

KHAL

TRUST CENTER

Segurança e suporte no nível da sua operação.

Como a KHAL protege os dados dos seus clientes, controla o que a IA pode fazer, mantém a plataforma no ar e responde quando algo sai do normal. Tudo o que um time de compras, segurança ou jurídico precisa para homologar a KHAL, em uma página.

98,7%

disponibilidade
mensal padrão

1h

primeira resposta
em incidente
crítico, 24/7

100%

dados
armazenados na
AWS São Paulo

48h

prazo máximo para
avisar incidente
com dado pessoal

Atualizado em outubro de 2026

O essencial em uma tabela

As respostas que todo questionário de fornecedor pede primeiro. O detalhe de cada linha está nas seções abaixo.

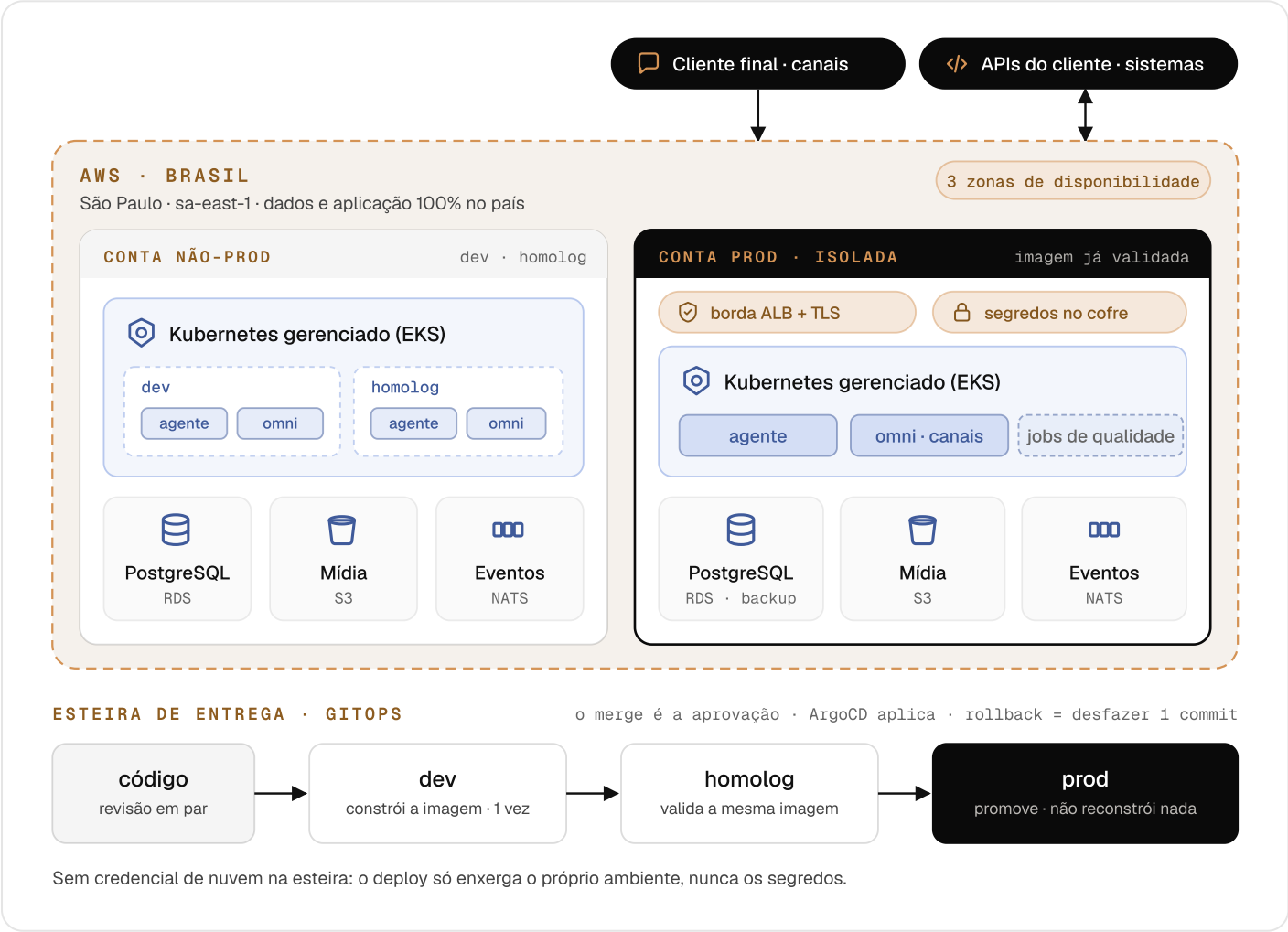
TEMA	COMO A KHAL ATENDE
Hospedagem	AWS, região São Paulo (sa-east-1), em 3 zonas de disponibilidade. Dados armazenados no Brasil.
Isolamento	Produção em conta AWS separada de desenvolvimento e homologação. Opção de rodar dentro da infraestrutura do cliente.
Criptografia	TLS 1.2 ou superior em trânsito, AES-256 em repouso, segredos em cofre.
Acesso	SSO (SAML 2.0 e OIDC), MFA obrigatório, perfis por função e revisão periódica de acessos.
Dados e IA	O agente nunca acessa os sistemas do cliente diretamente. CPF, e-mail e dados de cartão são mascarados antes de chegar ao modelo.
Treinamento	Dados de clientes não treinam modelos de terceiros. Só modelos internos da KHAL, com dado anonimizado e agregado.
LGPD	KHAL como operadora, DPA padrão, encarregado (DPO) nomeado, registro das operações de tratamento.
Incidentes	Página de status com atualização a cada 10 minutos. Incidente com dado pessoal comunicado em até 48 horas.
Disponibilidade	98,7% ao mês como padrão, apurado em painel auditável. Metas maiores por contrato.
Suporte	24/7 em português, três níveis de atendimento, primeira resposta em até 1 hora para incidente crítico.
Continuidade	Backup automático com restauração a ponto no tempo, troca automática de provedor de modelo, rollback em minutos.

