omnisblue
LGPD | COMPLIANCE

Política de Governança e Uso Responsável de Inteligência Artificial

1. Objetivo

Esta Política estabelece as regras, limites, responsabilidades e padrões mínimos para o uso de Inteligência Artificial (IA) pela Omnisblue, seus colaboradores, fornecedores autorizados, clientes e usuários das soluções disponibilizadas pela empresa.

O objetivo é garantir que o uso de IA ocorra de forma ética, segura, responsável, supervisionada e alinhada aos compromissos da Omnisblue com integridade corporativa, privacidade, proteção de dados, segurança da informação, qualidade técnica e desenvolvimento seguro de software.

Esta Política se aplica tanto ao uso de IA como ferramenta de produtividade no dia a dia dos colaboradores quanto ao uso de IA como parte das soluções tecnológicas, plataformas, agentes inteligentes e aplicações disponibilizadas pela Omnisblue, e está alinhada ao modelo interno de governança tecnológica da Omnisblue, especialmente ao Guia de Premissas e Padrões de Desenvolvimento de Software, que define critérios mínimos de qualidade, premissas e restrições aplicáveis a equipes internas e externas de desenvolvimento de software a serviço da empresa.

2. Glossário

Para fins desta Política, devem ser consideradas as seguintes definições:

- **Agente de IA**: aplicação, componente ou funcionalidade baseada em IA configurada para executar tarefas específicas, interagir com usuários, analisar informações, sugerir encaminhamentos ou apoiar processos dentro ou fora das soluções da Omnisblue.
- **Alucinação**: geração de resposta incorreta, imprecisa, inventada ou não verificável por um sistema de IA, ainda que apresentada de forma aparentemente convincente.
- **Dados de cliente**: informações, documentos, bases, registros, evidências, relatórios, interações, arquivos, dados pessoais ou dados corporativos fornecidos por clientes ou gerados em razão do uso das soluções Omnisblue.
- **Dados pessoais**: informações relacionadas a pessoa natural identificada ou identificável.
- **Dados pessoais sensíveis**: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dado referente à saúde, vida sexual, dado genético ou biométrico, conforme legislação aplicável.
- **IA generativa**: tipo de IA capaz de gerar textos, imagens, códigos, resumos, documentos, apresentações, respostas, análises ou outros conteúdos a partir de comandos, instruções ou dados fornecidos por usuários ou sistemas.
- **Inteligência Artificial ou IA**: conjunto de tecnologias, modelos, sistemas ou aplicações capazes de executar tarefas que normalmente demandariam algum grau de raciocínio, classificação, geração de conteúdo, previsão, automação, análise contextual ou interação com linguagem natural.
- **Intervenção humana**: revisão, validação, aprovação, ajuste ou decisão realizada por pessoa autorizada, não podendo ser substituída integralmente pela IA nos cenários definidos por esta Política.
- **Modelo de IA**: estrutura técnica treinada ou configurada para processar informações e produzir respostas, classificações, recomendações, previsões ou conteúdos.
- **Prompt**: comando, pergunta, instrução, texto ou conjunto de informações fornecidas a uma ferramenta ou agente de IA para orientar a produção de uma resposta ou resultado.

- **Prompt injection**: tentativa de manipular um sistema de IA por meio de comandos, instruções ou conteúdos maliciosos capazes de alterar sua finalidade, burlar restrições, expor informações ou gerar respostas indevidas.
- **Shadow IA**: uso de ferramenta, aplicação, modelo, agente ou plataforma de IA sem aprovação formal do Comitê de Segurança e Privacidade (CSP) da Omnisblue.
- **Treinamento de modelo**: processo pelo qual informações são utilizadas para ajustar, melhorar, aperfeiçoar ou alimentar modelos de IA.

