POLÍTICA CORPORATIVA DE USO RESPONSÁVEL DE INTELIGÊNCIA ARTIFICIAL

Documento: Política Corporativa de Uso Responsável de Inteligência Artificial
Versão: 1.0
Data: 09/2026
Aprovado por: Fábio Oliveira / Diretor
Periodicidade de Revisão: Anual

CONTROLE DE VERSÃO

Versão	Data	Descrição
1.0	09/2026	• Criação do Documento

1. OBJETIVO

A Iterative reconhece a Inteligência Artificial como uma tecnologia estratégica para evolução da engenharia de software, aumento de produtividade, melhoria da qualidade, automação de atividades e desenvolvimento de novas soluções.

A utilização de Inteligência Artificial deve, entretanto, ocorrer de maneira responsável, segura, ética e compatível com as obrigações assumidas pela Iterative perante seus clientes, colaboradores, parceiros e demais partes interessadas.

Esta Política estabelece princípios, responsabilidades, regras e boas práticas para utilização de ferramentas, modelos, agentes e soluções baseadas em Inteligência Artificial pelos prestadores da Iterative.

O objetivo não é restringir a utilização da IA, mas estabelecer condições para que seus benefícios sejam obtidos preservando:

- a segurança da informação;
- a confidencialidade;
- a privacidade e proteção de dados pessoais;
- a propriedade intelectual;
- os ativos e informações dos clientes;
- a qualidade do software;
- a rastreabilidade das decisões;
- a responsabilidade humana;
- os requisitos contratuais;
- as políticas internas da Iterative;
- e, principalmente, as políticas e diretrizes estabelecidas por cada cliente.

2. ABRANGÊNCIA

Esta Política aplica-se a todos os prestadores que atuem em nome da Iterative, incluindo colaboradores, prestadores de serviços, prestadores alocados, integrantes de squads, consultores, gestores e terceiros autorizados.

Aplica-se ao uso de Inteligência Artificial em atividades como:

desenvolvimento e revisão de código; elaboração de testes; documentação; análise de requisitos; arquitetura; UX/UI; qualidade; DevOps; segurança; sustentação; análise de dados; elaboração de documentos; pesquisa; planejamento; gestão de projetos; automação; atendimento; criação de agentes; análise de código legado e demais atividades prestadores.

3. PRINCÍPIO FUNDAMENTAL: AS REGRAS DO CLIENTE PREVALECEM

Quando o prestador estiver atuando para um cliente da Iterative, deverão ser observadas prioritariamente as políticas, normas, contratos, procedimentos de segurança e diretrizes de Inteligência Artificial estabelecidas pelo cliente.

Nenhuma ferramenta de IA deverá ser utilizada em ambiente, código, documentação ou informação de cliente quando seu uso for proibido pelo cliente.

Quando o cliente determinar ferramentas específicas ou ambientes autorizados para utilização de IA, somente essas soluções deverão ser utilizadas.

Caso o cliente não possua política formal de IA ou existam dúvidas quanto à utilização de determinada ferramenta, o prestador deverá solicitar orientação ao responsável pelo projeto ou gestor da Iterative e do Cliente antes de utilizá-la com informações relacionadas ao cliente.

A ausência de uma proibição expressa não deverá ser interpretada automaticamente como autorização para compartilhar informações do cliente com serviços externos de IA.

4. ANUÊNCIA E TRANSPARÊNCIA COM O CLIENTE

A utilização relevante de Inteligência Artificial em projetos de clientes deverá ocorrer com conhecimento e anuência do cliente, respeitando o modelo de governança estabelecido em cada contrato ou projeto.

Especial atenção deverá ser dada quando a IA:

- tiver acesso a código-fonte;
- acessar repositórios;
- processar documentação interna;
- utilizar dados reais;
- acessar tickets, chamados ou backlog;
- conectar-se ao ambiente do cliente;
- consultar bancos de dados;
- utilizar APIs ou credenciais;
- executar ações automaticamente;
- produzir decisões ou recomendações relevantes;
- ou integrar-se diretamente aos sistemas corporativos.

5. PROTEÇÃO DAS INFORMAÇÕES DO CLIENTE

É expressamente proibido inserir em ferramentas de IA não autorizadas informações confidenciais ou restritas da Iterative ou de seus clientes.

