VILLET PAG MANUAL CONHEÇA SEU CLIENTE (KYC / KYM)

Identificação • Qualificação • Due Diligence • Monitoramento

Empresa	VILLET PAG SOLUÇÕES DE PAGAMENTOS S.A.
CNPJ	53.183.086/0001-00
Documento	Manual KYC/KYM — versão 1.0
Data de elaboração	15 de Agosto de 2025
Aprovação	Equipe Jurídica
Responsável pela aprovação	Equipe Jurídica

DOCUMENTO INTERNO — USO CONTROLADO

CONTROLE DO DOCUMENTO

Este Manual estabelece os parâmetros internos para identificação, qualificação, validação, classificação, aprovação, monitoramento e revisão de clientes, representantes, sócios, administradores, beneficiários finais e parceiros, conforme o modelo de negócio e os serviços efetivamente oferecidos pela VILLET PAG SOLUÇÕES DE PAGAMENTOS S.A.

A versão deverá ser revisada pelo menos anualmente e sempre que houver alteração relevante de atividade, produto, canal, risco, estrutura societária ou requisito legal/regulatório. A entrada em vigor depende de aprovação formal.

1. OBJETIVO E ABRANGÊNCIA

1.1. O presente Manual Conheça Seu Cliente (KYC — Know Your Customer) e Conheça Seu Parceiro (KYP/KYM — Know Your Partner/Merchant) tem por objetivo estabelecer diretrizes e procedimentos para conhecer, verificar e manter atualizadas as informações das pessoas e empresas que se relacionem com a Instituição.

1.2. Os procedimentos buscam prevenir o uso indevido dos produtos, serviços, canais, tecnologia ou relações comerciais para fraude, lavagem de dinheiro, financiamento do terrorismo, financiamento da proliferação de armas de destruição em massa, corrupção, evasão de controles, ilícitos ou outras atividades incompatíveis.

1.3. Aplica-se, conforme pertinência, às áreas de Diretoria, Comercial, Credenciamento/Onboarding, Operações, Atendimento, Tecnologia, Segurança da Informação, Compliance/PLD-FTP, Risco, prestadores de serviços e parceiros que participem da jornada cadastral, operacional ou de relacionamento.

1.4. Os controles devem ser proporcionais à natureza do produto ou serviço, ao canal, à localização, ao perfil do cliente, ao volume esperado, à complexidade societária e aos riscos identificados. Este Manual não presume autorização regulatória, licença ou atividade específica não confirmada.

2. BASE LEGAL E REFERENCIAL

2.1. Os procedimentos deverão observar, conforme aplicabilidade ao modelo de negócio e ao enquadramento da Instituição:

Lei nº 9.613/1998 e alterações — prevenção à lavagem de dinheiro e ocultação de bens, direitos e valores;

Lei nº 13.260/2016 — terrorismo e financiamento do terrorismo;

Lei nº 12.865/2013 — arranjos e instituições de pagamento, quando aplicável;

Lei nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD);

Normas e orientações do Banco Central do Brasil, COAF e demais autoridades competentes, quando aplicáveis;

Normas relativas a sanções nacionais e internacionais, incluindo as implementadas no ordenamento brasileiro;

Contratos, políticas internas de PLD-FTP, prevenção a fraude, segurança da informação, privacidade e gestão de risco.

2.2. A área responsável deverá manter o referencial regulatório atualizado e confirmar a aplicabilidade de cada requisito ao status jurídico-regulatório e às atividades efetivamente desempenhadas pela Instituição.

3. DEFINIÇÕES

Cliente/Estabelecimento: pessoa física ou jurídica que contrata, utiliza ou se relaciona com produto, serviço, plataforma ou solução disponibilizada pela Instituição.

Representante legal: pessoa autorizada a agir em nome da pessoa jurídica, conforme documentos societários, procurações ou poderes válidos.

