

Política de Segurança da Informação

Afilya · produto operado por XTHUB Serviços e Tecnologias Ltda

CNPJ 32.044.027/0001-72

Versão 1.0 · Vigente desde agosto de 2026 · Revisão anual

Afilya é um produto da XTHUB Serviços e Tecnologias Ltda. Onde este documento diz XTHUB, refere-se a essa pessoa jurídica, responsável pelo tratamento. Afilya é a marca do serviço.

1. Objetivo e alcance

Esta política define como a XTHUB protege as informações que trata na operação do Afilya, plataforma de gestão de programas de afiliado. Aplica-se a todas as pessoas que acessam sistemas ou dados da empresa, incluindo sócios, colaboradores e prestadores.

O Afilya trata dados de clientes empresariais (lojistas e agências) e dados pessoais de criadores de conteúdo obtidos mediante autorização explícita do lojista através da API oficial do TikTok Shop.

2. Encarregado pelo tratamento de dados

Em atendimento ao artigo 41 da Lei 13.709/2018 (LGPD), a XTHUB mantém encarregado pelo tratamento de dados pessoais, acessível em:

contato@xthub.com.br

3. Classificação da informação

CLASSE	O QUE É	TRATAMENTO
Restrita	Credenciais, tokens de acesso, segredos de aplicativo	Nunca em código-fonte ou repositório. Somente em variável de ambiente com acesso nominal
Confidencial	Dados pessoais de criadores, dados comerciais de lojistas	Criptografados em trânsito e em repouso, acesso por privilégio mínimo
Interna	Documentação, código-fonte	Acesso restrito à equipe
Pública	Material de marketing e site	Sem restrição

4. Controle de acesso

O acesso segue o princípio do **privilegio mínimo**: cada pessoa recebe apenas o acesso necessário à sua função, e pelo menor tempo necessário.

- Autenticação multifator obrigatória em todos os serviços que a suportem
- Senhas únicas por serviço, geradas e guardadas em gerenciador de senhas
- Credenciais nominais, sem contas compartilhadas
- Revogação de acesso em até 24 horas do desligamento
- Revisão semestral de quem tem acesso a quê

5. Criptografia

- **Em trânsito:** todo tráfego por TLS 1.2 ou superior. Nenhum endpoint HTTP
- **Em repouso:** disco criptografado em todas as estações de trabalho (FileVault) e criptografia no volume do servidor
- **Segredos:** mantidos em variável de ambiente, fora do controle de versão, com o arquivo de configuração explicitamente ignorado pelo Git

6. Segurança de estações e rede

- Sistema operacional com atualizações automáticas
- Proteção antimalware nativa ativa (XProtect e Gatekeeper no macOS)
- Bloqueio automático de tela por inatividade
- Serviços em contêineres isolados, sem exposição pública de porta de banco
- Firewall com política de negação por padrão, liberando somente o necessário

7. Gestão de vulnerabilidades

- Verificação de dependências a cada mudança relevante e, no mínimo, mensal
- Correção de vulnerabilidade crítica em até 7 dias corridos, alta em até 30
- Atualização das imagens base e do runtime conforme o ciclo do fornecedor

8. Resposta a incidentes

Responsável pela condução: o encarregado (contato@xthub.com.br)

ETAPA	PRAZO
Registro e contenção inicial	24 horas da detecção
Avaliação de impacto e dados afetados	48 horas
Comunicação aos clientes afetados	72 horas da confirmação
Comunicação à ANPD, quando aplicável	prazo legal
Relatório pós-incidente com ação corretiva	15 dias

Canal para reportar incidente ou suspeita: **contato@xthub.com.br**

9. Retenção e eliminação

- Dados tratados apenas enquanto durar a relação contratual e a finalidade
- **Ao término do contrato, todos os dados do cliente são eliminados em até 30 dias**, salvo obrigação legal de guarda
- Eliminação confirmada por escrito ao cliente quando solicitado
- Registros de log de segurança guardados por 6 meses

10. Suboperadores e transferência internacional

A XTHUB utiliza os seguintes suboperadores:

SUBOPERADOR	FINALIDADE	PAÍS
Provedor de hospedagem	Execução da aplicação e banco de dados	Brasil
Anthropic PBC	Redação do texto da recomendação	Estados Unidos

A análise não é terceirizada. A detecção de situações, o cálculo do valor em jogo e a priorização são executados por lógica determinística da própria XTHUB, sem uso de

modelo de linguagem. O modelo é usado apenas para redigir a frase de recomendação já decidida pelo motor.

O que é enviado ao modelo é pseudonimizado. Antes de qualquer chamada, os identificadores de criador (apelido de perfil, nome e código de cupom) são substituídos por rótulos genéricos do tipo "Criador A", e a tradução de volta acontece dentro da infraestrutura da XTHUB. O suboperador recebe apenas dado operacional (situação detectada, métrica e valor), sem identificar pessoa alguma. Não são enviados documentos de identificação, dados bancários nem dados sensíveis.

Quando houver transferência internacional, ela observa o Capítulo V da LGPD.

11. Direitos dos titulares

A XTHUB atua majoritariamente como **operadora**, tratando dados por conta e ordem do lojista, que é o controlador. Pedidos de acesso, correção, portabilidade ou eliminação recebidos diretamente são encaminhados ao controlador em até 5 dias úteis, e a XTHUB dá o apoio técnico necessário para que ele responda no prazo legal.

Quando solicitado pelo lojista ou pelo TikTok Shop, a XTHUB fornece, atualiza ou elimina os dados de um titular específico.

12. Vigência e revisão

Esta política é revisada ao menos uma vez por ano, ou antes disso em caso de mudança relevante de operação, de fornecedor ou de legislação.

Contato: **contato@xthub.com.br**