3. Escopo

Esta Política se aplica a:

a. todos os colaboradores, sócios, gestores, estagiários, prestadores de serviço e terceiros autorizados que atuem em nome da Omnisblue;
b. todos os clientes e usuários que utilizem soluções, plataformas, agentes ou funcionalidades com IA disponibilizadas pela Omnisblue;
c. todos os usos de IA realizados em atividades internas, projetos, entregáveis, desenvolvimento de software, análise de documentos, atendimento, suporte, auditorias, diagnósticos, geração de código, análise de riscos, privacidade, compliance e demais atividades corporativas;
d. todas as ferramentas, modelos, plataformas, agentes e soluções de IA utilizados pela Omnisblue, sejam próprios, de terceiros, via API, embarcados em nuvem, integrados à plataforma Omnisblue ou utilizados como apoio operacional.

4. Princípios gerais de uso responsável de IA

O uso de IA pela Omnisblue deve observar, obrigatoriamente, os seguintes princípios:

✓ **Finalidade legítima:** a IA somente poderá ser utilizada para atividades relacionadas ao contexto da Omnisblue, suas operações, seus produtos, seus serviços, seus clientes e suas aplicações.

- ✓ **Proibição de uso externo para treinamento:** em nenhuma hipótese informações fornecidas pela Omnisblue, seus colaboradores, clientes ou usuários poderão ser utilizadas para treinamento de modelos externos de IA.
- ✓ **Aprovação prévia (proibição de *shadow IA*):** somente ferramentas, plataformas, modelos ou agentes previamente aprovados pelo Comitê de Segurança e Privacidade (CSP) poderão ser utilizados.
- ✓ **Supervisão e responsabilidade humana**: os resultados gerados por IA devem ser tratados como sugestões, insumos ou apoio à execução de atividades, nunca como decisão final automática. O colaborador, analista, desenvolvedor, gestor ou usuário responsável pela atividade permanece integralmente responsável pela análise, validação e uso do resultado produzido com apoio de IA.
- ✓ **Proteção de dados pessoais:** dados pessoais somente poderão ser tratados por IA mediante uso de agentes de IA formalmente aprovados e configurados para essa finalidade, nunca por meio de prompts inseridos livremente em ferramentas de IA. Além disso, eventuais tratamentos de dados pessoais pela IA devem ainda estrita compatibilidade com a *Política de Privacidade* da Omnisblue.
- ✓ **Transparência adequada:** quando aplicável, clientes e usuários devem ser informados sobre o uso de IA em soluções, agentes ou funcionalidades disponibilizadas pela Omnisblue.
- ✓ **Rastreabilidade e auditoria:** usos relevantes de IA em soluções da Omnisblue devem contar com registros, logs, trilhas de auditoria e controles compatíveis com a finalidade do agente ou funcionalidade.

5. Regras gerais aplicáveis a todos os usos de IA

Todo uso de IA pela Omnisblue deve obedecer às seguintes regras gerais:

a) Colaboradores que desejarem usar uma ferramenta, modelo ou plataforma de IA devem consultar seu líder imediato ou o Comitê de Segurança e Privacidade (CSP) para confirmar se a solução está autorizada;
b) Uma ferramenta de IA somente será considerada permitida após aprovação formal do Comitê de Segurança e Privacidade (CSP).

