Kalidash

Política de Divulgação Responsável de Vulnerabilidades

Kalidash Consultoria em Dados, Automação e IA Ltda.

Última atualização: Abril de 2026

1. Introdução

A Kalidash leva a segurança de seus sistemas e dos dados de seus clientes a sério. Valorizamos o trabalho de pesquisadores de segurança e da comunidade técnica que, de boa-fé, identificam e reportam vulnerabilidades de forma responsável.

Esta política estabelece as diretrizes para o reporte de vulnerabilidades, os compromissos da Kalidash com quem reporta e as regras para pesquisa de boa-fé.

2. Como Reportar

Se você identificou uma possível vulnerabilidade em qualquer sistema, aplicação ou serviço da Kalidash, envie um e-mail para privacidade@kalidash.com com o assunto Vulnerabilidade, incluindo:

- Descrição do problema encontrado.
- Passos para reprodução.
- Impacto potencial.
- Evidências, quando possível (capturas de tela ou logs).

3. Nosso Compromisso

Confirmaremos o recebimento do reporte em até 2 (dois) dias úteis.

Faremos a análise e retornaremos com um posicionamento em até 10 (dez) dias úteis.

Manteremos o pesquisador informado sobre o andamento da correção.

Não adotaremos medidas legais contra pesquisadores que atuem de boa-fé, dentro das regras desta política.

Reconheceremos publicamente a contribuição do pesquisador, mediante sua autorização, após a correção da vulnerabilidade.

4. Regras para Pesquisa de Boa-Fé

Para que a pesquisa seja considerada de boa-fé e esteja coberta por esta política, o pesquisador deve:

- Não acessar, alterar ou excluir dados de terceiros.
- Não executar ataques de negação de serviço (DoS/DDoS).
- Não utilizar engenharia social contra colaboradores, clientes ou parceiros da Kalidash.
- Interromper o teste e reportar imediatamente caso acesse dados pessoais de forma não intencional.
- Não divulgar publicamente a vulnerabilidade antes da correção e do alinhamento conjunto com a Kalidash.
- Não exigir pagamento ou contrapartida como condição para o reporte.

5. Escopo

Esta política cobre os sistemas e aplicações operados diretamente pela Kalidash.

Sistemas de clientes e de provedores terceiros (como Google, Supabase e demais serviços em nuvem) possuem seus próprios programas de divulgação de vulnerabilidades e devem ser reportados diretamente a eles.

6. Programa de Recompensas

A Kalidash não possui, no momento, um programa formal de recompensas (Bug Bounty). A implementação de um programa dessa natureza será avaliada conforme a maturidade e a escala das operações.

7. Contato

Kalidash Consultoria em Dados, Automação e IA Ltda.

E-mail: privacidade@kalidash.com

Responsável: Iago Braz (Encarregado de Proteção de Dados)