Isso inclui, entre outros:

- código-fonte proprietário;
- credenciais;
- senhas;
- tokens;
- certificados;
- chaves de API;
- connection strings;

- dados de produção;
- informações pessoais;
- dados pessoais sensíveis;
- informações financeiras;
- documentos jurídicos;
- estratégias comerciais;
- arquitetura confidencial;
- diagramas internos;
- vulnerabilidades ainda não tratadas;
- informações sobre infraestrutura;
- dados de clientes ou usuários finais;
- bases de dados;
- contratos;
- documentos classificados como confidenciais;
- propriedade intelectual da Iterative ou do cliente.

Antes de fornecer qualquer informação para uma IA, o prestador deverá considerar:

"Eu estaria autorizado a enviar esta mesma informação para uma empresa externa?"

Se a resposta for negativa ou houver dúvida, a informação não deverá ser inserida na ferramenta.

6. DADOS DEVEM SER MINIMIZADOS

Sempre que possível, deverão ser utilizados exemplos fictícios, dados anonimizados, pseudonimizados ou informações estritamente necessárias para execução da atividade.

O prestador deverá evitar fornecer à IA um documento, banco de dados, código ou conjunto de informações maior do que o necessário.

O princípio deve ser:

fornecer à IA apenas o mínimo de informação necessário para realizar a atividade.

7. FERRAMENTAS DE IA

Ferramentas públicas ou contas pessoais não deverão ser utilizadas para processamento de informações confidenciais ou proprietárias de clientes.

Nos projetos em que o cliente disponibilizar ferramentas corporativas de IA, ambientes privados ou licenças específicas, estas deverão ser priorizadas e utilizadas de acordo com as políticas do cliente.

Antes da adoção corporativa de uma ferramenta de IA, deverão ser avaliados, conforme a criticidade do uso:

- política de privacidade;

- retenção de dados;
- utilização dos dados para treinamento;
- localização e processamento dos dados;
- mecanismos de segurança;
- autenticação e controle de acesso;
- integração com sistemas corporativos;
- logs e auditoria;
- possibilidade de exclusão dos dados;
- termos de propriedade intelectual;
- fornecedores e suboperadores;
- e requisitos contratuais do cliente.

8. IA COMO ACELERADOR, NÃO COMO SUBSTITUTO DA RESPONSABILIDADE PRESTADOR

Todo conteúdo produzido por Inteligência Artificial deverá ser tratado inicialmente como conteúdo não validado.

A responsabilidade pelo resultado final permanece com o prestador.

Portanto:

IA não substitui conhecimento técnico.

IA não substitui Code Review.

IA não substitui testes.

IA não substitui homologação.

IA não substitui revisão de segurança.

IA não substitui validação funcional.

IA não substitui aprovação humana quando necessária.

O argumento de que determinado código, documento, decisão ou informação "foi gerado pela IA" jamais elimina a responsabilidade prestador pela sua utilização.

9. DESENVOLVIMENTO DE SOFTWARE ASSISTIDO POR IA

A Iterative incentiva a utilização responsável de Inteligência Artificial como acelerador da engenharia de software.

A IA poderá apoiar atividades como geração de código, refatoração, criação de testes, documentação, análise de código, investigação de defeitos, elaboração de queries, prototipação e estudo de alternativas técnicas, desde que observadas as políticas do cliente e desta Política.

Todo código gerado ou modificado com auxílio de IA deverá passar pelos mesmos critérios de engenharia aplicáveis ao código produzido manualmente.

Deverão ser observados, conforme o projeto:

- padrões de arquitetura;
- padrões de desenvolvimento;
- testes automatizados;
- análise estática;
- revisão de código;
- segurança;
- performance;
- observabilidade;
- tratamento de erros;
- documentação;
- versionamento;
- critérios de aceite;
- homologação;
- e processos de CI/CD.

A velocidade proporcionada pela IA não poderá justificar redução dos controles de qualidade.

10. NÃO CONFIAR AUTOMATICAMENTE NAS RESPOSTAS DA IA

Modelos de IA podem gerar informações incorretas, incompletas, desatualizadas ou aparentemente corretas, mas tecnicamente inadequadas.