Beneficiário Final (UBO): pessoa natural que, em última instância, detém, controla ou exerce influência significativa sobre a entidade, direta ou indiretamente; a identificação deve seguir os critérios aplicáveis e os procedimentos internos.

PEP: pessoa exposta politicamente, bem como familiares, estreitos colaboradores e pessoas relacionadas conforme legislação e regulamentação aplicáveis.

Due Diligence (DD): procedimento de diligência para validação cadastral, societária, reputacional, financeira e de risco.

Due Diligence Reforçada (DDR/EDD): diligência adicional aplicada a relações ou operações de maior risco.

Abordagem Baseada em Risco (ABR): alocação de controles e recursos de acordo com o risco identificado.

Mídia negativa: informações públicas confiáveis que possam indicar risco de fraude, ilícitos, integridade, reputação ou incompatibilidade de atividade.

Sanções/Restrições: listas e medidas restritivas cuja verificação seja exigida por lei, norma ou política interna.

4. PRINCÍPIOS E DIRETRIZES

Conhecer o cliente antes do início do relacionamento e validar informações essenciais.

Não aprovar cadastro com identidade, poderes de representação, atividade ou origem/fluxo financeiro sem validação suficiente.

Aplicar controles proporcionais ao risco e documentar as decisões.

Identificar a estrutura societária até as pessoas naturais beneficiárias finais, quando aplicável.

Verificar coerência entre atividade declarada, canais de venda, produtos/serviços, faturamento, volume, ticket médio e fluxo financeiro esperado.

Não permitir que a área comercial contorne critérios de risco, exigências documentais ou decisão de recusa.

Restringir acesso aos dados cadastrais a pessoas com necessidade legítima de acesso.

Registrar evidências das consultas, validações, aprovações, alertas e medidas adotadas.

5. PAPÉIS E RESPONSABILIDADES

Diretoria: aprovar o Manual e suas revisões; assegurar recursos e independência adequados aos controles; decidir ou delegar formalmente decisões de risco elevado.

Compliance/PLD-FTP/Risco: definir critérios; analisar casos complexos e de alto risco; avaliar PEP, sanções, mídia negativa e alertas; manter trilhas de auditoria; propor medidas mitigadoras; recomendar aprovação, restrição ou recusa.

Comercial/Relacionamento: coletar informações e documentos; fornecer informações completas; não prometer aprovação antes da conclusão das verificações; não interferir indevidamente em decisões de risco.

Onboarding/Credenciamento: conferir documentação, executar validações, registrar evidências, encaminhar pendências e garantir que o cadastro esteja completo antes de ativação.

Operações/Atendimento: monitorar inconsistências e mudanças de perfil; encaminhar alertas; cumprir determinações de restrição, suspensão ou revisão.

Tecnologia/Segurança da Informação: proteger dados e sistemas, controlar acessos, manter logs e apoiar ferramentas de validação e monitoramento.

Colaboradores e parceiros: cumprir o Manual, realizar treinamentos e reportar suspeitas, inconsistências ou violações.

6. FLUXO DE KYC/KYM — ETAPAS MÍNIMAS

1. Recebimento da solicitação e identificação do produto/serviço pretendido.
2. Coleta dos dados e documentos obrigatórios de acordo com o tipo de cliente.
3. Validação de identidade, CNPJ/CPF, situação cadastral, endereço, representação e poderes.
4. Verificação de estrutura societária e identificação de beneficiários finais.
5. Pesquisa em bases de PEP, sanções, mídia negativa e outras fontes de risco pertinentes.
6. Validação de atividade, site, canais, produtos, modelo de negócio e fluxo operacional.
7. Avaliação de capacidade financeira e estimativa de volume, ticket médio e frequência.
8. Classificação de risco e aplicação de diligência padrão ou reforçada.
9. Decisão formal: aprovado, aprovado com condições/limites, pendente ou recusado.
10. Registro das evidências, responsável, data, justificativa e eventuais condições.
11. Ativação somente após cumprimento dos requisitos aplicáveis e aprovação registrada.

