Política de Conhecimento do Fornecedor (KYS)

MARCHA LTDA
CNPJ: 58.300.812/0001-32
Avenida Paulista, Nº 1337, Bairro Bela Vista, São Paulo-SP. CEP: 01.311-200

Dados da Empresa

Razão Social	MARCHA LTDA
CNPJ	58.300.812/0001-32
Endereço	Avenida Paulista, Nº 1337, Bairro Bela Vista, São Paulo-SP.
CEP	01.311-200

Informações Gerais

Título	Política de Conhecimento do Fornecedor (KYS)
Versão	V1.0.01
Aprovador	Diretoria Executiva
Data da Aprovação	20/01/2026
Próxima Revisão	—
Responsável pela Política	Zijie Pan
Classificação da Informação	Interna

SUMÁRIO

OBJETIVO E ESCOPO

I. Objetivo

Esta Política de Conhecimento do Fornecedor (KYS – Know Your Supplier) estabelece os procedimentos, controles e responsabilidades para a identificação, verificação e monitoramento de todos os fornecedores, consultores e prestadores de serviços da MARCHAPAY LTDA E.P.P.. O objetivo principal é blindar a MarchaPay contra riscos de contágio que possam comprometer a segurança cibernética, a Propriedade Intelectual (PI), a continuidade operacional do Gateway e o compliance regulatório (LGPD e PLD/FT).

II. Escopo

a. Todos os fornecedores de bens e serviços, com foco especial em Fornecedores de Tecnologia e Infraestrutura (Cloud Computing, Hosting, soluções de Software).

b. Prestadores de serviços terceirizados, consultores e assessores externos.

c. Fornecedores de soluções de Risco (Antifraude, KYC Digital).

d. Todos os responsáveis pelas áreas de Compras, Tecnologia, Risco e Compliance no processo de contratação.

III. Finalidades

a. **Mitigar Risco Operacional e Cibernético:** Assegurar que os fornecedores críticos atendam aos padrões de Disponibilidade e Segurança da Informação da MarchaPay.

b. **Proteger Dados (LGPD):** Garantir que fornecedores que atuam como Operadores de Dados Pessoais adotem medidas de segurança compatíveis.

c. **Integridade:** Prevenir o relacionamento com fornecedores envolvidos em atividades ilícitas, corrupção ou PLD/FT.

d. **Garantir a Continuidade:** Assegurar que fornecedores críticos possuam Planos de Continuidade de Negócios (PCN) e DRP (Disaster Recovery Plan) eficazes.

BASE LEGAL E REGULATÓRIA

Consolida-se o arcabouço jurídico-regulatório aplicável que impõe o dever de diligência sobre a cadeia de fornecimento, sendo o cumprimento destes diplomas imperativo para a legitimidade dos procedimentos KYS.

I. Legislação Aplicável

a. **Lei nº 13.709/2018 (LGPD):** Fundamento para a diligência de fornecedores que atuam como Operadores de Dados.

b. **Lei nº 12.846/2013 (Lei Anticorrupção):** Base para a verificação de integridade e antecedentes dos fornecedores.

c. **Lei nº 9.613/1998 (Lei de Lavagem de Dinheiro):** Fundamenta a checagem de antecedentes financeiros dos sócios.

d. **Circular BACEN nº 3.978/2020:** Política de Conformidade (base para a gestão de riscos e compliance).

e. **Resolução BCB nº 119/2021:** Política de Gerenciamento de Riscos.

II. Regulamentações do Banco Central (Referencial Técnico)

a. **Resolução nº 4.893/2021:** Política de Segurança Cibernética (base para a avaliação técnica dos fornecedores de TI).

b. **Resolução BCB nº 80/2021:** Arranjos de Pagamento (contexto de atuação do Gateway).

III. Órgãos Reguladores

a. **Autoridade Nacional de Proteção de Dados (ANPD):** Supervisor da LGPD (foco na responsabilização do Controlador pela escolha do Operador).

b. **Conselho de Controle de Atividades Financeiras (COAF):** Unidade de Inteligência Financeira.

