Política de Conhecimento do Parceiro (KYP)

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 Parceiro (KYP)
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 Parceiro (KYP) estabelece os procedimentos, controles e responsabilidades para identificação, verificação e monitoramento de parceiros comerciais e estratégicos da MARCHAPAY LTDA E.P.P.. O objetivo é blindar a MarchaPay contra riscos operacionais, reputacionais e de compliance (PLD/FT e Segurança Cibernética) inerentes ao compartilhamento de tecnologia e de dados sensíveis.

II. Escopo

a. Todos os parceiros comerciais da MarchaPay, incluindo Parceiros White Label (Licenciados da Tecnologia), Integradores Tecnológicos (com acesso a APIs críticas), Fornecedores de Infraestrutura Crítica (Cloud) e Parceiros Estratégicos (Instituições de Pagamento/Adquirentes).

b. Todos os responsáveis pelos processos de parcerias, desde a prospecção até a gestão do relacionamento e offboarding.

III. Finalidades

a. Prevenir o relacionamento com parceiros envolvidos em atividades ilícitas, reforçando as Políticas de PLD/FT.

b. Mitigar o risco operacional e a exposição da Propriedade Intelectual (PI) da MarchaPay.

c. Assegurar a conformidade regulatória e a transferência de responsabilidade contratual nos acordos de licenciamento (White Label).

d. Proteger a reputação e integridade da instituição, garantindo o alinhamento de compliance e cultural.

BASE LEGAL E REGULATÓRIA

Consolida-se o arcabouço jurídico-regulatório aplicável, cujo cumprimento é imperativo para a legitimidade dos procedimentos KYP.

I. Legislação Aplicável

a. **Lei nº 9.613/1998:** Lei de Lavagem de Dinheiro (fundamenta a diligência PLD/FT).

b. **Lei nº 12.865/2013:** Lei dos Arranjos de Pagamento (regula o setor de atuação).

c. **Lei nº 13.709/2018 (LGPD):** Regula o compartilhamento e a proteção de dados pessoais (aplicável à transferência de dados de KYC).

d. **Lei nº 12.846/2013:** Lei Anticorrupção (fundamenta a verificação de integridade).

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

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

II. Regulamentações do Banco Central (Referencial)

a. **Resolução nº 4.893/2021:** Política de Segurança Cibernética (base para a avaliação de segurança tecnológica dos parceiros).

b. **Resolução BCB nº 80/2021:** Arranjos de Pagamento.

III. Órgãos Reguladores

a. **Banco Central do Brasil (BCB):** Supervisor principal (indiretamente, via parceiros IPs).

b. **Conselho de Controle de Atividades Financeiras (COAF):** Unidade de Inteligência Financeira (foco na PLD/FT do parceiro).

c. **Autoridade Nacional de Proteção de Dados (ANPD):** Proteção de dados pessoais (foco na adequação do parceiro à LGPD).

Política de Conhecimento do Parceiro (KYP)

DEFINIÇÕES

I. Termos Gerais

a. **Parceiro:** Pessoa jurídica que mantém relacionamento comercial ou tecnológico relevante com a MarchaPay.

b. **KYP (Know Your Partner):** Conjunto de procedimentos para identificação, verificação e conhecimento dos parceiros.

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

d. **Integrador Tecnológico:** Empresa que desenvolve soluções utilizando APIs críticas e o Gateway da MarchaPay.

e. **White Label:** Parceiro que licencia a tecnologia da MarchaPay para operar com sua própria marca.

II. Classificação de Risco (Risco de Contágio)

a. **Risco Baixo:** Parceiros com integração limitada (APIs públicas) e baixo impacto operacional.

b. **Risco Médio:** Parceiros com relacionamento relevante e impacto moderado nas operações, sem acesso direto a sistemas críticos.

c. **Risco Alto:** Parceiros estratégicos, Parceiros White Label, com alto impacto operacional e acesso a dados sensíveis ou código-fonte.

III. Tipos de Parceiro (Relevância para a MarchaPay)

a. **Parceiro Tecnológico Crítico:** Empresas com integração ampla à PI (APIs, ambientes de staging ou cloud).

b. **White Label (Licenciado):** Parceiro que assume a responsabilidade regulatória perante o cliente final.

c. **Parceiro Estratégico:** Instituições de Pagamento (IPs), Adquirentes ou Bureaus de Risco (Celcoin, Serasa).

ESTRUTURA DE GOVERNANÇA

Dispõe-se sobre a arquitetura de governança corporativa em matéria de KYP, assegurando independência funcional e fluxo de reporte tempestivo.

I. Responsabilidades da Diretoria

a. Aprovar e revisar periodicamente esta política.

b. Assegurar recursos adequados para implementação dos sistemas de diligência tecnológica.

c. Definir a estratégia de risco em relação ao compartilhamento da PI.

d. Aprovar formalmente relacionamentos com Parceiros de Risco Alto.

II. Comitê de Parcerias (Compliance e Risco)

a. **Composição:** Diretor de Compliance, Diretor Comercial, Responsável pela Área de Risco e Jurídico, e Gerente de Tecnologia/Segurança.

b. **Atribuições:** Monitorar a implementação desta política; Analisar casos de risco elevado (PLD/FT, sanções); Aprovar Parceiros de Risco Alto e Parceiros com Integração Ampla.