7. DOCUMENTOS E INFORMAÇÕES — PESSOA JURÍDICA

7.1. Documentação padrão, conforme tipo societário, risco e produto:

Razão social, nome fantasia, CNPJ e comprovante de situação cadastral atualizado;

Contrato/estatuto social e alterações, ou versão consolidada vigente;

Comprovante de endereço da sede e, quando relevante, dos locais de operação;

Identificação dos sócios, administradores e representantes legais;

Quadro societário atualizado e documentos que permitam identificar beneficiários finais;

Documento oficial de identificação e CPF dos representantes, administradores e UBOs relevantes;

Procuração, se o cadastro for conduzido por procurador, com poderes e validade verificados;

Dados da conta bancária de liquidação/recebimento, verificando titularidade e compatibilidade;

Site, domínio, redes sociais, canais de venda, plataforma/checkout e descrição dos produtos/serviços;

Descrição do modelo de negócio, origem dos clientes, forma de entrega e política de reembolso, quando pertinente;

Faturamento atual/estimado, volume mensal previsto, ticket médio, quantidade de transações e sazonalidade;

Origem dos recursos e finalidade do relacionamento, quando exigido pelo risco ou produto;

Licenças, autorizações ou registros específicos exigidos para atividade, quando aplicável.

7.2. Documentos adicionais poderão ser solicitados de acordo com o risco, segmento, estrutura societária, divergências, atividade regulada, volume esperado ou necessidade de esclarecimento.

8. PESSOA NATURAL, REPRESENTANTES E SÓCIOS

8.1. Quando pessoa física for cliente ou quando houver necessidade de identificar sócios, administradores, representantes e beneficiários finais, deverão ser coletadas e validadas informações suficientes para confirmar identidade e qualificação.

Nome completo e nome social, quando informado e pertinente;

CPF e documento oficial de identificação válido;

Data de nascimento e nacionalidade, quando necessárias;

Endereço e dados de contato;

Profissão/ocupação e vínculo com a empresa;

Poderes de representação e evidência documental;

Informações de PEP e relações relevantes, conforme aplicabilidade;

Validação de autenticidade documental, prova de vida ou biometria, quando o canal e o risco justificarem e houver ferramenta adequada.

9. BENEFICIÁRIO FINAL E ESTRUTURA SOCIETÁRIA

9.1. A Instituição deverá identificar e compreender a estrutura de propriedade e controle da pessoa jurídica, incluindo cadeias societárias, participações indiretas, acordos de controle e pessoas naturais que exerçam influência significativa.

9.2. O critério de participação societária utilizado para identificar UBO deverá ser compatível com a legislação/regulação aplicável e com a política interna vigente. A participação abaixo do critério percentual não afasta a análise de controle de fato ou influência significativa.

9.3. Estruturas complexas, opacas, com jurisdições de risco, sócios nominais sem explicação ou impossibilidade de identificar o beneficiário final deverão ser submetidas à análise reforçada e poderão resultar em recusa.

10. VALIDAÇÕES E PESQUISAS EXTERNAS

10.1. As verificações deverão utilizar fontes confiáveis, oficiais ou contratadas, de acordo com a disponibilidade e o risco:

Receita Federal e bases oficiais de situação cadastral;

Junta Comercial, documentos societários e registros públicos pertinentes;

Bases de PEP e sanções/restrições aplicáveis;

Mídia negativa e fontes públicas para notícias relacionadas a fraude, crimes financeiros, corrupção ou integridade;

Bases antifraude, de identidade e validação documental, quando contratadas;

Pesquisa de site, domínio, canais comerciais, catálogo, checkout e coerência da atividade;

Verificação de titularidade e compatibilidade da conta de liquidação;

Consultas de crédito ou risco, quando legalmente permitidas e necessárias.

10.2. Resultado de pesquisa deverá ser registrado com data, fonte, identificação pesquisada e conclusão. Homônimos devem ser tratados mediante análise de identificadores, sem atribuir automaticamente risco a pessoa não confirmada.

