IA corporativa sem governança: quais são os riscos jurídicos para empresas?

Como o uso de ChatGPT, Gemini, Copilot e outras ferramentas de inteligência artificial sem política interna pode expor dados pessoais, contratos, segredos empresariais e informações estratégicas da sua empresa.

Por Mariana Malaman
Advogada com atuação em contratos de tecnologia, LGPD, governança de IA, SaaS, proteção de dados e estruturação jurídica de produtos digitais.

Resposta curta: qual é o risco da IA sem governança?

O principal risco da IA corporativa sem governança é a perda de controle sobre informações sensíveis.

Quando colaboradores inserem dados pessoais, contratos, documentos internos, estratégias comerciais, bases de clientes, relatórios financeiros ou informações confidenciais em ferramentas de inteligência artificial não autorizadas, a empresa pode violar a LGPD, descumprir obrigações contratuais de confidencialidade, realizar transferência internacional irregular de dados e perder rastreabilidade sobre informações críticas.

O problema não é usar inteligência artificial.

O problema é usar IA sem saber **quais dados estão sendo inseridos, em quais ferramentas, por quais pessoas, sob quais termos de uso e com quais consequências jurídicas**.

O que é IA corporativa sem governança?

IA corporativa sem governança é o uso de ferramentas de inteligência artificial por colaboradores, áreas internas ou fornecedores sem política aprovada, sem controle sobre os dados inseridos, sem revisão contratual da plataforma utilizada, sem critérios de segurança da informação e sem validação humana dos resultados gerados.

Esse uso pode envolver ferramentas como ChatGPT, Gemini, Copilot, Claude, Perplexity, assistentes de reunião, tradutores automáticos, plataformas de transcrição, geradores de apresentações, soluções de automação, copilotos de código e sistemas de análise documental.

Na prática, a IA já está sendo usada dentro das empresas para:

- resumir contratos;
- revisar documentos;
- redigir e-mails;
- analisar planilhas;
- transcrever reuniões;

- criar apresentações;
- interpretar bases de dados;
- gerar relatórios;
- revisar propostas comerciais;
- estruturar respostas a clientes;
- apoiar pareceres, diagnósticos ou decisões internas.

A ferramenta pode ser excelente.

O risco está no conteúdo inserido nela.

Uma coisa é pedir para a IA organizar ideias públicas para uma apresentação. Outra, completamente diferente, é inserir uma minuta contratual confidencial, uma base de clientes, uma estratégia de preço, um relatório financeiro ou dados pessoais de colaboradores em uma plataforma externa sem qualquer validação jurídica ou técnica.

Por que esse risco já está acontecendo nas empresas?

Porque o uso de IA raramente começa pelo jurídico, pela segurança da informação ou pela diretoria.

Ele começa no operacional.

Um colaborador testa uma ferramenta para ganhar tempo. Outro usa para resumir uma reunião. Um terceiro sobe uma planilha para análise. Em pouco tempo, a IA deixa de ser experimento e vira rotina.

O problema é que essa rotina, na maioria das empresas, não passa por:

- aprovação formal da ferramenta;
- revisão dos termos de uso;
- análise de segurança da informação;
- avaliação de proteção de dados;
- verificação de transferência internacional;
- assinatura de DPA;
- política interna de uso;
- classificação da informação;
- treinamento dos usuários;
- regra de validação humana dos outputs;
- procedimento de resposta a incidentes.

Por isso, muitas empresas acreditam que estão apenas “testando IA”, quando, na prática, já criaram um canal informal de saída de informações estratégicas.

A empresa que usa IA sem governança não perde apenas controle sobre a ferramenta. Ela perde controle sobre os dados, os contratos, os outputs e a própria rastreabilidade das decisões tomadas com apoio tecnológico.

O que as ferramentas de IA fazem com os dados inseridos?

Depende da ferramenta, do plano contratado, das configurações de privacidade e dos termos aplicáveis.

E esse é exatamente o ponto.