c) As ferramentas atualmente utilizadas pela Omnisblue incluem ChatGPT, Gemini, Gamma.app e Claude, sem prejuízo de outras que venham a ser aprovadas formalmente conforme necessidade da empresa.
d) É proibido configurar ferramentas, plataformas, modelos ou agentes de IA de forma que informações da Omnisblue, de seus colaboradores, clientes ou usuários sejam utilizadas para treinamento externo.
e) Dados pessoais não podem ser inseridos em prompts de ferramentas de IA.
f) Dados pessoais somente podem ser tratados com IA por meio de agentes formalmente aprovados, parametrizados e controlados pela Omnisblue.
g) Especialmente os dados de clientes, documentos de clientes, informações de denúncias, evidências de auditoria, registros de compliance, códigos-fonte proprietários, credenciais, chaves de API, tokens, logs de segurança, estruturas de banco de dados, informações contratuais e segredos comerciais não podem ser inseridos, em nenhuma hipótese, em ferramentas públicas ou não homologadas de IA.
h) Todo resultado produzido por IA deve ser revisado por pessoa responsável antes de ser utilizado em decisões, documentos, entregáveis, comunicações externas, códigos-fonte, análises técnicas ou relatórios enviados a clientes.
i) A IA não deve ser tratada como colaborador, analista, auditor, investigador, DPO, desenvolvedor autônomo, gestor ou decisor. A IA é ferramenta de apoio.
j) Violações a esta Política poderão gerar medidas corretivas, disciplinares, contratuais ou legais, conforme gravidade do caso.

6. Uso de IA como ferramenta de produtividade

A Omnisblue permite o uso de ferramentas de IA aprovadas para apoiar atividades de produtividade, desde que observadas as regras desta Política.

São usos permitidos, desde que realizados em plataformas aprovadas:

a) produção, análise e revisão de textos;
b) apoio à elaboração de documentos e relatórios;
c) revisão ortográfica, gramatical, estrutural e argumentativa;
d) apoio à criação de atas de reunião;

e) transcrição de reuniões online via Microsoft Teams;
f) apoio a pesquisas e organização de ideias;
g) geração de apresentações;
h) apoio à criação, revisão, explicação e validação inicial de código-fonte;
i) apoio à criação de casos de teste;
j) apoio à estruturação de planos, checklists, cronogramas e materiais de treinamento.

O uso de IA em produtividade deve respeitar os seguintes limites:

a) o conteúdo gerado pela IA deve ser tratado como sugestão;
b) o colaborador responsável deve revisar, ajustar, validar e assumir responsabilidade pelo resultado produzido;
c) entregáveis para clientes não podem ser enviados sem revisão humana;
d) relatórios, pareceres, diagnósticos, análises de compliance, materiais de auditoria e documentos técnicos não podem ser emitidos apenas com base em resultado de IA;
e) dados pessoais não devem ser inseridos em prompts, mesmo para fins de produtividade;
f) dados confidenciais ou de clientes não devem ser inseridos em ferramentas não homologadas ou fora das condições aprovadas pelo Comitê de Segurança e Privacidade (CSP).

Exemplo prático: um analista pode usar IA para estruturar a primeira versão de um relatório de auditoria de compliance, organizar tópicos e melhorar a clareza textual. Porém, a avaliação dos achados, a classificação das não conformidades, a conclusão técnica e a recomendação final devem ser realizadas e validadas pelo próprio analista responsável.

7. Uso de IA no desenvolvimento de software

O uso de IA em desenvolvimento de software é permitido como ferramenta de apoio técnico, desde que limitado às plataformas aprovadas e respeitados os padrões de desenvolvimento seguro da Omnisblue.

A IA poderá apoiar atividades como:

a) análise de requisitos;
b) interpretação de regras de negócio;
c) produção de código-fonte;
d) revisão e refatoração de código;
e) identificação de erros lógicos ou técnicos;
f) criação de casos de teste;
g) automação de testes unitários e funcionais;
h) apoio à documentação técnica;
i) apoio à criação e parametrização de agentes de IA.

É proibido inserir em ferramentas de IA não homologadas:

a) código-fonte proprietário da Omnisblue ou de clientes;
b) credenciais, senhas, tokens ou chaves de API;
c) estruturas completas de banco de dados;
d) logs de produção ou homologação com informações sensíveis;
e) vulnerabilidades conhecidas ainda não corrigidas;
f) informações de arquitetura sensível;
g) documentos técnicos de clientes;
h) dados pessoais ou dados confidenciais.