11. PEP, SANÇÕES E MÍDIA NEGATIVA

11.1. Identificação de PEP, pessoa relacionada, correspondência em lista de sanções ou mídia negativa relevante deverá gerar análise específica e registro da conclusão.

11.2. A condição de PEP, por si só, não determina recusa automática. Deve ser aplicada diligência reforçada, avaliação de risco e aprovação por autoridade competente, conforme regra interna e legislação aplicável.

11.3. Correspondências em listas de sanções devem ser confirmadas por identificadores e tratadas conforme as obrigações legais e procedimentos de bloqueio/reporte aplicáveis. Não se deve liberar relacionamento quando houver impedimento legal confirmado.

11.4. Mídia negativa deve ser avaliada quanto à confiabilidade, atualidade, gravidade, conexão com a pessoa pesquisada, desfecho conhecido e relevância para o risco do relacionamento.

12. MODELO DE NEGÓCIO, ATIVIDADE E FLUXO FINANCEIRO

12.1. A Instituição deverá compreender o negócio do cliente e a finalidade do relacionamento, incluindo:

Produtos e serviços vendidos e respectivos preços;

Público-alvo e canais de aquisição;

Site, checkout, marketplaces, redes sociais e canais de atendimento;

Processo de venda, entrega, cancelamento e reembolso;

Origem dos pagamentos, pagadores, recebedores e destino dos recursos;

Estimativa de volume mensal, número de transações, ticket médio e sazonalidade;

Uso de terceiros, afiliados, intermediários ou plataformas;

Compatibilidade entre atividade declarada, documentação e operação observada.

12.2. Atividade não verificável, produtos proibidos, oferta enganosa, ausência de evidências de entrega, discrepância entre atividade declarada e real, ou fluxo financeiro sem justificativa deverão ser escalados para análise.

13. CLASSIFICAÇÃO DE RISCO

13.1. A classificação deverá considerar fatores cumulativos e contexto, sem depender exclusivamente de um indicador isolado.

Nível	Indicadores exemplificativos	Tratamento
Baixo	Cadastro consistente; atividade e	Diligência padrão; revisão
Médio	Volume elevado ou crescente;	Validações adicionais; limites
Alto	PEP/relacionados; estrutura	Diligência reforçada; aprovação

13.2. Os fatores, pesos e critérios de classificação deverão ser documentados em matriz interna e calibrados com base no perfil real da operação. A classificação deve ser registrada com justificativa.

14. DUE DILIGENCE REFORÇADA (EDD)

14.1. A diligência reforçada poderá incluir, conforme necessidade:

Documentos societários adicionais e organograma societário até o UBO;

Comprovação e esclarecimentos sobre origem dos recursos e patrimônio, quando pertinente;

Evidências adicionais de atividade, produtos, entrega, contratos, fornecedores ou canais;

Verificação independente de informações relevantes e análise aprofundada de mídia negativa;

Entrevista ou contato de validação com representante autorizado;

Revisão de capacidade financeira e justificativa de volume/ticket esperado;

Aprovação por Compliance/PLD-FTP e/ou Diretoria conforme alçada;

Definição de limites, condicionantes e prazo para reavaliação.

14.2. A impossibilidade de sanar dúvidas relevantes ou identificar as partes relacionadas poderá resultar em não aprovação, suspensão do onboarding ou encerramento, conforme análise e base legal/contratual.

15. APROVAÇÃO, PENDÊNCIAS E RECUSA

15.1. O resultado da análise será formalizado como: (i) aprovado; (ii) aprovado com condições; (iii) pendente de documentos/esclarecimentos; ou (iv) recusado.

15.2. Aprovação condicionada deverá indicar claramente as condições, limites, responsável, prazo e mecanismo de acompanhamento. Não deverá haver ativação antes do cumprimento das condições consideradas essenciais.