O prestador deverá validar informações relevantes antes de utilizá-las.

Especial atenção deverá ser aplicada a:

- bibliotecas sugeridas;
- versões;
- comandos;
- configurações de infraestrutura;
- queries;
- código relacionado à segurança;
- autenticação e autorização;
- criptografia;
- alterações de banco de dados;
- configurações de cloud;
- permissões;
- integrações;
- decisões arquiteturais;
- e recomendações que possam afetar ambientes produtivos.

Quanto maior o impacto potencial da ação, maior deverá ser o nível de validação humana.

11. SEGURANÇA ESPECÍFICA PARA SOLUÇÕES DE IA

Projetos envolvendo LLMs, RAG, agentes, MCPs, ferramentas externas ou automações baseadas em IA deverão considerar riscos específicos dessa tecnologia.

Entre eles:

- Prompt Injection;
- vazamento de informações;
- exposição indevida de contexto;
- acesso excessivo a ferramentas;
- execução indevida de comandos;
- permissões excessivas;
- manipulação de respostas;
- tratamento inadequado da saída do modelo;
- vulnerabilidades de integrações;
- dependência de modelos ou componentes externos;
- envenenamento de dados;
- utilização indevida de informações recuperadas;
- e ações autônomas não autorizadas.

As aplicações deverão ser desenvolvidas considerando princípios de segurança desde sua concepção.

12. AGENTES E AUTOMAÇÕES COM IA

Quanto maior a autonomia concedida a uma IA, maior deverá ser o controle aplicado.

Agentes capazes de executar ações deverão utilizar apenas as permissões estritamente necessárias.

Sempre que tecnicamente aplicável deverão existir:

- autenticação;
- autorização;
- segregação de funções;
- limitação de privilégios;
- logs;
- rastreabilidade;
- monitoramento;
- limites de execução;
- tratamento de exceções;
- possibilidade de interrupção;
- e aprovação humana para ações críticas.

A IA não deverá possuir autonomia irrestrita sobre ambientes críticos.

Ações relacionadas a produção, exclusão de dados, alterações de permissões, movimentações financeiras, segurança, publicação, alteração de infraestrutura ou outras atividades de alto impacto deverão possuir controles adicionais e, quando aplicável, aprovação humana.

13. HUMAN-IN-THE-LOOP

A Iterative adota o princípio de supervisão humana proporcional ao risco.

Quanto maior o impacto potencial de uma decisão ou ação executada com apoio de Inteligência Artificial, maior deverá ser a participação humana no processo.

Em atividades críticas, a IA deverá atuar prioritariamente como instrumento de apoio à análise e à decisão, e não como autoridade final independente.

14. PROPRIEDADE INTELECTUAL

Os prestadores deverão observar as condições de propriedade intelectual, licenciamento e utilização de conteúdos produzidos ou sugeridos por ferramentas de Inteligência Artificial.

Não deverá ser solicitado intencionalmente à IA que reproduza código, documentação ou material proprietário ao qual o prestador ou a Iterative não possua direito de utilização.

Código ou conteúdo gerado por IA deverá ser avaliado antes de sua incorporação a produtos ou projetos.

15. PROTEÇÃO DE DADOS E LGPD

Qualquer tratamento de dados pessoais utilizando Inteligência Artificial deverá observar a legislação aplicável, as políticas internas da Iterative, os contratos e as orientações do cliente.

Dados pessoais deverão ser utilizados somente quando necessários e autorizados para a finalidade pretendida.

Dados pessoais sensíveis exigem cautela adicional.

Sempre que possível, dados pessoais deverão ser removidos, anonimizados ou substituídos antes de utilização em ferramentas de IA.

16. DESENVOLVIMENTO DE SOLUÇÕES DE IA PARA CLIENTES

Projetos da Iterative que incluam Inteligência Artificial deverão considerar segurança e governança durante todo o ciclo de desenvolvimento.

Conforme a natureza e criticidade da solução, deverão ser avaliados:

Descoberta e planejamento

- objetivo da IA;
- benefício esperado;
- riscos;
- informações utilizadas;
- usuários impactados;
- necessidade de intervenção humana.