Todo código, teste, componente ou artefato técnico produzido com apoio de IA deverá passar por revisão técnica, testes funcionais, testes de segurança e homologação antes de ser incorporado a produtos, serviços ou soluções da Omnisblue.

O desenvolvimento somente será considerado concluído após liberação pelo time responsável pela homologação e autorização para *deployment*, preservando o padrão já definido no processo de engenharia de software da Omnisblue, e em conformidade com o *Padrão de Desenvolvimento Seguro* da empresa.

8. Uso de IA como parte das soluções da Omnisblue

A Omnisblue poderá incorporar IA em suas soluções, plataformas, produtos e aplicações, especialmente por meio de agentes inteligentes.

Os agentes de IA da Omnisblue poderão ser utilizados para:

a) atendimento a usuários dentro e fora da plataforma Omnisblue;
b) apoio à análise de documentos cadastrados na plataforma;
c) análise e cruzamento de informações registradas na plataforma;
d) análise e sugestão de riscos;
e) sugestão de atividades de mitigação de riscos;
f) apoio à interpretação de informações fornecidas por usuários;
g) apoio à organização de dados, documentos e registros relacionados às soluções contratadas.

Os agentes de IA da Omnisblue deverão observar, além dos princípios já definidos nesta Política, os seguintes requisitos mínimos:

a) base de conhecimento controlada;
b) limites de atuação documentados;
c) parametrização realizada pela Omnisblue;
d) segregação de dados por cliente;
e) monitoramento periódico;
f) possibilidade de intervenção humana;
g) respostas apresentadas como sugestões, e não como decisões finais;
h) testes prévios antes da entrada em produção;
i) aprovação do responsável pelo produto;
j) aprovação obrigatória do DPO quando houver tratamento de dados pessoais.

Os agentes de IA nunca poderão tomar decisões finais automáticas em nome da Omnisblue, de seus clientes ou usuários. Suas respostas devem deixar claro que se trata de sugestões, cabendo ao usuário avaliar, aceitar, rejeitar ou ajustar o resultado apresentado.

Exemplo prático: um agente pode sugerir riscos relacionados a um processo de tratamento de dados pessoais descrito na plataforma, bem como sugerir medidas de mitigação. Porém, a decisão sobre aceitar o risco, alterar o controle, aprovar o plano de ação ou registrar a conclusão final caberá sempre ao usuário responsável.

9. Decisões que não podem ser tomadas exclusivamente por IA

É proibido que agentes, modelos ou ferramentas de IA tomem decisões finais ou automáticas sobre:

a) classificação definitiva de bases legais de tratamento de dados pessoais;
b) resultado de investigação de denúncias;
c) resultado de processos de ouvidoria;
d) autorização ou decisão final sobre compartilhamento de dados pessoais;
e) reprovação de processos de *due diligence*;
f) aplicação de sanções disciplinares;
g) conclusões finais de auditorias, investigações, diagnósticos ou avaliações de conformidade;
h) decisões que gerem impacto jurídico, contratual, reputacional, financeiro ou regulatório relevante para a Omnisblue, seus clientes ou titulares de dados.

Nesses casos, a IA poderá apenas apoiar a análise, organizar informações, sugerir caminhos ou apontar inconsistências, sempre com revisão e decisão humana.

10. Governança das informações de clientes em agentes de IA

As informações fornecidas por clientes aos agentes de IA da Omnisblue serão tratadas exclusivamente para as finalidades contratadas e dentro do ambiente da plataforma ou solução correspondente.

A Omnisblue adota as seguintes regras de governança para dados de clientes em agentes de IA:

a) dados de clientes nunca serão utilizados para treinamento de modelos externos, em nenhuma hipótese;

b) cada cliente possui base de dados segregada;
c) as informações tratadas ou produzidas por agentes permanecem associadas à base segregada do respectivo cliente;
d) agentes de IA são parametrizados pela Omnisblue;
e) informações inseridas por clientes serão utilizadas apenas dentro da finalidade da solução contratada;
f) logs e registros de interação poderão ser mantidos conforme configurações da própria plataforma;
g) as configurações de retenção poderão ser ajustadas pelos usuários conforme recursos disponíveis na plataforma;
h) clientes e usuários serão informados sobre o uso de IA por meio de termos de uso, documentos contratuais, políticas específicas ou documentos equivalentes.