15.3. Recusas e decisões excepcionais devem registrar os motivos, evidências, responsáveis e alçada. A comunicação ao cliente deve preservar informações sigilosas e não revelar eventual comunicação a autoridades.

16. MONITORAMENTO CONTÍNUO E REVISÃO CADASTRAL

16.1. Após a aprovação, o cliente será monitorado em relação à atividade, perfil transacional, alterações cadastrais, risco e cumprimento das condições.

Alteração brusca de volume, frequência ou ticket médio;

Transações incompatíveis com o ramo, perfil ou capacidade declarada;

Concentração incomum de transações, pagamentos ou destinos;

Aumento de estornos, chargebacks, reclamações, MED ou indicadores de fraude;

Mudanças de sócios, administradores, UBO, endereço, domínio ou atividade;

Sinais de transações simuladas, uso indevido de credenciais, identidade ou canais;

Informações públicas negativas novas ou alertas em bases de risco;

Descumprimento de limites, condições ou solicitações de atualização.

16.2. A revisão cadastral poderá ser periódica e/ou acionada por eventos. A periodicidade deve ser definida na matriz de risco, com maior frequência para alto risco. Como parâmetro interno sugerido, sujeito à aprovação: alto risco — revisão a cada 6 meses; médio — a cada 12 meses; baixo — a cada 24 meses. Revisões extraordinárias devem ocorrer quando houver gatilho relevante.

16.3. A ausência de atualização, quando essencial, poderá resultar em restrição, suspensão ou encerramento após análise e comunicação apropriada, conforme contrato e regras aplicáveis.

17. ALERTAS, INVESTIGAÇÃO E ESCALONAMENTO

17.1. Alertas cadastrais, transacionais, antifraude ou reputacionais deverão ser registrados e analisados por área competente. A análise deverá documentar:

Origem do alerta, data, cliente e operações envolvidas;

Dados e documentos consultados;

Explicação obtida e consistência com o perfil;

Análise de risco e decisão;

Medidas adotadas (monitoramento, solicitação de documentos, limites, suspensão ou encerramento);

Responsável e aprovador, quando exigido.

17.2. Quando houver suspeita relevante, o caso será encaminhado à área responsável por PLD-FTP para avaliação das medidas e comunicações cabíveis. O tratamento deve preservar o sigilo e evitar comunicação indevida ao cliente sobre reporte às autoridades.

18. FRAUDE, MED, CHARGEBACK E DISPUTAS

18.1. Indicadores de fraude, MED, chargeback, reclamações, contestação e disputas serão considerados elementos de risco no KYC/KYM e no monitoramento. Tais indicadores não constituem, isoladamente, conclusão de lavagem de dinheiro ou suspeita legal.

18.2. A Instituição poderá solicitar comprovantes de venda, entrega, atendimento, reembolso, contratos, evidências de consentimento e demais documentos pertinentes, conforme o tipo de operação.

18.3. Recorrência, concentração, padrões anormais, inconsistências ou ausência de documentação serão escalados para análise de risco e, quando aplicável, PLD-FTP.

19. SUSPENSÃO, RESTRIÇÃO E ENCERRAMENTO

19.1. Conforme contrato, legislação e análise de risco, poderão ser aplicadas medidas como solicitação de esclarecimentos, revisão de limites, restrição de funcionalidades, suspensão temporária, não aprovação ou encerramento.

19.2. As medidas deverão ser proporcionais, documentadas, aprovadas por alçada adequada e executadas de acordo com os procedimentos internos e obrigações legais. O tratamento de valores pendentes deverá observar contratos, regras aplicáveis e determinações de autoridades.

20. PROTEÇÃO DE DADOS, ACESSO E GUARDA

20.1. Dados e documentos deverão ser tratados para finalidades legítimas, com base legal adequada, minimização, segurança, controle de acesso e transparência compatível com a LGPD.