Nem toda ferramenta de IA trata os dados da mesma forma. Algumas podem reter prompts por determinado período. Outras podem usar informações para aprimoramento do serviço. Algumas permitem desativar o uso dos dados para treinamento. Outras oferecem planos corporativos com controles administrativos, segregação de ambiente, DPA, logs, gestão centralizada e regras mais restritivas de privacidade.

Sem revisão prévia, a empresa simplesmente não sabe.

E, quando não sabe, não governa.

A pergunta correta não é:

> "A ferramenta é boa?"

A pergunta correta é:

> "Essa ferramenta pode receber os dados que os nossos colaboradores estão inserindo nela?"

Essa diferença muda toda a análise jurídica.

Usar IA no trabalho pode violar a LGPD?

Sim, se envolver dados pessoais sem base legal, finalidade, transparência, segurança, controle contratual ou governança adequada.

A LGPD se aplica ao tratamento de dados pessoais, inclusive em meios digitais, realizado por pessoas naturais ou jurídicas de direito público ou privado. A lei tem como objetivo proteger direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.

O conceito de tratamento de dados é amplo. Ele pode envolver coleta, acesso, utilização, armazenamento, processamento, transmissão, compartilhamento, transferência, eliminação e outras operações com dados pessoais. Portanto, quando um colaborador insere dados de clientes, colaboradores, leads, usuários ou parceiros em uma ferramenta de IA, a empresa pode estar realizando tratamento de dados por meio de um terceiro.

Isso exige respostas claras:

- qual dado foi inserido?
- qual a finalidade?

- qual a base legal?
- quem é o fornecedor?
- os dados são armazenados?
- por quanto tempo?
- há uso para treinamento?
- há revisão humana pelo fornecedor?
- há suboperadores?
- há transferência internacional?
- existe DPA?
- há mecanismos de segurança?
- o titular foi informado, quando necessário?
- o uso é compatível com a finalidade original da coleta?

Se a empresa não sabe responder essas perguntas, o uso de IA já está fora de um padrão mínimo de governança.

O uso de IA pode gerar transferência internacional de dados?

Sim.

Muitas ferramentas de IA operam com infraestrutura global, servidores fora do Brasil, subcontratados internacionais ou cadeias técnicas distribuídas entre diferentes países.

A ANPD regulamentou a transferência internacional de dados pessoais por meio da Resolução CD/ANPD nº 19/2024, que estabelece procedimentos e mecanismos como decisões de adequação, cláusulas-padrão contratuais, cláusulas específicas e normas corporativas globais.

Isso significa que, antes de liberar uma ferramenta de IA para uso corporativo, a empresa deve verificar se existe mecanismo jurídico adequado para eventual transferência internacional de dados.

O ponto não é impedir o uso de tecnologia estrangeira.

O ponto é saber se a empresa consegue demonstrar que o uso é compatível com a LGPD, com os contratos assinados com clientes e com suas próprias políticas internas.

A matriz dos 5 riscos da IA corporativa sem governança

O risco jurídico do uso descontrolado de IA nas empresas pode ser dividido em cinco frentes principais:

1. dados pessoais e LGPD;
2. confidencialidade e segredos empresariais;
3. propriedade intelectual;
4. outputs sem validação humana;
5. responsabilidade contratual perante clientes, parceiros e terceiros.

Essa matriz ajuda a empresa a sair da discussão genérica sobre “usar ou não usar IA” e entrar na pergunta certa:

> “Quais usos de IA são permitidos, com quais dados, em quais ferramentas e sob quais controles?”

1. Risco de exposição de dados pessoais

Dados pessoais de clientes, colaboradores, candidatos, fornecedores, leads e usuários podem circular em prompts, anexos, planilhas, transcrições, imagens, relatórios e bases de conhecimento inseridas em ferramentas de IA.

O risco aumenta quando há:

- dados pessoais sensíveis;
- dados de crianças e adolescentes;
- dados de saúde;
- dados financeiros;
- dados de geolocalização;
- documentos de identificação;
- bases de clientes;
- informações de RH;
- registros de atendimento;
- dados de consumidores;
- informações protegidas por sigilo.