11. Testes, segurança e homologação de soluções com IA

Toda solução, funcionalidade ou agente com IA deverá passar por testes antes da entrada em produção.

Os testes deverão considerar, no mínimo:

a) funcionamento esperado;
b) aderência à finalidade do agente;
c) segurança da informação;
d) proteção de dados pessoais, quando aplicável;
e) risco de alucinação;
f) risco de vazamento de dados;
g) risco de prompt injection;
h) risco de respostas enviesadas;
i) uso indevido por usuários;
j) consistência das respostas.

A entrada em produção de uma solução com IA dependerá de aprovação do responsável pelo produto.

Quando houver tratamento de dados pessoais, a aprovação do DPO será também obrigatória.

O Comitê de Segurança e Privacidade (CSP) poderá ser consultado em casos específicos, especialmente quando houver risco elevado, dúvida sobre finalidade, uso de novas tecnologias, integração com terceiros, impacto relevante a clientes ou tratamento de informações sensíveis.

12. Responsabilidades

12.1 Comitê de Segurança e Privacidade (CSP)

Compete ao CSP:

a) aprovar ferramentas, modelos e plataformas de IA;
b) manter ou orientar a manutenção da lista de soluções de IA permitidas;
c) avaliar solicitações de uso de novas ferramentas;
d) deliberar sobre exceções;
e) apoiar análises de risco envolvendo IA;
f) orientar colaboradores e gestores sobre uso seguro e responsável de IA;
g) avaliar casos de possível *shadow IA*;
h) apoiar e aprovar a revisão periódica desta Política.

12.2 DPO

Compete ao DPO, além de suas atribuições padrão:

a) avaliar usos de IA que envolvam tratamento de dados pessoais;
b) aprovar soluções com IA que tratem dados pessoais antes da entrada em produção;
c) orientar sobre riscos de privacidade e proteção de dados;
d) avaliar a necessidade de documentos, registros ou análises específicas de privacidade;
e) apoiar o tratamento de incidentes ou não conformidades envolvendo dados pessoais e IA.

12.3 Gerente do Produto

Compete ao Gerente do Produto:

a) aprovar a entrada em produção de agentes ou funcionalidades com IA associados aos produtos de software sob sua gestão;
b) garantir que a finalidade desses agentes esteja claramente definida;
c) assegurar que esses agentes estejam parametrizados conforme regras desta Política;
d) garantir que testes e homologações sejam realizados;
e) avaliar riscos funcionais, técnicos e de negócio;
f) garantir que os agentes apresentem suas respostas como sugestões;
g) acionar o DPO quando houver tratamento de dados pessoais associados ao uso da IA;
h) acionar o Comitê quando houver dúvidas ou riscos relevantes sobre o uso da IA em seus produtos.

12.4 Colaboradores Omnisblue

Compete aos colaboradores:

a) tomar conhecimento de todas as regras definidas nesta Política;
b) utilizar apenas ferramentas de IA aprovadas;
c) não utilizar *shadow IA*;
d) não inserir dados pessoais em prompts;
e) não inserir informações confidenciais, técnicas, estratégicas ou de clientes em plataformas não autorizadas;
f) revisar todos os resultados gerados por IA antes de utilizá-los;
g) assumir responsabilidade pelo conteúdo final produzido com apoio de IA;
h) consultar o líder imediato ou o Comitê em caso de dúvida;
i) reportar usos indevidos, suspeitas de vazamento, incidentes ou descumprimentos desta Política.