III. Área de Compliance

a. **Responsabilidades:** Implementar e manter os procedimentos KYP; Realizar as verificações de integridade (screening); Monitorar a conformidade regulatória dos parceiros críticos (LGPD, PLD).

IV. Área de Parcerias e Canais

a. **Responsabilidades:** Coletar a documentação do parceiro; Aplicar o Questionário de Conhecimento (KYP); Conduzir processos de seleção; Gerenciar o relacionamento e a performance comercial.

CLASSIFICAÇÃO DE PARCEIROS

Fixa-se a metodologia de avaliação baseada em risco que segmenta parceiros por fatores críticos.

I. Matriz de Risco (Fatores-Chave)

a. **Fatores de Risco por Tipo de Parceria (Foco na PI e Risco Regulatório)**

- Risco Baixo: Fornecedores de soluções complementares ou softwares não essenciais.
- Risco Médio: Integradores com APIs amplas que acessam dados de clientes, mas não o código-fonte.
- Risco Alto: Parceiros White Label (assunção de risco regulatório/cliente final) e Integradores com acesso crítico (sistemas de liquidação ou deploy).

b. **Fatores de Integração**

- Integração Limitada (Risco Baixo): Uso de APIs públicas básicas, sem acesso a dados sensíveis.
- Integração Ampla (Risco Alto): Acesso a sistemas críticos, compartilhamento de bases de dados ou integração operacional profunda com risco de downtime sistêmico.

II. Impacto Estratégico

a. **Alto Impacto (Risco Alto):** Relacionamento crítico para a continuidade da operação do Gateway (Ex: Provedor Cloud ou parceiro de liquidação).

PROCEDIMENTOS DE IDENTIFICAÇÃO

Normatizam-se as etapas de seleção e contratação para diferentes tipos de parceiros.

I. Processo de Seleção

Disciplina-se o fluxo de coleta de informações, verificação documental e validação de capacidade técnica e de compliance antes do início do relacionamento.

a. **Informações Básicas**

- Dados da Empresa: Razão social, CNPJ, Website e Atividade Principal.
- Informações dos Sócios: Identificação completa dos sócios, participação societária e Verificação de PEPs (Pessoas Politicamente Expostas).

b. **Informações Complementares**

- Capacidade Comercial/Técnica: Experiência no mercado de pagamentos, Certificações e Estrutura da equipe técnica.
- Situação Financeira: Faturamento anual, Demonstrações financeiras (para capacidade de investimento) e Histórico de inadimplência.

II. Questionário de Conhecimento (KYP)

Impõe-se a aplicação de questionários detalhados.

a. **Conformidade e Governança (Foco no Risco Contratual)**

b. Possui políticas de compliance implementadas (PLD/FT e LGPD)?

c. Possui Certificações de Segurança (ISO 27001, PCI-DSS)?

d. Já foi objeto de investigações ou sanções (CADE, BACEN)?

III. Validação de Informações

Define-se o rol de consultas obrigatórias a bases oficiais, bureaus de crédito e listas restritivas.

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

DOCUMENTAÇÃO EXIGIDA

Estabelecem-se os requisitos documentais mínimos e complementares.

I. Documentos Obrigatórios

a. **Documentação Societária:** Contrato social consolidado, Cartão CNPJ atualizado.

b. **Documentação Fiscal e Trabalhista:** Certidões negativas de débitos federais, estaduais e trabalhistas.

II. Documentos Complementares (conforme risco)

a. **Risco Médio/Alto (Tecnológico/Regulatório) — Due Diligence Reforçada:**

- Relatórios de Auditoria Independente (demonstrando a segurança de dados).
- Políticas de compliance e Código de Ética do parceiro.
- Apólices de seguro (responsabilidade civil, E&O) compatíveis com o risco da parceria.

b. **Parceiros Estratégicos (Foco na PI):**

- Política de Segurança da Informação detalhada (para acesso à PI).
- Certificações de segurança (ISO 27001, PCI-DSS, se aplicável).
- Planos de Continuidade de Negócios (PCN) e DRP (Disaster Recovery Plan).

VERIFICAÇÃO E VALIDAÇÃO

Regulamenta-se o processo de verificação e os critérios de aprovação.

I. Processo de Verificação

a. **Verificação Automática:** Aplicada a Risco Baixo (Validação de CNPJ e Ausência em listas restritivas).

b. **Verificação Manual:** Exigida para Risco Médio/Alto e Parceiros Estratégicos. Procedimentos: Pesquisa em fontes abertas, contato com referências, Parecer fundamentado do Compliance.

II. Níveis de Due Diligence

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

b. **Due Diligence Padrão (Risco Médio):** Verificação completa e consulta a bureaus de crédito.

c. **Due Diligence Reforçada (Risco Alto):** Verificação detalhada de antecedentes, Visita técnica às instalações (para Parceiros Críticos/Cloud) e Aprovação obrigatória pelo Comitê.