Arquitetura

- modelo utilizado;
- localização dos dados;
- integrações;
- autenticação;
- autorização;
- isolamento;
- logs;
- custos;
- disponibilidade;
- dependências externas.

Desenvolvimento

- segurança;
- controle de versões;
- qualidade;
- testes;
- proteção de prompts e configurações;
- tratamento seguro das respostas.

Validação

- precisão;
- segurança;
- comportamento inesperado;
- respostas inadequadas;
- possibilidade de vazamento;
- testes adversariais quando aplicável;
- critérios de aceite.

Produção

- monitoramento;
- logs;
- custos;

- performance;
- erros;
- comportamento do modelo;
- incidentes;
- atualização de modelos e dependências.

Evolução

- avaliação periódica;
- correção de vulnerabilidades;
- atualização de modelos;
- revisão de prompts;
- análise de qualidade;
- acompanhamento de riscos.

17. RASTREABILIDADE

Em soluções corporativas de IA, especialmente quando houver agentes ou execução automatizada, deverá existir rastreabilidade proporcional ao risco da solução.

Quando aplicável, deverão ser registradas informações como:

- usuário solicitante;
- agente ou modelo utilizado;
- data e horário;
- ação solicitada;
- sistemas acessados;
- ferramentas executadas;
- resultado da operação;
- erros;
- aprovações humanas;
- e ações realizadas.

Logs também deverão respeitar as regras de segurança e privacidade, não devendo se tornar um novo ponto de exposição de informações confidenciais.

18. INCIDENTES RELACIONADOS À IA

Qualquer suspeita de exposição indevida de informações, credenciais, dados pessoais, código-fonte ou informações confidenciais através de uma ferramenta de IA deverá ser tratada como potencial incidente de segurança.

O prestador deverá comunicar imediatamente pelos canais definidos pela Iterative e, quando aplicável, seguir o procedimento de segurança estabelecido pelo cliente.

O prestador não deverá tentar ocultar o ocorrido.

A comunicação rápida é fundamental para reduzir eventuais impactos.

Procedimento mínimo diante de possível incidente envolvendo IA:

• interromper imediatamente a atividade ou integração que possa ampliar a exposição;

• preservar evidências, registros e logs relevantes, evitando apagá-los ou alterá-los;

• comunicar imediatamente os canais de Segurança da Informação e o responsável pelo projeto;

• quando houver credencial potencialmente comprometida, seguir o processo de revogação ou rotação definido pela Iterative ou pelo cliente;

• não realizar comunicação externa ou ao cliente fora do fluxo corporativo de resposta a incidentes, salvo quando formalmente autorizado.

19. CAPACITAÇÃO

A Iterative entende que a utilização eficiente e segura de Inteligência Artificial depende de capacitação contínua.

Os prestadores deverão ser orientados e capacitados sobre:

- engenharia assistida por IA;
- segurança da informação;
- proteção de dados;
- elaboração adequada de prompts;
- validação das respostas;
- segurança de aplicações com IA;
- desenvolvimento com agentes;
- riscos de LLMs;
- propriedade intelectual;
- políticas dos clientes;
- e boas práticas de engenharia.

Programas como o Itera360 poderão incorporar esses princípios na formação e evolução dos prestadores.

20. USO RESPONSÁVEL PARA GANHO DE PRODUTIVIDADE

A Iterative incentiva seus prestadores a utilizar Inteligência Artificial para ampliar sua capacidade, produtividade e qualidade.

Entretanto, produtividade não deverá ser entendida apenas como quantidade de código ou velocidade de execução.

A utilização adequada de IA deverá buscar melhoria conjunta de:

Produtividade + Qualidade + Segurança + Assertividade + Conhecimento.

O ganho de velocidade não será considerado positivo quando resultar em aumento de defeitos, vulnerabilidades, retrabalho ou dívida técnica.

21. RESPONSABILIDADES DO PRESTADOR

Todo prestador da Iterative deverá:

1. conhecer as regras de IA aplicáveis ao cliente em que atua;
2. utilizar somente ferramentas permitidas;
3. proteger informações confidenciais;
4. não compartilhar credenciais ou dados restritos com IA;
5. minimizar os dados enviados;
6. revisar os resultados produzidos;
7. testar código gerado;
8. observar padrões técnicos do projeto;
9. comunicar incidentes;
10. solicitar orientação sempre que houver dúvida.