12.5 Clientes e usuários

Compete aos clientes e usuários:

a) tomar ciência desta Política e as regras aqui definidas;
b) utilizar agentes e funcionalidades de IA conforme os termos de uso e orientações da Omnisblue;
c) compreender que respostas de agentes são sugestões e não decisões finais;
d) avaliar criticamente os resultados produzidos por agentes;
e) manter responsabilidade pelas decisões tomadas a partir das sugestões apresentadas;
f) observar configurações disponíveis na plataforma, inclusive quanto à retenção de registros e interações;
g) não tentar manipular, burlar, explorar ou utilizar agentes fora de sua finalidade.

13. Treinamento e conscientização

A Omnisblue deverá promover treinamentos e ações de conscientização sobre uso responsável de IA.

Os treinamentos poderão ser segmentados por público, incluindo:

a) colaboradores em geral;
b) analistas;
c) desenvolvedores;
d) gestores;
e) time de produto;
f) DPO e responsáveis por privacidade;
g) usuários de agentes incorporados às soluções Omnisblue, quando aplicável.

Os treinamentos deverão reforçar todos os parâmetros detalhados nesta Política e, em especial, que IA é ferramenta de apoio, e não substitui julgamento profissional, responsabilidade técnica, revisão humana, governança, privacidade, segurança da informação ou tomada de decisão autorizada.

14. Violações e consequências

O descumprimento desta Política poderá resultar em medidas corretivas, disciplinares, contratuais ou legais, conforme o vínculo da pessoa envolvida, a gravidade da conduta, o risco gerado e os impactos causados.

São exemplos de violações:

a) uso de ferramenta de IA não aprovada;
b) inserção de dados pessoais em prompts;
c) inserção de informações de clientes em ferramentas não autorizadas;
d) configuração de ferramenta de IA permitindo treinamento externo com dados da Omnisblue ou de clientes;
e) uso de IA para decisões proibidas por esta Política;
f) envio de entregável gerado por IA sem revisão humana;
g) uso de IA para finalidade pessoal, ilícita, antiética ou incompatível com os interesses da Omnisblue;
h) tentativa de burlar controles, logs, segregação de dados ou limitações de agentes.

As medidas aplicáveis poderão incluir orientação, treinamento adicional, bloqueio de acesso, revisão de permissões, advertência, medidas disciplinares, rescisão contratual, comunicação a clientes, apuração interna, comunicação a autoridades competentes ou adoção de medidas judiciais, quando cabível.

15. Exceções

Qualquer exceção às regras desta Política deverá ser previamente justificada, documentada e aprovada pelo Comitê de Segurança e Privacidade (CSP).

Quando a exceção envolver tratamento de dados pessoais, o DPO deverá ser obrigatoriamente envolvido.

Nenhuma exceção poderá autorizar:

a) uso de dados da Omnisblue, clientes ou usuários para treinamento de modelos externos;
b) uso de *shadow IA*;
c) tratamento de dados pessoais em prompts livres;
d) eliminação da revisão humana em decisões críticas;
e) violação de lei, contrato, obrigação regulatória ou compromisso assumido com clientes.

16. Disposições gerais

Esta Política integra os programas de Governança de Integridade, Governança de Privacidade, Segurança da Informação e o Guia de Premissas e Padrões de Desenvolvimento Seguro de Software da Omnisblue.

A Omnisblue poderá revisar esta Política periodicamente para refletir mudanças tecnológicas, legais, regulatórias, contratuais, operacionais ou estratégicas.

Casos omissos deverão ser submetidos ao Comitê de Segurança e Privacidade (CSP), ao DPO ou à Gerência de Produto, conforme a natureza do tema.

Novas versões desta Política passam a ser vigentes apenas após aprovação formal do Comitê de Segurança e Privacidade (CSP) e distribuição.

Versão: 1.1
Última atualização e início de vigência desta política: 27 de maio de 2026