TEMA	COMO A KHAL ATENDE
Fim de contrato	Exportação em formato estruturado e eliminação ou devolução dos dados.
Certificações	ISO/IEC 27001, SOC 2 e pentest independente previstos para o 1º trimestre de 2027.

02 · INFRAESTRUTURA

Nuvem gerenciada no Brasil, produção isolada

A plataforma roda na AWS em São Paulo. Produção vive em uma conta própria, separada de desenvolvimento e homologação. A esteira de entrega promove para produção a mesma imagem que foi validada, sem reconstruir nada no caminho.



O MODELO DE IA CAI

O gateway troca de provedor sozinho

Roteamento entre AWS Bedrock e Microsoft Azure. O agente segue igual.

A API DO CLIENTE OSCILA

Nova tentativa e, se preciso, transbordo para humano

Nenhum cliente final fica sem resposta.

UM DEPLOY SAI RUIM

A versão anterior volta em minutos

Desfazer um commit. A imagem anterior continua intacta no registro.

E A REGIÃO

Redundância em 3 zonas dentro de São Paulo

A AWS tem uma região no Brasil. Os dados não precisam sair do país para ter redundância.

O que sustenta esse desenho

- Kubernetes gerenciado (EKS) com ambientes de desenvolvimento, homologação e produção separados.
- PostgreSQL gerenciado (RDS) com backup automático, mídia em S3 e eventos em NATS.
- Borda com balanceador e TLS. Credenciais e chaves ficam no cofre de segredos, nunca no código.
- GitOps com ArgoCD. O merge revisado em par é a aprovação. Rollback é desfazer um commit.
- Nenhuma credencial de nuvem na esteira. O deploy só enxerga o próprio ambiente, nunca os segredos.

03 · MODELOS DE IMPLANTAÇÃO

Onde a KHAL roda é decisão do cliente

Quando a política de dados do cliente não permite que nenhuma informação saia do ambiente dele, a KHAL vai até o dado. Os três modelos usam a mesma plataforma e os mesmos controles.

PADRÃO

SaaS KHAL

Ambiente gerenciado pela KHAL na AWS São Paulo. Começa mais rápido e recebe atualizações sem esforço do cliente.

DADOS QUE NÃO SAEM

Dedicado no ambiente do cliente

A plataforma roda em máquina dedicada dentro da rede do cliente, com acesso por VPN. Já operamos assim com um grande grupo de telecomunicações, e isso encurtou a aprovação de segurança.

QUALQUER NUVEM

Gateway do lado do cliente

O cliente expõe só o necessário em uma camada própria (gateway ou BFF), que já filtra campos sensíveis. Funciona com Azure, GCP ou ambiente local.

04 · SEUS DADOS E A IA

O agente nunca toca os seus sistemas diretamente

Toda chamada do agente passa por uma camada de software, as tools. Ela conversa com as APIs que o cliente já tem e entrega ao modelo só o que ele precisa para responder, com os campos sensíveis já mascarados.