Em caso de dúvida sobre segurança ou autorização, o prestador deverá interromper o compartilhamento da informação e buscar orientação antes de prosseguir.

22. RESPONSABILIDADES DA LIDERANÇA

Gestores, Tech Leads e responsáveis pelos projetos deverão apoiar os prestadores na interpretação desta Política e das regras específicas dos clientes.

Também deverão promover o uso consciente da IA, evitando tanto sua utilização irresponsável quanto restrições desnecessárias que impeçam ganhos legítimos de produtividade e qualidade.

O objetivo da governança é permitir a inovação com segurança.

23. CONDUTAS NÃO PERMITIDAS

São consideradas incompatíveis com esta Política, entre outras:

- enviar código confidencial para IA pública sem autorização;
- fornecer senhas, tokens ou credenciais;
- inserir dados pessoais ou sensíveis sem necessidade e autorização;
- ignorar política de IA do cliente;
- utilizar ferramenta expressamente proibida pelo cliente;
- instalar extensões ou agentes não autorizados em ambientes corporativos;
- permitir acesso indiscriminado de agentes a sistemas;
- utilizar código gerado sem validação;
- colocar diretamente em produção uma alteração gerada por IA sem seguir o processo definido;
- ocultar a ocorrência de incidente;

- utilizar dados do cliente para treinamento de modelos sem autorização específica;
- contornar controles de segurança para permitir acesso de uma IA;
- utilizar IA para acessar informações às quais o próprio prestador não deveria ter acesso.

24. REGRA PRÁTICA ANTES DE UTILIZAR IA

Antes de fornecer informações relacionadas à Iterative ou a um cliente para uma Inteligência Artificial, todo prestador deverá fazer cinco perguntas:

1. **Posso usar IA nesta atividade?**
   A política do cliente permite?

2. **Posso utilizar esta ferramenta?**
   A ferramenta ou ambiente está autorizado?

3. **Posso enviar esta informação?**
   Existe código, dado pessoal, segredo, credencial ou informação confidencial?

4. **Consigo enviar menos informação?**
   Posso anonimizar, mascarar ou substituir dados reais?

5. **Quem validará o resultado?**
   Existe revisão humana adequada ao risco?

Se qualquer uma dessas respostas gerar dúvida, o prestador deverá consultar sua liderança antes de prosseguir.

25. RELAÇÃO COM OUTRAS POLÍTICAS

Esta Política deverá ser interpretada em conjunto com as demais normas e políticas corporativas da Iterative, especialmente:

- Política de Segurança da Informação;
- Política de Tratamento e Proteção de Dados Pessoais;
- Código de Ética e Conduta;
- Política Anticorrupção;
- compromissos de confidencialidade;
- contratos com clientes;
- políticas de desenvolvimento seguro;
- políticas e procedimentos específicos de cada cliente.

Em caso de divergência entre esta Política e uma regra mais restritiva estabelecida pelo cliente para seu ambiente ou suas informações, deverá ser observada a regra mais restritiva aplicável.

26. DESCUMPRIMENTO

O descumprimento desta Política poderá resultar na adoção das medidas administrativas, contratuais cabíveis, de acordo com a natureza e gravidade da ocorrência e com as demais políticas da Iterative.

27. GOVERNANÇA DE INTELIGÊNCIA ARTIFICIAL

A governança de IA da Iterative deverá assegurar que decisões sobre ferramentas, dados, integrações e soluções de IA tenham responsáveis definidos e sejam proporcionais ao risco.

Papéis mínimos:

• Responsável Corporativo pela Política de IA: mantém esta Política, coordena sua revisão e promove sua aplicação corporativa;

• Segurança da Informação: avalia riscos técnicos, acessos, integrações, incidentes e requisitos de segurança;

• Privacidade/DPO ou responsável equivalente: participa quando houver tratamento relevante de dados pessoais ou sensíveis;

• Responsável Iterative pelo cliente/projeto: confirma regras contratuais e diretrizes específicas do cliente;

• Tech Lead/Arquitetura: avalia impacto técnico, arquitetura, integrações, agentes e controles de engenharia;

• Prestador usuário: utiliza somente recursos autorizados, minimiza dados, valida resultados e comunica dúvidas ou incidentes.