Em caso de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, o controlador deve comunicar a ANPD e os titulares, nos termos da regulamentação aplicável. A ANPD publicou a Resolução nº 15/2024 para disciplinar a comunicação de incidentes de segurança e fortalecer práticas de governança, prevenção, responsabilização e prestação de contas.

Ou seja: quando a IA é usada sem controle, um simples prompt pode se transformar em evento relevante de privacidade.

2. Risco de violação de confidencialidade e segredos empresariais

O risco da IA corporativa não se limita à LGPD.

Em muitos casos, o maior problema está na confidencialidade.

Imagine as seguintes situações:

- um contrato em negociação é inserido em uma IA pública;
- uma proposta comercial estratégica é resumida por uma ferramenta externa;
- uma planilha de margem é analisada por uma plataforma não autorizada;
- uma reunião de diretoria é transcrita por um assistente sem revisão contratual;
- um documento recebido sob NDA é usado como input;

- uma tese jurídica é enviada para uma ferramenta sem controle de retenção;
- um roadmap de produto é compartilhado com IA;
- uma base de clientes é usada para gerar segmentações comerciais.

Nesses casos, mesmo que não exista dado pessoal, pode haver violação de sigilo, descumprimento contratual e perda de proteção sobre informação estratégica.

Confidencialidade não é apenas “não publicar na internet”.

Confidencialidade também significa não compartilhar informação protegida com terceiros não autorizados, inclusive plataformas digitais, fornecedores de tecnologia e ferramentas externas de processamento.

3. Risco de propriedade intelectual

Ferramentas de IA também levantam questões relevantes de propriedade intelectual.

A empresa precisa definir, em política interna e contratos, como serão tratados:

- prompts criados por colaboradores;
- outputs gerados pela IA;
- uso de materiais de terceiros como input;
- inserção de códigos, imagens, textos ou bases protegidas;
- titularidade de conteúdos gerados;
- risco de reprodução de conteúdo protegido;
- uso de marca, voz, imagem ou identidade de terceiros;
- reaproveitamento de documentos internos para treinamento ou automação.

O risco não está apenas no que a IA entrega.

Está também no que a empresa fornece para que a IA produza o resultado.

Se um colaborador usa material de cliente, documento protegido, código proprietário ou conteúdo de terceiro em uma ferramenta de IA, a empresa pode criar uma cadeia de risco difícil de rastrear depois.

4. Risco de decisões baseadas em outputs não validados

IA pode errar.

Pode inventar informações. Pode omitir contexto. Pode gerar respostas convincentes e juridicamente frágeis. Pode produzir análises financeiras incompletas, interpretações contratuais equivocadas, diagnósticos incorretos ou recomendações incompatíveis com a realidade da empresa.

Por isso, a governança de IA deve estabelecer uma regra simples:

> Nenhum output de IA deve ser usado em decisão relevante, comunicação externa, entrega a cliente, parecer, proposta comercial, análise jurídica, avaliação de risco ou documento estratégico sem validação humana qualificada.

O problema não é usar IA como apoio.

O problema é terceirizar julgamento.

A IA pode acelerar o trabalho. Mas não deve substituir responsabilidade profissional, revisão técnica e decisão humana em temas sensíveis.

5. Risco de responsabilidade contratual perante clientes e terceiros

Empresas normalmente assumem obrigações de confidencialidade, segurança da informação, proteção de dados, uso restrito de informações, limitação de acesso e cuidado com documentos de clientes.

Se um colaborador insere informações protegidas em uma ferramenta de IA não autorizada, a empresa pode violar contratos já assinados.

Isso vale especialmente para empresas que atuam com:

- tecnologia;
- SaaS;
- saúde;
- educação;
- financeiro;
- jurídico;
- RH;
- segurança da informação;
- marketing;
- dados;
- atendimento ao consumidor;
- outsourcing;
- consultoria;
- desenvolvimento de software;
- serviços regulados.

