VLK ADV

Onde o **Direito** impulsiona a **Inovação.**

INTELIGÊNCIA ARTIFICIAL: Riscos, Incidentes e Governança

DA INCERTEZA REGULATÓRIA À VANTAGEM COMPETITIVA

- 10 razões para governar a IA agora
- 10 etapas do programa de governança de IA

INCIDENTES DE IA

- O que são incidentes e “perigos” de IA
- Caso prático: estratégia de atuação

vlklaw.com.br

1 GOVERNANÇA DE IA: DA INCERTEZA REGULATÓRIA À VANTAGEM COMPETITIVA

Governar a IA não significa limitar seu potencial, mas criar as condições para inovar com proteção de direitos, eficiência, confiança e segurança.

10 RAZÕES PARA GOVERNAR A IA AGORA

1. Proteger pessoas e direitos fundamentais

Prevenir discriminação, vieses, falta de transparência, erros, decisões inadequadas e violações à privacidade, assegurando supervisão humana proporcional ao risco e proteção aos direitos potencialmente afetados pela IA.

2. Cumprir as normas já aplicáveis

Conforme o contexto de uso, a IA já está sujeita à legislação vigente (como LGPD, Código Civil, Código de Defesa do Consumidor, Marco Civil da Internet e Lei de Direitos Autorais) e a normas setoriais e orientações de autoridades e entidades (como ANPD, Anatel, ANS, CFM e MEC), além de legislações estaduais (tais quais as existentes em Goiás e no Ceará). A aplicação dessas normas já se traduz em procedimentos fiscalizatórios e precedentes judiciais (inclusive em superior instância) diretamente relacionados ao uso de IA.

3. Demonstrar conformidade

Transformar obrigações jurídicas e princípios éticos em processos, controles e evidências verificáveis perante autoridades, clientes, investidores e parceiros.

4. Prevenir responsabilização e perdas

Mitigar riscos civis, regulatórios, trabalhistas, consumeristas e concorrenciais, além de reduzir a ocorrência e os impactos de incidentes, sanções, perdas financeiras e danos reputacionais.

5. Proteger ativos empresariais

Preservar dados, propriedade intelectual, informações confidenciais e segredos de negócio durante todo o ciclo de vida das aplicações de IA.

6. Definir responsabilidades

Estabelecer papéis, competências e alçadas decisórias entre administradores, áreas internas, desenvolvedores, fornecedores e usuários, reduzindo zonas cinzentas na cadeia de IA.

7. Fortalecer a segurança cibernética e a resiliência

Proteger aplicações, modelos, dados e infraestruturas contra ataques, manipulação, vazamentos e usos indevidos, bem como mitigar riscos decorrentes do uso da IA para potencializar ameaças cibernéticas.

8. Antecipar futura regulação e seguir padrões internacionais

O PL nº 2.338/2023 propõe marco regulatório baseado em gestão de riscos, governança, transparência, supervisão humana e responsabilização dos agentes, em convergência com parâmetros internacionais como o EU AI Act, entre outras normas e boas práticas. Antecipar essas tendências reduz custos de adequação.

9. Fortalecer confiança e reputação

Demonstrar responsabilidade perante clientes, colaboradores, investidores, reguladores e sociedade

88%
das organizações reconhecem benefícios da IA responsável para a construção de confiança
Cisco 2025 Data Privacy Benchmark Study

43%
dos executivos associam a IA responsável à reputação e à confiabilidade da marca
Accenture–Stanford Executive Survey, N=1.000

51%
dos líderes associam a IA responsável à melhoria da cibersegurança e da proteção de dados
PwC, Responsible AI Survey 2025.

10. Transformar segurança jurídica em vantagem competitiva

Criar condições para experimentar, aprovar e escalar soluções com maior previsibilidade, velocidade e adoção.