As aprovações deverão ser proporcionais ao risco. Situações que envolvam dados confidenciais, produção, agentes com capacidade de ação, integrações corporativas ou decisões de alto impacto não deverão depender exclusivamente da decisão individual do usuário.

28. INVENTÁRIO E HOMOLOGAÇÃO DE FERRAMENTAS DE IA

A Iterative deverá manter, conforme aplicável, inventário das ferramentas de IA autorizadas para uso corporativo e/ou por projeto.

O inventário deverá registrar, quando pertinente: ferramenta e fornecedor; finalidade autorizada; projetos/clientes aplicáveis; tipos de informação permitidos; possibilidade de processamento de código; regras para dados pessoais; modalidade de conta/licença; retenção; utilização de dados para treinamento; integrações habilitadas; responsável pela aprovação; restrições; e data da última avaliação.

Ferramenta não constante do inventário ou não explicitamente autorizada deverá ser tratada como uso condicionado até sua avaliação, quando envolver informações, ativos ou ambientes da Iterative ou de clientes.

29. CLASSIFICAÇÃO DA INFORMAÇÃO PARA USO COM IA

Para decisões de uso de IA, as informações deverão observar a classificação adotada pela Iterative e/ou pelo cliente. Como referência operacional, deverão ser consideradas as categorias Público, Interno, Confidencial e Restrito, quando compatíveis com a política aplicável.

• Público: informação cuja divulgação é autorizada; pode ser utilizada em ferramentas permitidas, observadas propriedade intelectual e finalidade.

• Interno: informação destinada ao uso interno; utilizar apenas em ambientes corporativos autorizados.

• Confidencial: código proprietário, arquitetura, contratos, estratégias, dados de clientes e informações equivalentes; somente em ferramentas e finalidades explicitamente autorizadas.

• Restrito: credenciais, chaves privadas, senhas, tokens, secrets, certificados privados, dados pessoais sensíveis de alta criticidade e demais informações cuja exposição possa causar impacto relevante. Credenciais, segredos de autenticação e chaves privadas nunca deverão ser inseridos em ferramentas de IA. As demais informações classificadas como Restritas somente poderão ser processadas em solução especificamente autorizada para essa finalidade, mediante controles técnicos e aprovação formal aplicáveis.

A classificação mais restritiva estabelecida pelo cliente prevalece.

30. CADEIA DE SUPRIMENTOS DE IA (AI SUPPLY CHAIN)

Modelos, datasets, bibliotecas, embeddings, MCP Servers, plugins, extensões, agentes, frameworks e demais componentes de terceiros utilizados em soluções de IA deverão ter seus riscos avaliados de forma proporcional à criticidade.

A avaliação deverá considerar, quando aplicável: origem e reputação; licença; integridade e autenticidade; vulnerabilidades conhecidas; manutenção e atualizações; permissões solicitadas; dependências; procedência de modelos e datasets; possibilidade de código malicioso; privacidade; telemetria; e impacto de eventual comprometimento do fornecedor.

Componentes não confiáveis ou de procedência desconhecida não deverão ser incorporados a soluções corporativas ou de clientes sem avaliação e autorização.

31. CICLO DE DESENVOLVIMENTO SEGURO DE IA (AI SECURE SDLC)

Para soluções de IA desenvolvidas para clientes ou para uso interno, os controles previstos nesta Política deverão ser incorporados ao ciclo de desenvolvimento e não tratados apenas ao final do projeto.

Conforme risco e criticidade, deverão existir gates de validação:

• Gate 1 - Descoberta: finalidade, benefício, dados, usuários impactados, riscos e necessidade de supervisão humana;

• Gate 2 - Arquitetura: modelo, fornecedores, integrações, localização dos dados, autenticação, autorização, isolamento, custos e dependências;

• Gate 3 - Desenvolvimento: desenvolvimento seguro, proteção de prompts/configurações, controle de versões, tratamento seguro de saídas e revisão de componentes;

• Gate 4- Validação: qualidade, precisão, segurança, prompt injection direta e indireta, vazamento, comportamento inesperado, testes adversariais quando aplicável e critérios de aceite;

• Gate 5 - Produção: aprovação para implantação, monitoramento, logs, limites, rollback/interrupção, custos, performance e resposta a incidentes;

• Gate 6 - Evolução: reavaliação periódica de modelos, prompts, dependências, vulnerabilidades, qualidade e riscos.