Nesses setores, informações de clientes e usuários são ativos críticos.

E ativos críticos não podem circular em ferramentas invisíveis.

Tabela prática: situações comuns e riscos jurídicos

Situação	Risco jurídico	Medida recomendada

Colaborador insere contrato de cliente em IA pública	Violação de confidencialidade e possível tratamento indevido de dados pessoais	Proibir documentos confidenciais em ferramentas não autorizadas
Área comercial usa IA para analisar base de leads	Tratamento de dados pessoais sem controle adequado	Revisar base legal, finalidade, DPA e política de privacidade
Reunião estratégica é transcrita por ferramenta externa	Exposição de segredo empresarial	Autorizar apenas ferramentas aprovadas e com contrato corporativo
RH usa IA para resumir avaliações de colaboradores	Tratamento de dados pessoais e risco trabalhista/discriminatório	Criar regras específicas para dados de colaboradores
Jurídico usa IA para revisar contrato sob NDA	Violação de sigilo profissional ou contratual	Usar apenas ambiente autorizado e, quando possível, anonimizar dados
TI usa IA para revisar código-fonte	Exposição de propriedade intelectual	Definir ferramentas permitidas e política de uso de código
IA gera resposta enviada ao cliente sem revisão	Erro técnico, comercial ou jurídico	Exigir validação humana antes de qualquer uso externo
Ferramenta processa dados fora do Brasil	Transferência internacional de dados	Verificar mecanismo legal aplicável e cláusulas contratuais

Posso usar ChatGPT, Gemini ou Copilot com dados da empresa?

A resposta depende da versão da ferramenta, do plano contratado, das configurações de privacidade, dos termos de uso e do tipo de dado inserido.

O uso de contas pessoais ou versões públicas para processar dados corporativos tende a ser mais arriscado, especialmente quando envolve:

- dados pessoais;
- documentos de clientes;
- informações financeiras;
- contratos;
- código-fonte;
- estratégias comerciais;

- informações protegidas por NDA;
- dados de colaboradores;
- segredos empresariais;
- documentos ainda não divulgados ao mercado.

Em ambiente corporativo, a empresa deve avaliar planos empresariais, controles administrativos, retenção de dados, uso para treinamento, localização do processamento, subprocessadores, DPA, segurança da informação e possibilidade de auditoria.

Não basta perguntar se a ferramenta é famosa.

É preciso verificar se ela é adequada ao risco da informação que será processada.

“Minha empresa tem jurídico. Isso não resolve?”

Não necessariamente.

Ter jurídico não significa ter governança de IA.

O jurídico normalmente é acionado para revisar contratos, responder incidentes, apoiar negociações e analisar riscos. Mas o uso cotidiano de IA raramente começa com uma consulta formal.

Ele começa com frases simples:

> “Vou jogar esse contrato na IA para resumir.”
>
> “Vou subir essa planilha para organizar os dados.”
>
> “Vou pedir para a ferramenta melhorar esse e-mail.”
>
> “Vou transcrever essa reunião para ganhar tempo.”
>
> “Vou pedir para a IA revisar essa proposta antes de enviar.”

Quando esse comportamento se espalha sem política interna, o jurídico só descobre depois.

E governança feita depois do incidente é sempre mais cara.

O que a empresa não deve fazer

A empresa não deve:

- permitir uso livre de IA sem política interna;
- aceitar que colaboradores usem contas pessoais para documentos corporativos;
- inserir dados pessoais sensíveis em ferramentas não autorizadas;
- usar contratos, propostas ou documentos de clientes em plataformas sem revisão;
- subir planilhas estratégicas em ferramentas externas não aprovadas;

- transcrever reuniões confidenciais sem avaliar o fornecedor;
- usar outputs de IA em decisões relevantes sem validação humana;
- contratar ferramentas de IA sem revisar DPA, confidencialidade, retenção e transferência internacional;
- tratar governança de IA como responsabilidade exclusiva do jurídico;
- acreditar que bloquear completamente a IA resolverá o problema.