DEFINIÇÕES

I. Termos Gerais

a. **Fornecedor:** Pessoa física ou jurídica que provê bens ou serviços à MarchaPay.

b. **KYS (Know Your Supplier):** Conjunto de procedimentos para identificação, verificação e conhecimento dos fornecedores.

c. **Due Diligence:** Processo de investigação e verificação detalhada das informações do fornecedor.

d. **Fornecedor Crítico:** Prestador de serviços essencial que, em caso de falha, compromete a Disponibilidade do Gateway, a Integridade do código-fonte ou a Confidencialidade dos dados.

e. **SLA (Service Level Agreement):** Acordo de nível de serviço que define padrões de qualidade e performance, especialmente em relação ao uptime e segurança.

II. Classificação de Risco

a. **Risco Baixo:** Fornecedores de bens e serviços básicos sem acesso a informações sensíveis.

b. **Risco Médio:** Fornecedores com acesso limitado a sistemas ou informações importantes.

c. **Risco Alto/Crítico:** Fornecedores estratégicos com amplo acesso a sistemas, dados ou operações essenciais (Ex: Cloud Providers, Software Developers).

ESTRUTURA DE GOVERNANÇA

Dispõe-se sobre a arquitetura de governança corporativa em matéria de KYS, atribuindo competências indelegáveis às áreas de defesa.

I. Responsabilidades da Diretoria

A Diretoria é responsável por aprovar e revisar periodicamente esta política, definir o apetite ao risco da instituição e supervisionar a efetividade dos controles KYS, garantindo os recursos tecnológicos e humanos para a due diligence.

II. Comitê de Fornecedores (Risco e Compliance)

a. **Composição:** Diretor de Compliance, Gerente de Compras, Responsável pela Área de Risco, Representante da Área de Tecnologia (TI/Cibersegurança) e Jurídico.

b. **Atribuições:** Analisar e aprovar formalmente Fornecedores de Risco Alto/Crítico; Avaliar a adequação do PCN e das certificações de segurança do fornecedor; Propor melhorias nos procedimentos de KYS.

III. Área de Compliance (Segunda Linha)

a. **Responsabilidades:** Implementar os procedimentos KYS, realizar as verificações de integridade e PLD/FT dos sócios do fornecedor e monitorar a conformidade regulatória contínua.

IV. Área de Compras e Tecnologia (Primeira Linha)

a. **Responsabilidades:** Coletar a documentação inicial, aplicar o Questionário de KYS e garantir que os contratos incluam os SLAs e as cláusulas de segurança/LGPD obrigatórias.

CLASSIFICAÇÃO DE FORNECEDORES

Fixa-se a metodologia de avaliação baseada no Impacto na Continuidade Operacional e no Nível de Acesso aos Ativos da MarchaPay.

I. Matriz de Risco (Fatores-Chave)

a. **Fatores de Risco por Tipo de Serviço (Foco na Tecnologia)**

- Risco Alto/Crítico: Provedores de nuvem, Empresas de segurança da informação, Desenvolvedores de software crítico, Fornecedores de soluções de PLD/FT.

b. **Fatores de Acesso**

- Acesso Limitado (Risco Baixo): Sem acesso a sistemas internos.
- Acesso Amplo (Risco Alto): Acesso a sistemas críticos de pagamento, bases de dados de clientes (LGPD) ou infraestrutura de TI essencial.

II. Criticidade Operacional

a. **Crítico (Risco Alto):** Serviços essenciais às operações do Gateway; Impacto severo e poucas alternativas viáveis no mercado.

PROCEDIMENTOS DE IDENTIFICAÇÃO

Normatizam-se as etapas de seleção e contratação, abrangendo coleta de dados, validação documental e verificação de antecedentes.

I. Processo de Seleção

Disciplina-se o fluxo de coleta de informações sobre a Razão Social, CNPJ, Informações dos Sócios e o Histórico profissional (PEPs).

II. Questionário de Conhecimento (KYS)

Impõe-se a aplicação de questionários detalhados, com foco na capacidade técnica de segurança e compliance.

a. **Conformidade e Governança:** Questionamentos sobre a existência de políticas de PLD/FT, Programa de Integridade e a designação de DPO.

III. Validação de Informações

Define-se o rol de consultas obrigatórias a bases oficiais.

a. **Consultas Obrigatórias:** CNPJ na Receita Federal, Consulta ao SERASA/SPC, Certidões negativas trabalhistas, Consulta ao CEIS (Cadastro de Empresas Inidôneas) e Verificação em Listas de Sanções.

DOCUMENTAÇÃO EXIGIDA

Estabelecem-se os requisitos documentais mínimos e complementares segundo o grau de risco.

I. Documentos Obrigatórios

Documentação Societária e Fiscal (CNPJ, Contrato social consolidado, Certidões negativas de débitos).