Em soluções com RAG, agentes, MCPs ou conteúdo externo, deverá ser considerada a possibilidade de prompt injection indireta: instruções maliciosas presentes em documentos, páginas, e-mails, repositórios ou outras fontes podem ser interpretadas pelo modelo como comandos. Conteúdo recuperado deve ser tratado como dado não confiável e não como instrução autorizada.

32. MATRIZ DE USO DE INTELIGENCIA ARTIFICIAL

Esta Matriz estabelece critérios práticos para orientar os prestadores da Iterative sobre situações de uso de Inteligência Artificial durante suas atividades prestadores.

🟢 **VERDE — USO PERMITIDO:** A atividade pode ser realizada, desde que sejam observadas as políticas do cliente, da Iterative e as boas práticas estabelecidas. REGRA: Pode utilizar.

🟡 **AMARELO — USO CONDICIONADO / REQUER VALIDAÇÃO:** Existe algum risco relacionado a informações, integração, autonomia, segurança, propriedade intelectual ou impacto da atividade.

A utilização deverá ocorrer somente após confirmação de que a ferramenta, informação e finalidade estão autorizadas.

Dependendo da situação, deverá haver validação do Tech Lead, Gestor, Segurança da Informação, responsável Iterative pelo cliente ou do próprio cliente.

REGRA: Na dúvida, não execute antes de validar.

🔴 **VERMELHO — USO PROIBIDO:** A atividade representa risco incompatível com as políticas da Iterative ou viola regras de segurança, confidencialidade, proteção de dados ou determinações do cliente.

REGRA: Não executar.

Situação	Classificação	Orientação
Utilizar IA para explicar um conceito técnico genérico	🟢 VERDE	Permitido
Pesquisar documentação pública de tecnologia	🟢 VERDE	Permitido
Pedir exemplos genéricos de código	🟢 VERDE	Permitido
Criar código sem utilizar informações do cliente	🟢 VERDE	Permitido
Criar testes utilizando exemplos fictícios	🟢 VERDE	Permitido
Criar documentação utilizando informações públicas	🟢 VERDE	Permitido
Brainstorming de alternativas técnicas sem informações confidenciais	🟢 VERDE	Permitido
Utilizar IA para aprender uma nova tecnologia	🟢 VERDE	Permitido

Criar massa de dados totalmente fictícia	🟢 VERDE	Permitido
Criar histórias de usuário utilizando cenário fictício	🟢 VERDE	Permitido
Criar diagramas genéricos de arquitetura	🟢 VERDE	Permitido
Revisar texto sem informações confidenciais	🟢 VERDE	Permitido
Criar documentação técnica genérica	🟢 VERDE	Permitido
Utilizar IA corporativa oficialmente disponibilizada pelo cliente	🟢 VERDE*	Permitido dentro das regras definidas pelo cliente
Utilizar IA para código real do cliente em ferramenta explicitamente homologada para isso	🟢 VERDE*	Permitido respeitando escopo e regras da ferramenta
Utilizar IA para gerar testes sobre código autorizado	🟢 VERDE*	Permitido, mantendo revisão humana
Analisar código-fonte do cliente	🟡 AMARELO	Somente em ferramenta e contexto autorizados
Enviar trecho de código real para uma IA	🟡 AMARELO	Confirmar autorização e classificação da informação
Utilizar documentação interna do cliente	🟡 AMARELO	Somente em ambiente autorizado
Utilizar backlog, Jira ou chamados do cliente	🟡 AMARELO	Avaliar conteúdo e autorização
Conectar IA ao Git/GitHub/GitLab/Azure DevOps do cliente	🟡 AMARELO	Requer autorização e controle de acesso
Utilizar IA para análise de pull requests	🟡 AMARELO	Somente com ferramenta aprovada
Criar RAG utilizando documentos do cliente	🟡 AMARELO	Exige avaliação de arquitetura, segurança e autorização
Utilizar IA para analisar logs	🟡 AMARELO	Verificar presença de dados pessoais, credenciais ou informações confidenciais
Utilizar IA para analisar banco de dados	🟡 AMARELO	Requer autorização e controles de segurança
Utilizar dados reais de produção	🟡 AMARELO	Excepcional; exige autorização específica e controles adequados
Criar agente que consulte sistemas internos	🟡 AMARELO	Requer avaliação de segurança e permissões
Criar agente que execute ações automaticamente	🟡 AMARELO	Exige governança, limites, logs e aprovação conforme criticidade