Proibir sem orientar apenas empurra o uso para a informalidade.

E uso informal é exatamente o que aumenta o risco.

Como estruturar uma política interna de uso de IA?

A política não precisa ser longa.

Precisa ser clara, aplicável e compreendida pelas áreas de negócio.

Uma boa política interna de IA deve responder a seis perguntas.

1. Quais ferramentas são autorizadas?

A empresa deve manter uma lista de ferramentas permitidas, separando, por exemplo:

- ferramentas autorizadas para uso geral;
- ferramentas autorizadas apenas para áreas específicas;
- ferramentas permitidas somente com dados anonimizados;
- ferramentas em teste;
- ferramentas proibidas.

Sem lista oficial, cada colaborador vira seu próprio comitê de tecnologia.

2. Quais dados não podem ser inseridos?

A política deve proibir, salvo autorização expressa, o uso de IA com:

- dados pessoais sensíveis;
- dados de crianças e adolescentes;
- documentos de clientes;
- contratos em negociação;
- informações financeiras não públicas;
- bases de clientes;
- informações de RH;
- segredos empresariais;
- código-fonte;
- credenciais;

- dados de saúde;
- documentos sob NDA;
- informações protegidas por sigilo profissional;
- estratégias comerciais;
- documentos de M&A;
- relatórios de incidente.

A regra deve ser simples: quanto mais sensível a informação, maior o controle.

3. Quando a IA pode ser usada?

A empresa pode permitir o uso de IA em atividades de menor risco, como:

- organização de ideias;
- criação de rascunhos;
- revisão de clareza;
- elaboração de checklists;
- apoio em apresentações;
- tradução de textos não confidenciais;
- criação de estruturas iniciais;
- pesquisa preliminar;
- melhoria de linguagem.

Mas deve exigir validação humana antes de qualquer uso externo ou decisão relevante.

4. Quem aprova exceções?

Exceções envolvendo dados pessoais, documentos confidenciais, informações estratégicas ou materiais de clientes devem passar por uma instância formal de aprovação.

Essa instância pode envolver:

- jurídico;
- DPO ou encarregado;
- segurança da informação;
- compliance;
- área de tecnologia;
- gestor da área de negócio;
- comitê de governança digital.

O importante é que a exceção não fique na mão de quem quer apenas ganhar velocidade.

5. Como os outputs devem ser validados?

A política deve deixar claro que outputs de IA são materiais de apoio.

Não são decisões finais.

Isso vale para:

- pareceres;
- relatórios;
- respostas a clientes;
- propostas comerciais;
- documentos jurídicos;
- análises financeiras;
- decisões de RH;
- diagnósticos técnicos;
- comunicações externas;
- documentos regulatórios.

A revisão humana deve ser proporcional ao risco do uso.

6. Quais são as consequências do descumprimento?

Política sem consequência vira sugestão.

A empresa deve prever medidas proporcionais para uso indevido, especialmente quando houver exposição de dados pessoais, informações confidenciais, documentos de clientes, credenciais, código-fonte ou segredos empresariais.

O objetivo não é punir o colaborador que busca produtividade.

É deixar claro que inovação não elimina responsabilidade.

Modelo de regra interna simples para começar

Uma política inicial pode começar com uma regra objetiva:

> É vedado inserir em ferramentas de inteligência artificial não autorizadas quaisquer dados pessoais, informações confidenciais, documentos de clientes, contratos em negociação, dados financeiros, segredos de negócio, credenciais, códigos, informações estratégicas ou conteúdos protegidos por sigilo profissional, salvo aprovação prévia da área responsável e validação das condições contratuais, técnicas e de proteção de dados aplicáveis.

Essa regra não resolve tudo.

Mas muda o padrão de comportamento.

E, em governança de IA, mudar o padrão de comportamento é o primeiro passo.

O que revisar nos contratos com fornecedores de IA?

Ferramentas de IA usadas em ambiente corporativo devem ser tratadas como fornecedores relevantes.