II. Documentos Complementares (Fornecedores Críticos)

a. **Due Diligence Reforçada:** Demonstrações financeiras auditadas, Certificações de segurança (ISO 27001, PCI-DSS), Relatórios de auditoria independente, Planos de Continuidade de Negócios (PCN) e Apólices de seguro (responsabilidade civil, E&O) compatíveis com o risco.

VERIFICAÇÃO E VALIDAÇÃO

Regulamenta-se o processo de verificação e os critérios de aprovação, assegurando rastreabilidade decisória.

I. Processo de Verificação

a. **Verificação Automática:** Aplicada a Risco Baixo.

b. **Verificação Manual:** Exigida para Risco Médio/Alto, incluindo Parecer fundamentado da Área de Compliance e TI.

II. Níveis de Due Diligence

a. **Due Diligence Simplificada (Risco Baixo):** Verificação básica.

b. **Due Diligence Reforçada (Risco Alto):** Verificação detalhada de antecedentes, Auditoria Técnica In Loco (visita) ou remota das instalações e Aprovação obrigatória pelo Comitê.

III. Critérios de Aprovação

a. **Aprovação pelo Comitê:** Obrigatória para Fornecedores Críticos, Contratos de alto valor ou histórico de restrições superadas.

MONITORAMENTO CONTÍNUO

Institui-se a obrigação de atualização cadastral periódica e de monitoramento de performance.

I. Atualização Cadastral

a. **Periodicidade:** Fornecedores Críticos: Trimestral ou imediatamente após Gatilhos para Atualização (Ex: Vencimento de certificações, Incidente de segurança).

II. Monitoramento de Performance

Monitoramento do cumprimento de SLAs (Ex: Uptime e tempo de resposta) e Indicadores de Risco (Ex: Problemas de segurança da informação, Envolvimento em processos judiciais).

FORNECEDORES CRÍTICOS E ESTRATÉGICOS

Esta seção é dedicada aos fornecedores de maior risco à PI e à operação.

I. **Infraestrutura Tecnológica Crítica:** Provedores de nuvem, Desenvolvedores de software crítico e Fornecedores de soluções de PLD/FT.

II. **Procedimentos Específicos:** Exigência de Certificações de Segurança (ISO 27001, PCI-DSS) e Planos de Continuidade de Negócios (PCN).

III. **Aprovação:** Aprovação obrigatória do Comitê de Fornecedores, Parecer técnico e Plano de contingência obrigatório.

CONTROLES ESPECIAIS

Determina-se salvaguardas adicionais.

I. **Controles de Acesso (Cibersegurança):** Menor privilégio necessário, Segregação de ambientes e Autenticação Multifator obrigatória para acesso a APIs e sistemas críticos.

II. **Controles Contratuais (Transferência de Risco):** Os contratos devem incluir Cláusula de Direito de Auditoria (pela MarchaPay) e Cláusula de Penalidade/Indenização (multas por descumprimento de SLA/Segurança).

SISTEMA DE INFORMAÇÕES

Todos os documentos de KYS devem ser armazenados de forma segura e inalterável.

I. Retenção: Registros mantidos pelo prazo mínimo de 5 (cinco) anos após o término do relacionamento.

II. Segurança: Armazenamento digital seguro, com criptografia e controle de acesso (LGPD).

TREINAMENTO E CAPACITAÇÃO

I. **Programa Anual:** Treinamento anual obrigatório para as áreas de Compras, Tecnologia e Compliance sobre as diretrizes KYS e o mapeamento de riscos de terceiros.

AUDITORIA E CONTROLES INTERNOS

O programa KYS será submetido a auditorias para validar a eficácia dos controles.

I. **Auditoria Interna:** Revisão periódica da efetividade dos controles KYS e adequação da classificação de risco.

II. **Controles de Segunda Linha:** Monitoramento independente realizado pela área de Compliance sobre a documentação de KYS.

DISPOSIÇÕES FINAIS

I. **Vigência e Revisão:** Esta Política entra em vigor na data de sua aprovação e será revista anualmente.

II. **Sanções:** O descumprimento desta política por fornecedores pode resultar em Suspensão temporária dos serviços, Rescisão contratual e Aplicação de penalidades contratuais (multas por falha de segurança ou descumprimento de SLA).

III. **Documentos Relacionados:** Política de PLD, Política de Segurança Cibernética, Política de Privacidade.