Integrar IA com APIs do cliente	🟡 AMARELO	Avaliar autenticação, autorização e dados processados
Utilizar IA para criar scripts de infraestrutura	🟡 AMARELO	Código deve ser revisado e testado antes da execução
Utilizar IA para alterações de banco de dados	🟡 AMARELO	Requer revisão técnica antes da execução
Utilizar IA para configuração de Cloud	🟡 AMARELO	Requer revisão antes da execução
Utilizar IA para identificar vulnerabilidades	🟡 AMARELO	Utilizar somente em ambientes e escopos autorizados
Utilizar nova ferramenta de IA não homologada	🟡 AMARELO	Consultar responsável antes da utilização com informações corporativas
Utilizar plugin/extensão de IA no IDE	🟡 AMARELO	Verificar se ferramenta e envio de código são autorizados
Utilizar MCP ou integração equivalente	🟡 AMARELO	Avaliar dados, ferramentas, permissões e autonomia concedida
Utilizar IA para tomar decisão de alto impacto sem revisão humana	🔴 VERMELHO	Proibido
Inserir senha em ferramenta de IA	🔴 VERMELHO	Proibido
Inserir token de acesso	🔴 VERMELHO	Proibido
Inserir chave de API	🔴 VERMELHO	Proibido
Inserir certificado ou chave privada	🔴 VERMELHO	Proibido
Inserir connection string contendo credenciais	🔴 VERMELHO	Proibido
Enviar código confidencial para IA pública/não autorizada	🔴 VERMELHO	Proibido
Enviar base de dados do cliente para ferramenta não autorizada	🔴 VERMELHO	Proibido
Enviar dados pessoais/sensíveis sem autorização e necessidade	🔴 VERMELHO	Proibido
Utilizar IA expressamente proibida pelo cliente	🔴 VERMELHO	Proibido
Contornar bloqueios do cliente para utilizar IA	🔴 VERMELHO	Proibido
Copiar código completo de repositório do cliente para IA pública	🔴 VERMELHO	Proibido
Fornecer informações comerciais confidenciais do cliente	🔴 VERMELHO	Proibido
Solicitar que IA execute comandos diretamente em produção sem controles adequados	🔴 VERMELHO	Proibido

Dar acesso administrativo irrestrito a um agente de IA	🔴 VERMELHO	Proibido
Permitir que agente exclua dados de produção sem aprovação/controles	🔴 VERMELHO	Proibido
Utilizar informações de um cliente para solucionar problema de outro cliente	🔴 VERMELHO	Proibido
Utilizar dados do cliente para treinamento de modelo sem autorização específica	🔴 VERMELHO	Proibido
Ocultar incidente envolvendo IA	🔴 VERMELHO	Proibido

*** Importante:** mesmo uma atividade classificada como VERDE depende de estar de acordo com as regras específicas do cliente.

33. PRINCÍPIO FINAL

A Iterative acredita que a Inteligência Artificial deve ampliar a capacidade de seus prestadores, e não substituir responsabilidade, conhecimento ou julgamento prestador.

Por isso, todo uso de IA na Iterative deverá observar quatro compromissos fundamentais:

- INOVAR COM IA.
- PROTEGER AS INFORMAÇÕES.
- RESPEITAR AS REGRAS DO CLIENTE.
- MANTER O HUMANO RESPONSÁVEL PELO RESULTADO.

A tecnologia pode acelerar o trabalho.

A responsabilidade continua sendo nossa.