01

Canal

Cliente final escreve ou liga.

02

Agente decide

Escolhe a próxima ação dentro do que foi permitido.

03

Tool chama a API

Só endpoints liberados, com parâmetros validados.

04

Mascaramento

CPF, e-mail, cartão e outros campos sensíveis saem antes do modelo.

05

Modelo responde

Pelo gateway de modelos, com opt-out de treinamento.

06

Registro

Cada interação com identificador, horário e trilha de auditoria.

- **Sem refatoração:** as tools usam os endpoints que o cliente já tem hoje.
- **Mínimo necessário:** o modelo recebe o dado da tarefa, não a base do cliente.
- **Anonimização local no diagnóstico.** Para medir o potencial de automação, transcrevemos e anonimizamos as interações dentro da infraestrutura do cliente, com modelos locais. Anonimização completa, não pseudonimização. Nada sai antes disso.
- **Dados do cliente são do cliente.** A KHAL usa esses dados só para executar o contrato.

Limites claros para o que a IA pode fazer

Modelos de linguagem são probabilísticos. Por isso a KHAL desenha cada agente com permissões mínimas, defesas contra manipulação, medição contínua de qualidade e saída para um humano sempre que o caso pede.

Treinamento de modelos

- Dados de clientes **não treinam modelos de terceiros**. Os provedores de modelo operam com opt-out de treinamento.
- A KHAL só usa dados **anonimizados e agregados** para melhorar os próprios modelos internos, com anonimização irreversível e proibição de reidentificação. Nenhum cliente ou titular é identificável.
- O cliente pode recusar esse uso no contrato.

Defesa contra prompt injection

INSTRUÇÃO SEPARADA DE CONTEÚDO

Texto de usuário é dado, nunca ordem

Mensagens, e-mails e documentos que chegam ao agente entram como conteúdo. As regras do agente ficam em uma camada que o usuário não alcança.

PERMISSÃO MÍNIMA

O agente só faz o que a tool permite

Cada agente tem uma lista fechada de ações, com parâmetros validados no software. Pedir outra coisa não abre outra porta.

VALIDAÇÃO DE SAÍDA

Resposta conferida antes de sair

Bloqueio de dado pessoal indevido, de assunto fora do escopo e de promessa fora da alçada definida pelo cliente.

DETECÇÃO

Tentativa de manipulação vira transbordo

Padrões de jailbreak e de extração de instruções são detectados e registrados. O atendimento segue com um humano.

Avaliação contínua (evals)

- **Conjunto de testes por cliente**, montado a partir de interações reais anonimizadas, separado por motivo de contato.
- **Teste antes de cada versão**. Uma mudança de prompt, modelo ou fluxo só vai para produção se não piorar os resultados.
- **Testes adversariais** de prompt injection e jailbreak antes da entrada em produção.
- **Qualidade medida em produção** por rotinas próprias, com acurácia acompanhada por motivo de contato. A acurácia pode virar meta contratual.

Supervisão humana

- Transbordo para atendente humano em qualquer ponto do fluxo, com o contexto da conversa.
- Operações críticas e limites de alçada definidos pelo cliente, com aprovação humana quando ele exigir.
- Suporte para avisar o usuário final de que ele fala com um agente de IA.

06 · PRIVACIDADE E LGPD

Operadora de dados, com regras escritas

Nos dados pessoais tratados para o cliente, a KHAL atua como operadora e o cliente como controlador (Lei 13.709/2018). A KHAL trata esses dados só para executar o contrato e seguindo as instruções do controlador.

TEMA	COMPROMISSO
Contrato	Acordo de tratamento de dados (DPA) padrão, anexo ao contrato.
Encarregado (DPO)	Cezar Vasconcelos · dpo@namastex.ai
Direitos dos titulares	Pedido recebido pela KHAL é encaminhado ao cliente em até 2 dias úteis, com apoio para o atendimento.
Dados sensíveis	Só com autorização prévia e por escrito (art. 11 da LGPD).
Transferência internacional	Quando houver, segue os arts. 33 a 36 da LGPD e a Resolução CD/ANPD 19/2024, com registro no DPA.
Registros	Registro das operações de tratamento (ROPA), relatório de impacto (RIPD) e inventário de dados pessoais.
Segurança	Medidas técnicas e administrativas alinhadas ao Guia Orientativo de Segurança da Informação da ANPD.
Comprovação	Relatórios e questionário de segurança uma vez por ano ou após incidente confirmado.

