa ou de segurança nacional ficam fora do AI Act, seja qual for a técnica.

> **Dica de prova:** Uso exclusivamente militar, de defesa ou de segurança nacional: fora do AI Act.

D4. C) A Diretiva (UE) 2019/1937, sobre denunciantes → revise o capítulo 2

Por quê: O Art. 87 estabelece que a Diretiva (UE) 2019/1937 se aplica à denúncia de infrações à Lei da IA e à proteção das pessoas que as denunciam. O Considerando 172 explica que quem atua como denunciante de infrações à Lei da IA deve ser protegido pelo direito da União.

✗ A) Incorreta. O Regulamento 2019/1020 trata da fiscalização do mercado de produtos, e não da proteção de denunciantes.
✗ B) Incorreta. A Diretiva 2019/790 trata de direitos autorais no mercado único digital (citada no Art. 53(1)(c)), e não de denunciantes.
✗ D) Incorreta. O GDPR protege dados pessoais; a denúncia de violações da Lei da IA segue a Diretiva (UE) 2019/1937.

> **Dica de prova:** Denunciantes na Lei da IA = Art. 87 + Diretiva (UE) 2019/1937.

D5. C) Declaração UE de conformidade e marcação CE → revise o capítulo 2

Por quê: Pelos artigos 47 e 48 do AI Act, o fornecedor de sistema de risco elevado redige a declaração UE de conformidade, assumindo a responsabilidade pelo cumprimento dos requisitos, e aplica a marcação CE de forma visível, legível e indelével, ou em formato digital quando o sistema for digital. Depois, registra o sistema na base de dados da UE.

✗ A) Incorreta. Auditoria financeira não integra a conformidade do AI Act.
✗ B) Incorreta. O Gabinete de IA não emite licenças de operação para sistemas.
✗ D) Incorreta. Não existe selo voluntário que substitua a marcação CE.

> **Dica de prova:** Conformidade concluída: declaração UE, marcação CE e registro.

D6. D) Investigar as causas e informar as autoridades de fiscalização do mercado competentes → revise o capítulo 2

Por quê: Quando um sistema de risco elevado apresenta risco na acepção do artigo 79(1) e o fornecedor toma conhecimento, o artigo 20(2) exige que ele investigue imediatamente as causas, em colaboração com o responsável pela implantação que relatou o problema, e informe as autoridades de fiscalização do mercado competentes e, se for o caso, o organismo notificado, indicando a natureza do problema e as ações corretivas adotadas.

✗ A) Incorreta. A obrigação de informar a autoridade é do fornecedor; o distribuidor tem deveres próprios, mas não assume esse.
✗ B) Incorreta. Registrar internamente sem comunicar as autoridades descumpre o dever de informação do artigo 20(2).
✗ C) Incorreta. A lei não condiciona a ação do fornecedor a instruções da Comissão; ele deve investigar e informar as autoridades nacionais competentes.

> **Dica de prova:** Fornecedor que descobre risco: investiga e informa a autoridade de fiscalização do mercado.

D7. A) Não, porque o texto passou por revisão humana e há responsabilidade editorial pela publicação → revise o capítulo 3

Por quê: O Art. 50(4) tem duas regras para o responsável pela implantação: deepfakes de imagem, áudio ou vídeo devem ser divulgados (com divulgação limitada em obras artísticas, satíricas ou ficcionais); e textos gerados por IA publicados para informar o público sobre assuntos de interesse público também, exceto quando houver revisão humana ou controle editorial com responsabilidade editorial, ou uso autorizado por lei para fins penais.

✗ B) Incorreta. O segundo parágrafo do Art. 50(4) trata justamente de texto gerado ou manipulado por IA publicado para informar o público.

✗ C) Incorreta. A divulgação limitada, que não prejudica a fruição, vale para deepfakes em obras evidentemente artísticas, criativas, satíricas ou ficcionais, e não para notícias.

✗ D) Incorreta. Além da exceção penal, o Art. 50(4) dispensa a divulgação quando o texto passou por revisão humana ou controle editorial e alguém detém a responsabilidade editorial.

> **Dica de prova:** Texto de interesse público gerado por IA: divulgar, salvo revisão humana com responsabilidade editorial.

D8. D) Demonstrar que a detecção não pode ser feita com outros dados, como dados sintéticos ou anonimizados → revise o capítulo 3

Por quê: O Art. 4a da Lei da IA, incluído pelo Omnibus Digital (antes Art. 10(5)), permite tratar excepcionalmente categorias especiais de dados na medida estritamente necessária para detectar e corrigir vieses, com salvaguardas cumulativas: impossibilidade de usar outros dados (sintéticos ou anonimizados), limites técnicos à reutilização e pseudonimização, controle e documentação de acesso, proibição de transmissão a terceiros, eliminação após a correção e justificativa no registro das atividades de tratamento.

✗ A) Incorreta. O Art. 4a não prevê autorização do Gabinete de IA; o fornecedor documenta, no registro das atividades de tratamento, por que o tratamento foi estritamente necessário.

✗ B) Incorreta. O Art. 4a(1)(e) manda apagar esses dados assim que o viés for corrigido ou ao fim do prazo de retenção, o que ocorrer primeiro.

✗ C) Incorreta. O Art. 4a(1)(d) exige que as categorias especiais de dados não sejam transmitidas, transferidas nem acessadas por terceiros.

