

Política de Gestão de Fornecedores

Empresa SaaS S.A.

Área responsável: Segurança da Informação

Aprovada pela Diretoria Executiva

1. Objetivo. Definir como a empresa escolhe, contrata e acompanha os fornecedores que acessam informações ou sistemas, para proteger os dados dos clientes.

2. Abrangência. Todo fornecedor de produto ou serviço com acesso a dados de clientes, a dados pessoais ou aos sistemas da empresa.

3. Classificação.

- Crítico: trata dados de clientes ou sustenta a plataforma (por exemplo, nuvem, monitoramento e atendimento).
- Relevante: acessa dados internos ou dados pessoais de colaboradores.
- Comum: não tem acesso a dados.

4. Antes da contratação.

- A equipe de segurança avalia o risco por questionário e pela análise das certificações do fornecedor.
- Para os críticos, confere também a região onde os dados ficam e o mecanismo de transferência internacional, quando houver.
- Os críticos e os relevantes só são contratados com a aprovação do Gerente de Segurança da Informação.

5. Contrato. Cláusulas de confidencialidade, segurança, proteção de dados, comunicação de incidentes, subcontratação e devolução ou eliminação dos dados ao término.

6. Acompanhamento.

- Os fornecedores críticos são reavaliados todo ano.
- Uma mudança relevante no serviço exige nova avaliação.
- Os subprocessadores com acesso a dados de clientes ficam na lista pública do Trust Center.

7. Encerramento. No fim do contrato, os acessos são revogados e a devolução ou a eliminação dos dados é confirmada.

8. Revisão. Esta política é revisada uma vez por ano.