III. Critérios de Aprovação

a. **Aprovação Automática:** Risco Baixo e documentos válidos.

b. **Aprovação com Restrições:** Risco Médio, com imposição de controles adicionais (Ex: Limites de acesso à API reduzidos e SLAs mais rigorosos).

c. **Aprovação pelo Comitê:** Obrigatória para Risco Alto, Parceiros Estratégicos e casos com histórico de restrições superadas.

MONITORAMENTO CONTÍNUO

Institui-se a obrigação de monitoramento de performance e conformidade contínuo.

I. Atualização Cadastral

a. **Periodicidade:** Risco Baixo: Anual; Risco Médio: Semestral; Risco Alto/Estratégicos: Trimestral.

b. **Gatilhos para Atualização:** Mudança na estrutura societária, vencimento de certificações de segurança (ISO/PCI), surgimento de restrições financeiras ou Incidentes de Segurança/Conformidade.

II. Monitoramento de Performance (Indicadores Críticos)

a. **Indicadores de Risco:** Envolvimento em processos judiciais, problemas de Segurança da Informação (ex: vulnerabilidades não corrigidas), e descumprimento de obrigações contratuais.

PARCEIROS ESTRATÉGICOS E CRÍTICOS

Dispõem-se procedimentos específicos para parceiros de maior risco.

I. Definição e Categorias

a. **Parceiros Tecnológicos Críticos:** Integradores com acesso amplo a APIs, Desenvolvedores de soluções White Label e Provedores de infraestrutura crítica.

II. Procedimentos Específicos

a. **Due Diligence Reforçada:** Exigência de Demonstrações financeiras auditadas, Certificações de segurança (ISO 27001, PCI-DSS) e Planos de Continuidade de Negócios (PCN).

b. **Aprovação:** Aprovação obrigatória do Comitê, Parecer técnico e jurídico fundamentado e estabelecimento de SLAs rigorosos (para downtime).

CONTROLES ESPECIAIS

Determina-se salvaguardas adicionais para parceiros com acesso a informações críticas.

I. Controles de Acesso (Segurança Cibernética)

a. **Princípios:** Menor privilégio necessário, Segregação de ambientes (Produção/Desenvolvimento) e Autenticação Multifator obrigatória.

II. Monitoramento de Sistemas

a. **Controles Técnicos:** Monitoramento de acessos em tempo real (Logs) e Análise de comportamento de usuário (para detectar anomalias no acesso a APIs).

III. Controles Contratuais (Transferência de Risco)

a. **Cláusulas Obrigatórias:** Conformidade com regulamentações (LGPD, PLD), Direito de auditoria pela MarchaPay sobre os sistemas do parceiro e Responsabilidade por danos e incidentes (indenização Hold Harmless).

IV. Gestão de Parceiros Estratégicos (Risco de Saída)

a. **Planos de Transição e Saída:** Deve ser estabelecido um plano de contingência para o encerramento da parceria, garantindo a migração segura dos dados e a continuidade da operação.

SISTEMA DE INFORMAÇÕES

I. Gestão de Documentos

a. **Segurança:** Criptografia de dados, Controle de acesso e Retenção de documentos pelo prazo legal (mínimo de 5 anos após o término da parceria).

II. Relatórios Gerenciais

a. **Relatórios de Risco:** Distribuição por classificação, Alertas gerados e Incidentes de conformidade (PLD/LGPD) para a Alta Administração.

TREINAMENTO E CAPACITAÇÃO

Impõe-se programa anual de formação contínua.

I. Programa de Treinamento

a. **Público-Alvo:** Equipe de Parcerias e Canais, Área de Compliance e Equipe de TI (para Integrações).

II. Conteúdo Específico

a. **Compliance:** Análise avançada de riscos (identificação de red flags PLD/FT).

b. **Parcerias e Canais:** Aspectos legais contratuais e Procedimentos de seleção.

AUDITORIA E CONTROLES INTERNOS

Prevê-se a realização de auditorias internas periódicas.

I. Auditoria Interna

a. **Escopo:** Efetividade dos controles KYP, Qualidade da documentação e Adequação da classificação de risco.

b. **Periodicidade:** Auditoria completa anual e revisões por amostragem trimestrais.

II. Controles de Segunda Linha

a. **Compliance:** Monitoramento independente, Testes de efetividade e Análise de indicadores de risco.

DISPOSIÇÕES FINAIS

I. Vigência e Revisão

Esta política entra em vigor na data de sua aprovação pela Diretoria e sua revisão ordinária é obrigatória em periodicidade mínima anual.

II. Responsabilidades e Sanções

a. **Diretoria:** Responder pela efetividade da política.

b. **Parceiros:** O descumprimento pode resultar em Suspensão temporária da parceria e Rescisão contratual, além de Aplicação de penalidades contratuais (multas por descumprimento de SLA/Segurança).

III. Documentos Relacionados

a. Política de Prevenção à Lavagem de Dinheiro (PLD).

b. Política de Segurança da Informação e Cibernética.

c. Política de Privacidade e Proteção de Dados Pessoais.

d. Código de Ética e Conduta.