> **Dica de prova:** Art. 4a: dados sensíveis para corrigir viés só se outros dados não bastarem; sem repasse a terceiros e com eliminação depois.

D9. B) Impressão digital usada para identificar de forma única cada aluno na catraca de entrada
→ revise o capítulo 3

Por quê: Categorias especiais (Art. 9 do GDPR): origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos para identificar uma pessoa de forma única, dados de saúde e dados sobre vida sexual ou orientação sexual. O tratamento é proibido salvo em hipóteses como consentimento explícito, obrigações trabalhistas, interesse vital, interesse público relevante ou saúde.

✗ A) Incorreta. O e-mail profissional com nome e sobrenome é dado pessoal comum, e não dado sensível.
✗ C) Incorreta. Endereço IP e identificador de cookie são dados pessoais, mas não estão entre as categorias especiais do Art. 9.
✗ D) Incorreta. Dados de localização são dados pessoais e podem ter regras setoriais, mas não integram as categorias especiais do GDPR.

> **Dica de prova:** Biometria para identificar de forma única = dado sensível (Art. 9). IP, cookie e localização = pessoais, não sensíveis.

D10. D) Diversidade, não discriminação e equidade (acessibilidade e desenho universal); Art. 16(l) → revise o capítulo 4

Por quê: Requisito 5 do HLEG (diversidade, não discriminação e equidade) inclui evitar vieses injustos, acessibilidade e desenho universal e participação das partes interessadas: sistemas centrados no usuário, utilizáveis por todos, independentemente de idade, gênero ou capacidades, seguindo normas de acessibilidade. Na Lei da IA, o Art. 16(l) exige do fornecedor de risco elevado conformidade com os requisitos de acessibilidade das Diretivas 2016/2102 e 2019/882.

✗ A) Incorreta. O bem-estar social e ambiental trata de sustentabilidade e impacto social; e o Art. 16(l) trata de acessibilidade, e não de consumo de energia.
✗ B) Incorreta. A robustez trata de segurança, exatidão e resiliência técnica; o problema descrito é de acesso de pessoas com deficiência.
✗ C) Incorreta. O Art. 14 trata da supervisão humana pelo responsável pela implantação, e não da acessibilidade para as pessoas que usam o serviço.

> **Dica de prova:** Acessibilidade e desenho universal = requisito de diversidade e equidade (HLEG) + Art. 16(l) da Lei da IA.

D11. A) Estruturar a governança interna com elas, cumprindo à parte os requisitos legais do AI Act → revise o capítulo 4

Por quê: As Orientações Éticas para uma IA de Confiança (HLEG, 2019) não têm força de lei. O considerando 27 do AI Act reconhece seus sete princípios como base para uma IA confiável e para códigos de conduta voluntários, mas as obrigações do sistema de risco elevado vêm do regulamento: gestão de riscos, dados, documentação, supervisão humana e avaliação de conformidade.

✗ B) Incorreta. As orientações são voluntárias e não substituem os requisitos obrigatórios do AI Act.
✗ C) Incorreta. A presunção de conformidade vem de normas harmonizadas publicadas no Jornal Oficial (artigo 40), não das orientações do HLEG.
✗ D) Incorreta. As orientações foram feitas para todos os setores, inclusive a indústria e o setor público.

> **Dica de prova:** Orientações do HLEG: boas práticas voluntárias; AI Act: obrigação legal.

D12. B) Apresentar reclamação à autoridade de fiscalização do mercado, como qualquer pessoa física ou jurídica → revise o capítulo 4

Por quê: O Art. 85 garante a qualquer pessoa física ou jurídica com motivos para considerar que houve infração o direito de reclamar à autoridade de fiscalização do mercado competente. As reclamações são consideradas nas atividades de fiscalização, conforme o Regulamento (UE) 2019/1020, sem prejuízo de outros recursos administrativos ou judiciais. É diferente do direito à explicação (Art. 86), que exige ser pessoa afetada por decisão.

✗ A) Incorreta. O Art. 85 não cria etapa prévia junto ao fornecedor; o prazo de 15 dias lembra a notificação de incidentes graves, que é outra obrigação.

✗ C) Incorreta. O Art. 85 não exige ser afetado: basta ter motivos para considerar que houve infração ao regulamento.

✗ D) Incorreta. O Art. 85 indica a autoridade de fiscalização do mercado; o Gabinete de IA atua sobretudo na supervisão de modelos de IA de finalidade geral.

> **Dica de prova:** Art. 85: qualquer pessoa física ou jurídica reclama à autoridade de fiscalização do mercado; não precisa ser afetada.

Agora, treine no formato real

Faça as 6 provas completas do curso EXIN AI Compliance: 240 questões inéditas, tempo do exame, explicação de cada alternativa e link da documentação para revisar.

Ver as 6 provas completas e o cupom do mês →

Até o dia da prova, uma revisão por dia no seu feed

Instagram @strecht.simulados

Um post de prova por dia: questão comentada, pegadinhas e o "não confunda" de cada certificação.

Seguir no Instagram →

YouTube Strecht Simulados

Shorts diários com pegadinhas de prova e, aos sábados, um simulado comentado.

Inscrever-se no canal →

Material independente de preparação, sem afiliação ou endosso de EXIN. As questões são inéditas e não reproduzem a prova real.