49%
dos executivos consideram a IA responsável fator relevante para o crescimento da receita relacionada à tecnologia
Accenture–Stanford Executive Survey, N=1.000

18%
Esse é o percentual que as empresas pioneiras podem alcançar de incremento médio em sua receita
Accenture–Stanford Executive Survey, N=1.000

58%
dos executivos nos EUA afirmam que iniciativas de IA responsável aumentam o ROI e a eficiência organizacional
PwC, Responsible AI Survey 2025

Organizações com políticas de IA responsável reportam resultados melhores de negócio, maior confiança dos clientes, redução de incidentes e maior eficiência operacional.
AI Index Report 2026 (Stanford HAI)

10 ETAPAS DO PROGRAMA DE GOVERNANÇA DE IA

1

Alinhamento entre governança, estratégia de inovação e apetite a risco
Alinhar o uso da IA à estratégia de inovação, aos objetivos e aos valores corporativos, definindo princípios, prioridades, limites e riscos aceitáveis

2

Modelo de governança e responsabilidades
Definir responsabilidades e comprometimento da alta direção, a instância central de governança, demais instâncias decisórias, distribuindo atribuições entre negócio, tecnologia, jurídico, privacidade, riscos, compliance e cibersegurança, com alçadas decisórias, segregação de funções e escalonamento

3

Inventário e classificação
Mapear sistemas, modelos, agentes, casos de uso, dados, integrações e fornecedores, classificando riscos (proibitivo, alto ou baixo) e papéis dos agentes de IA na cadeia de valor (desenvolvedor, aplicador, integrador, distribuidor ou usuário)

4

Avaliação de riscos e impactos
Identificar os requisitos legais aplicáveis no contexto de uso, riscos jurídicos, éticos, operacionais e cibernéticos, com requisitos proporcionais para qualidade, representatividade, proveniência, uso legítimo dos dados, e proteção de modelos, sistemas e infraestruturas contra ataques, manipulações e vazamentos

5

Políticas e documentação
Estruturar políticas, procedimentos, registros, documentação técnica e cláusulas contratuais

6

Incorporação da governança aos processos
Integrar as políticas e controles de IA aos fluxos de inovação, desenvolvimento, contratação, aprovação e uso, com registros e documentação técnica, como model cards, system cards, além de supervisão humana, quando aplicáveis

7

Gestão de terceiros e da cadeia de IA
Estabelecer critérios de avaliação, seleção, due diligence, requisitos contratuais, monitoramento e responsabilização de fornecedores e parceiros

8

Letramento e cultura de IA
Treinar a liderança, equipes técnicas e usuários conforme suas funções e exposição ao risco, promovendo uso crítico, seguro e responsável da IA

9

Validação e implementação
Realizar avaliações de impacto algorítmico e testes de desempenho, acurácia, robustez, vieses, segurança e efetividade da supervisão humana antes da entrada em produção, com critérios de aceitação, mitigação de riscos e aprovação competente

10

Monitoramento, incidentes e melhoria contínua
Monitorar desempenho, desvios, mudanças, incidentes e conformidade durante todo o ciclo de vida da IA, com medidas corretivas, resposta a incidentes, revisão periódica e descontinuação segura

Governança madura não se limita a princípios e políticas:
integra e exige comprometimento da alta gestão, cultura, responsabilidades, classificação, avaliações de impacto, evidências, critérios de liberação, monitoramento em produção, gestão de mudanças e resposta a incidentes.

2 INCIDENTES DE IA

O QUE SÃO INCIDENTES E "PERIGOS" DE IA?

Incidentes: eventos relacionados ao desenvolvimento, uso ou o mau funcionamento de um sistema de IA que provoque, direta ou indiretamente: danos à saúde de pessoas; interrupção da gestão e operação de infraestruturas críticas; violações de direitos humanos ou descumprimento de obrigações destinadas a proteger direitos fundamentais, trabalhistas e de propriedade intelectual; ou danos ao patrimônio, comunidades ou ao meio ambiente.

"Perigo" de IA (*AI hazard*): é o evento que poderia plausivelmente provocar um incidente de IA, ainda que o dano não tenha se materializado.
Fonte: OCDE.