Antes de contratar ou autorizar uma ferramenta, a empresa deve revisar:

- termos de uso;
- política de privacidade;
- DPA;
- cláusulas de confidencialidade;
- localização dos dados;
- retenção de prompts;
- uso dos dados para treinamento;
- subprocessadores;
- transferência internacional;
- medidas de segurança;
- criptografia;
- logs;
- auditoria;
- exclusão de dados;
- suporte em incidentes;
- limitação de responsabilidade;
- indenização por violação de direitos de terceiros;
- propriedade intelectual sobre inputs e outputs;
- disponibilidade de plano corporativo;
- controles administrativos;
- possibilidade de desativar treinamento com dados da empresa.

Se a ferramenta vai processar informação corporativa, ela não pode ser tratada como aplicativo informal.

Ela deve passar por diligência jurídica, técnica e operacional.

Planos corporativos de IA eliminam o risco?

Não.

Eles podem reduzir o risco, mas não substituem governança.

Planos corporativos normalmente oferecem controles melhores, como:

- gestão centralizada de usuários;
- configurações de privacidade;
- logs;
- segregação de ambiente;
- contratos empresariais;

- DPA;
- suporte;
- opções de retenção;
- controles administrativos;
- políticas de segurança mais claras.

Mas a contratação de um plano corporativo não resolve, sozinha, três problemas:

1. colaboradores ainda podem inserir dados que não deveriam;
2. outputs ainda podem ser usados sem revisão;
3. áreas ainda podem contratar ou usar ferramentas paralelas.

A ferramenta pode ser adequada.

O uso pode continuar inadequado.

Como implementar governança mínima de IA em 30 dias?

A empresa não precisa começar com um projeto complexo.

Pode começar com um plano de governança mínima.

Semana 1: mapeamento

Identificar:

- quais ferramentas de IA são usadas;
- por quais áreas;
- com quais finalidades;
- se há uso de contas pessoais;
- se há documentos de clientes;
- se há dados pessoais;
- se há transcrição de reuniões;
- se há uso em decisões relevantes.

Semana 2: classificação de risco

Separar usos em categorias:

- permitido;
- permitido com dados públicos;
- permitido com dados anonimizados;
- permitido apenas em ferramenta corporativa;
- depende de aprovação;
- proibido.

Semana 3: política e fornecedores

Criar política curta e revisar os principais fornecedores.

Prioridades:

- ferramentas mais usadas;
- ferramentas que processam dados pessoais;
- ferramentas usadas com documentos de clientes;
- ferramentas de transcrição;
- ferramentas conectadas a e-mail, agenda, CRM, drive ou sistemas internos.

Semana 4: treinamento e comunicação

Treinar as equipes com exemplos práticos.

Não basta dizer:

> "Usem IA com responsabilidade."

É preciso mostrar:

- o que pode;
- o que não pode;
- o que precisa ser anonimizado;
- o que exige aprovação;
- quais ferramentas são permitidas;
- quais dados nunca devem ser inseridos;
- quem procurar em caso de dúvida.

Treinamento genérico não muda comportamento.

Exemplo prático muda.

Checklist executivo: sua empresa já tem governança mínima de IA?

A empresa deve conseguir responder "sim" para estas perguntas:

1. Sabemos quais ferramentas de IA são usadas internamente?
2. Temos lista de ferramentas autorizadas?
3. Existe política interna de uso de IA?
4. A política define dados proibidos?
5. Há regra específica para documentos de clientes?
6. Há regra para dados pessoais e dados sensíveis?
7. Há orientação sobre uso de contas pessoais?
8. Revisamos os termos das principais ferramentas?
9. Temos DPA com fornecedores relevantes?
10. Sabemos se há transferência internacional de dados?
11. Verificamos se os dados podem ser usados para treinamento?
12. Exigimos validação humana dos outputs?