20.2. A Instituição manterá trilhas de auditoria e registros das consultas, decisões e documentos, pelo prazo previsto em legislação, regulamentação, contrato e tabela interna de retenção. Prazos específicos deverão ser confirmados pela área jurídica/Compliance.

20.3. O acesso será concedido por necessidade de trabalho e revisto periodicamente. Dados não deverão ser compartilhados por canais não autorizados ou armazenados em dispositivos/ambientes sem controles adequados.

21. TREINAMENTO

21.1. Colaboradores envolvidos em onboarding, relacionamento, operações, risco, atendimento, tecnologia e PLD-FTP deverão receber treinamento inicial e periódico.

21.2. O conteúdo incluirá identificação documental, UBO, PEP, sanções, mídia negativa, sinais de alerta, abordagem baseada em risco, LGPD, escalonamento e registro de evidências. A participação deverá ser registrada.

22. CONTROLES, TESTES E REVISÃO

22.1. A efetividade do KYC deverá ser avaliada por indicadores, amostragens, testes de qualidade e análise de falhas. Achados devem gerar plano de ação com responsável, prazo e validação de conclusão.

Percentual de cadastros completos e pendências;

Tempo de onboarding por nível de risco;

Percentual de clientes com UBO identificado/validado;

Alertas, casos escalonados, aprovações excepcionais e recusas;

Clientes com revisão cadastral vencida;

Falhas de validação, incidentes e ações corretivas.

23. DISPOSIÇÕES FINAIS E APROVAÇÃO

23.1. Casos omissos serão encaminhados à área de Compliance/PLD-FTP e, quando necessário, à Diretoria.

23.2. Este Manual entra em vigor após aprovação formal. A aprovação deverá ser registrada e a versão vigente disponibilizada às áreas pertinentes.

VILLET PAG SOLUÇÕES DE PAGAMENTOS S.A.CNPJ: 53.183.086/0001-00

Ossian Vitor Silva DantasPresidente

ANEXO I — CHECKLIST DE ONBOARDING KYC/KYM

☐ Identificação da empresa e CNPJ validado

☐ Situação cadastral consultada

☐ Contrato/estatuto social vigente analisado

☐ Quadro societário e organograma obtidos

☐ UBO(s) identificados e validados

☐ Representante legal e poderes validados

☐ Documentos de sócios/representantes coletados conforme aplicabilidade

☐ Endereço e contatos validados

☐ Conta de liquidação e titularidade conferidas

☐ Atividade, site, canais, produtos e fluxo operacional compreendidos

☐ Faturamento, TPV, ticket médio e volume esperado documentados

☐ PEP/sanções/mídia negativa pesquisados

☐ Risco atribuído e justificativa registrada

☐ Diligência reforçada aplicada, se necessário

☐ Decisão e alçada registradas

☐ Condições/limites definidos, se houver

☐ Cadastro aprovado antes da ativação

☐ Evidências e trilha de auditoria arquivadas

ANEXO III — MATRIZ DE RESPONSABILIDADE (RACI SIMPLIFICADA)

Etapa	Execução	Revisão/Controle	Aprovação
Coleta cadastral	Comercial/Onboarding	Onboarding	Conforme alçada
Validação documental	Onboarding	Risco/Compliance	Conforme alçada
UBO e estrutura	Onboarding	Compliance/PLD-FTP	Alçada superior se risco
PEP/sanções/mídia	Onboarding/Sistema	Compliance/PLD-FTP	Conforme política
Classificação de risco	Onboarding/Risco	Compliance/PLD-FTP	Conforme matriz
Cliente alto risco	Compliance/PLD-FTP	Diretoria ou alçada	Diretoria/alçada formal
Monitoramento	Operações/Sistemas	Risco/Compliance	Conforme gatilho
Suspensão/	Operações	Compliance/Jurídico, se	Conforme

ANEXO IV — REGISTRO DE REVISÕES

Versão	Data	Descrição	Aprovação
1.0	15/08/2025	Emissão inicial do	Pendente