Quem mais participa do tratamento

Provedores de nuvem e de modelos de IA são suboperadores da KHAL. Todos assumem obrigações de proteção de dados no mínimo equivalentes às do contrato com o cliente.

SUBOPERADOR	FINALIDADE	LOCAL	DADOS
Amazon Web Services	Infraestrutura, banco de dados e armazenamento	Brasil (São Paulo)	Dados da operação, criptografados
AWS Bedrock	Inferência de modelos de IA	Conforme o modelo	Conteúdo mascarado, sem treinamento
Microsoft Azure	Inferência de modelos de IA (contingência)	Conforme o modelo	Conteúdo mascarado, sem treinamento
WorkOS	Login, SSO e MFA dos usuários da plataforma	EUA	Nome e e-mail corporativo
Cloudflare	DNS e proteção da borda (WAF)	Global	Metadados de requisição
Sentry	Monitoramento de erros	EUA	Dados técnicos, sem dado pessoal

A lista vale para o ambiente SaaS. No modelo dedicado, a infraestrutura é a do cliente. Mudanças na lista são comunicadas aos clientes com antecedência.

Segurança em camadas

IDENTIDADE E ACESSO

Quem entra e o que pode fazer

SSO por SAML 2.0 ou OIDC (Microsoft Entra ID, Google Workspace), MFA obrigatório, perfis por função com menor privilégio, revogação imediata e revisão periódica de acessos.

CRIPTOGRAFIA

Dado protegido em trânsito e em repouso

TLS 1.2 ou superior em todas as conexões. AES-256 em banco, backups e armazenamento. Segredos em cofre, com rotação.

DESENVOLVIMENTO

Nada chega à produção sem revisão

Toda mudança passa por pull request revisado por outro engenheiro. Varredura de segredos no código. Uma imagem construída, testada e promovida.

MONITORAMENTO

Quem fez o quê, e quando

Logs de auditoria das ações relevantes, alertas de erro em tempo real e trilha por interação de agente.

BORDA

Proteção antes da aplicação

Firewall de aplicação (WAF) e mitigação de DDoS na borda, TLS terminado no balanceador.

PESSOAS

Regras para o time

Termo de confidencialidade, políticas de trabalho remoto e de dispositivos móveis, acesso a produção restrito a quem precisa.

Preparada para falhar sem parar

- Backup automático do banco com restauração a ponto no tempo. Em falhas comuns, a perda real é de minutos.
- Objetivos declarados: RTO de 8 horas e RPO de 24 horas para o pior cenário, com testes de restauração registrados.
- Redundância em 3 zonas de disponibilidade na região de São Paulo.
- Contingência de modelo: se um provedor de IA cai, o gateway roteia para outro sem mudar o agente.
- Plano formal: política de backup, plano de continuidade de negócios, plano de recuperação de desastres e análise de impacto no negócio (BIA).

Aviso rápido, atualização constante

INSTABILIDADE

status.khal.ai

Reporte imediato e atualização a cada 10 minutos até a normalização.

DADO PESSOAL

Aviso em até 48 horas

Comunicação por escrito ao cliente em até 2 dias do conhecimento confirmado, para que ele cumpra o prazo da ANPD.

DEPOIS

Causa raiz e correção

Relatório de causa raiz após incidente crítico, com as medidas para evitar que se repita.

O que o aviso de incidente com dado pessoal traz

- Data e hora do incidente e de quando ele foi conhecido.
- Descrição e causa provável.
- Categorias e número estimado de titulares afetados.
- Medidas de segurança adotadas antes e depois do incidente.
- Providências para reverter ou reduzir os efeitos, e apoio na comunicação à ANPD e aos titulares.

Um padrão para todos, ajustes para cada operação

Alguns níveis de serviço valem para todo cliente. Outros são definidos em contrato de acordo com

a natureza da operação, como volume, canais e criticidade.

Severidades e primeira resposta

SEVERIDADE	QUANDO	PRIMEIRA RESPOSTA
Crítica	Plataforma indisponível, mais da metade dos usuários sem acesso, ou parada de login, canais ou execução de agentes sem alternativa.	até 1 hora, 24/7
Alta	Funcionalidade indisponível ou degradada sem alternativa, ou impacto relevante restrito a um agente, app ou integração.	até 4 horas
Média	Baixo impacto, com alternativa disponível.	até 48 horas úteis

Todo chamado é classificado em até 1 hora útil. O cliente pode contestar a classificação e escalar para o gestor responsável.