13. Há regra para ferramentas de transcrição de reunião?
14. Há procedimento para incidentes envolvendo IA?
15. Os colaboradores foram treinados com exemplos práticos?
16. A empresa revisa periodicamente novas ferramentas?
17. Jurídico, TI, segurança e áreas de negócio atuam juntos?
18. Há registro de exceções aprovadas?

Se a empresa não consegue responder a essas perguntas, ela não tem governança de IA.

Tem apenas uso informal de IA com risco jurídico acumulado.

FAQ: perguntas frequentes sobre IA corporativa e governança

Empresas podem usar IA no trabalho?

Sim. O uso de IA no ambiente corporativo é possível e, em muitos casos, recomendável. O problema não é usar IA, mas usar ferramentas sem política, sem controle de dados, sem revisão contratual, sem segurança da informação e sem validação humana.

Posso colocar contratos de clientes em ferramentas de IA?

Em regra, não sem avaliação prévia. Contratos podem conter dados pessoais, informações confidenciais, segredos comerciais e obrigações de sigilo. Antes de inserir qualquer documento em IA, é necessário verificar se a ferramenta é autorizada, se há proteção contratual adequada e se o conteúdo pode ser anonimizado.

Usar ChatGPT com dados da empresa viola a LGPD?

Pode violar, dependendo dos dados inseridos, da finalidade, da base legal, do plano utilizado, dos termos de uso, da retenção de dados, da transferência internacional e da existência ou não de contrato adequado com o fornecedor.

A IA pode usar os dados da empresa para treinamento?

Depende da ferramenta, do plano contratado e das configurações de privacidade. Por isso, a empresa deve revisar os termos de uso, política de privacidade, DPA e configurações administrativas antes de autorizar o uso corporativo.

A empresa precisa ter uma política interna de IA?

Sim. Ainda que não exista uma obrigação legal única chamada “política de IA”, a ausência de regras internas aumenta significativamente o risco de incidente, violação de confidencialidade, tratamento inadequado de dados pessoais e falha de prestação de contas.

O colaborador é responsável se usar IA de forma errada?

Pode ser, mas a empresa também precisa demonstrar que orientou, treinou e estabeleceu regras claras. Se não houver política interna, o problema tende a ser visto como falha de governança, não apenas como erro individual.

Plano corporativo de IA resolve o problema?

Não sozinho. Planos corporativos podem oferecer controles melhores, mas a empresa ainda precisa de política interna, classificação de dados, treinamento, revisão contratual, validação humana e monitoramento contínuo.

A empresa deve proibir totalmente o uso de IA?

Na maioria dos casos, não. Proibir completamente pode apenas empurrar o uso para a informalidade. O melhor caminho costuma ser autorizar ferramentas adequadas, definir limites claros e treinar as equipes.

Conclusão: a IA já entrou na empresa. A governança precisa entrar também.

O uso de IA no ambiente corporativo não tem volta.

Colaboradores já usam essas ferramentas para ganhar tempo, reduzir tarefas repetitivas, melhorar textos, organizar dados, resumir documentos e acelerar entregas.

A questão não é mais se a empresa vai usar IA.

A questão é se ela sabe como a IA está sendo usada.

Empresas que estruturam governança conseguem capturar produtividade com segurança jurídica, proteção de dados e responsabilidade operacional.

Empresas que ignoram o tema transformam cada prompt em um potencial ponto de vazamento, cada ferramenta não autorizada em um fornecedor invisível e cada output não validado em um risco de decisão.

A diferença entre inovação e exposição jurídica não está na ferramenta.

Está na governança.

Como o Assis e Mendes pode ajudar

Empresas que ainda não possuem política de uso de IA, matriz de risco, revisão contratual dos fornecedores, treinamento interno e avaliação de LGPD devem tratar o tema como prioridade de governança.

O primeiro passo não é proibir a IA.

É organizar seu uso com segurança jurídica, proteção de dados e clareza operacional.

Para estruturar uma política interna de IA, revisar contratos com fornecedores, avaliar riscos de LGPD ou treinar equipes, fale com a equipe do **Assis e Mendes Advogados**.