Uma governança madura deve identificar, registrar e tratar ambas as situações

São **800 a 900 incidentes** únicos envolvendo IA até o primeiro trimestre de 2026, com um crescimento de cerca de **130 a 180 novos incidentes por ano**
(AI Incident Database - AIID)

Em 2025, foram **362 incidentes de IA**, com crescimento de aproximadamente **55%** em relação ao ano anterior
(Stanford AI Index 2026)

COMO INCIDENTES E RISCOS DE IA SE MANIFESTAM?

VETORES E CAUSAS
prompt injection, envenenamento de dados, manipulação de modelos, comprometimento de fornecedores e uso não autorizado de IA.

FALHAS DOS SISTEMAS OU CONTROLES
perda de desempenho ao longo do tempo, respostas não fundamentadas, permissões excessivas, supervisão humana ineficaz, segregação insuficiente entre dados e instruções, perda de controle sobre agentes ou indisponibilidade.

IMPACTOS
exposição de dados pessoais e segredos de negócio, discriminação, decisões imprecisas ou incorretas, danos à segurança, interrupções de operação, violações de direitos e prejuízos financeiros e reputacionais.

CASO PRÁTICO
Uma empresa utiliza agente de IA conectado a bases internas para responder dúvidas de colaboradores e clientes. Sem homologação corporativa, ferramenta externa é integrada ao agente. Ao processar o conteúdo que continha instrução maliciosa (*prompt injection*), o agente executa ação não pretendida e expõe dados salariais, avaliações de desempenho e outras informações confidenciais. O incidente combina integração não autorizada, permissões excessivas e ausência de segregação entre dados e instruções.

COMO AGIR DIANTE DESSE INCIDENTE?

1. **Detectar e classificar**
confirmar os sistemas, ferramentas e integrações envolvidos. Avaliar o nexo entre a IA e o dano

2. **Conter e preservar evidências**
Isolar ou desabilitar o agente, bloquear a integração, revogar acessos e preservar prompts, configurações, versões, logs e ações executadas, mantendo a integridade e a cadeia de custódia das evidências

3. **Avaliar gravidade e obrigações**
Determinar a natureza, volume e criticidade dos dados expostos e operações afetadas. Avaliar severidade e obrigação legal ou dever ético de reportar a reguladores, pessoas expostas e ao mercado

4. **Investigar a causa-raiz**
Identificar, eventualmente com apoio de peritos especializados, a origem do incidente, as vulnerabilidades exploradas e as falhas técnicas, humanas ou de governança que permitiram sua ocorrência

5. **Corrigir e recuperar**
Reduzir permissões, segregar dados e instruções, revisar filtros de entrada, restringir ferramentas não autorizadas, reverter versões e testar a segurança do sistema antes de sua retomada

6. **Registrar**
Manter o registro cronológico do incidente, das evidências, decisões, comunicações e medidas adotadas, formalizando sua conclusão e os riscos residuais

7. **Aprender e monitorar**
Atualizar avaliações de impacto, indicadores de risco, contratos e critérios de liberação. Reforçar treinamentos, aprimorar controles e adotar monitoramento intensificado após a retomada

Governança madura não é sinônimo de que incidentes de IA nunca ocorrerão, mas a capacidade de detectá-los precocemente, conter e reparar seus impactos, prestar contas, recuperar as operações com segurança e transformar cada ocorrência em aprendizado e maior resiliência.

VLK Direito, Inovação & Tecnologia

SOBRE NÓS

No VLK, **o Direito não é barreira**. É impulso para **inovar, viabilizar negócios** e construir uma sociedade mais próspera e justa.

Somos uma **boutique de Direito Digital** movida por **entregas que fazem a diferença**.

Conciliamos:

» Riscos e oportunidades;
» Complexidade e clareza; e
» Proteção e progresso.

Não importa o quão ousado seja o projeto: **faremos acontecer**, com segurança e **quebrando formalismos desnecessários**, nas seguintes áreas:

» Proteção de Dados Pessoais
» Governança Ética e Responsável de IA
» Cibersegurança e Resposta a Incidentes
» Legal Marketing e Propriedade Intelectual
» Regulação de Tecnologia
» Contencioso Estratégico