PADRÃO · TODO CLIENTE

O que vale sempre

- Disponibilidade de 98,7% ao mês, apurada em painel auditável.
- Suporte 24/7 em português por support@khal.ai, WhatsApp e canal na plataforma.
- Atendimento em três níveis: uso e acesso (N1), configuração de agentes e fluxos (N2), engenharia e integrações (N3).
- Manutenção programada avisada com 24 horas e mudança com impacto avisada com 72 horas.

POR OPERAÇÃO · EM CONTRATO

O que se ajusta

- Meta de disponibilidade maior, com ambiente dedicado.
- Meta de acurácia por motivo de contato.
- Horas mensais de engenheiro de IA dedicado ao cliente.
- Janelas de atendimento, operações críticas e alçadas.
- Créditos de serviço por descumprimento.

Ficam fora do cálculo de disponibilidade a manutenção programada avisada e falhas em sistemas, integrações ou canais do próprio cliente.

Seus dados saem com você

- Exportação dos dados do cliente em formato estruturado e de uso corrente.
- Eliminação ou devolução dos dados pessoais, conforme instrução do cliente, guardado só o que a lei obriga.
- Transição assistida para a migração, quando solicitada.

O que já cumprimos e o que vem a seguir

REFERÊNCIA	SITUAÇÃO
LGPD	em vigor Programa de privacidade com DPO, DPA, ROPA, RIPD e procedimentos de titulares e incidentes.
ISO/IEC 27002:2022	em vigor Políticas de segurança mapeadas para os controles da norma.
Infraestrutura AWS	em vigor Herança dos controles certificados da AWS (ISO 27001, SOC 2) na camada física e de nuvem.
ISO/IEC 27001	1º tri 2027 Certificação do sistema de gestão de segurança.
SOC 2	1º tri 2027 Relatório de auditoria independente dos controles.
Pentest	1º tri 2027 Teste de intrusão por empresa independente, com resumo disponível sob NDA.

Setores regulados

ENERGIA · ANEEL REN 964/2021

O que entregamos ao distribuidor

Comunicação de incidentes no prazo do contrato, controles de acesso, gestão de vulnerabilidades e a opção de rodar dentro da rede da empresa.

FINANCEIRO · RES. CMN 4.893/2021

O que a instituição precisa saber

Local de armazenamento e processamento, acesso para auditoria, plano de continuidade e eliminação dos dados no fim do contrato.

14 · DOCUMENTOS E PERGUNTAS FREQUENTES

Para o seu time de segurança

Disponíveis sob acordo de confidencialidade. Peça por support@khal.ai.

DOCUMENTO	CONTEÚDO
Política de Segurança da Informação	Princípios, papéis e controles.
Arquitetura de segurança	Camadas de proteção e fluxo de dados.
Controles criptográficos	Algoritmos, chaves e rotação.
Resposta a incidentes	Política e procedimento de notificação.
Backup e continuidade	Política de backup, plano de continuidade, plano de recuperação e BIA.
Privacidade	DPA modelo, política de privacidade e procedimento de direitos dos titulares.
Questionário de segurança	Respostas padrão para homologação de fornecedor.

Os dados dos meus clientes saem do Brasil?

Os dados ficam armazenados na AWS em São Paulo. A inferência de modelos recebe só o conteúdo necessário, já mascarado. Se o cliente exigir que nada saia do ambiente dele, a KHAL roda dentro da sua infraestrutura.

Vocês treinam modelos com os nossos dados?

Modelos de terceiros, não. Modelos internos da KHAL só com dado anonimizado e agregado, e o cliente pode recusar em contrato.

Nossa nuvem é Azure. Isso é um problema?

Não. A KHAL integra por um gateway do lado do cliente ou roda em ambiente dedicado na sua rede.

O que acontece se o provedor de IA cair?

O gateway de modelos troca de provedor sozinho e o agente segue funcionando. Se não houver como responder, o atendimento vai para um humano.

Como reporto um problema de segurança?

Por support@khal.ai, marcando o assunto como segurança, ou com o encarregado de dados em dpo@namastex.ai.

We are AI CX builders.

Creating better customer experiences.

KHAL é uma marca da Namastex Labs Serviços em Tecnologia Ltda.

Suporte: support@khal.ai

Status: status.khal.ai

Privacidade: dpo@namastex.ai