VILLET PAG SOLUÇÕES DE PAGAMENTOS S.A

POLÍTICA INSTITUCIONAL DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (PLD-FTP)

CNPJ: 53.183.086/0001-00

Classificação da Informação: PúblicaÁrea Responsável: ComplianceSociedades Aplicáveis: VILLET PAG SOLUÇÕES DE PAGAMENTOS S.AData da Aprovação: 15/08/2025Aprovadores: Conselho e Diretoria VILLET PAG SOLUÇÕES DE PAGAMENTOS S.A

ÍNDICE

1. Aspecto Geral e Objetivo da Política

2. Abrangência

3. Vigência, Aprovação e Atualizações

4. Bases Regulatórias e Normativas

5. Definições e Termos Essenciais

6. Princípios Norteadores

7. Governança e Estrutura de Responsabilidades (3 Linhas de Defesa)

8. Abordagem Baseada no Risco (ABR) – Metodologia Completa

9. Identificação, Cadastro, KYC/KYB/KYS/KYP e Due Diligence

10. Avaliação de Risco de Clientes, Parceiros, Produtos e Canais

11. Monitoramento de Transações e Modelos de Alerta (AML Monitoring)

12. Procedimentos de Investigação Interna

13. Comunicação de Operações ao COAF

14. Controles Internos, Indicadores e Testes de Efetividade

15. Gestão de Registros, Sigilo e Proteção de Dados

16. Treinamento, Capacitação e Certificações Internas

17. Auditoria Interna e Externa

18. Penalidades, Medidas Disciplinares e Ações Corretivas

19. Melhoria Contínua e Revisões Periódicas

20. Disposições Finais

21. Anexo – Termo de Ciência e Compromisso

1. ASPECTO GERAL E OBJETIVO DA POLÍTICA

A VILLET PAG SOLUÇÕES DE PAGAMENTOS S.A instituição atuante no setor de soluções de pagamentos, credenciamento de estabelecimentos comerciais, captura, processamento e liquidação de transações por meio de maquininhas de cartão (POS, TEF, SmartPOS, E-commerce e pagamentos digitais), adota esta Política com o objetivo de estabelecer um programa robusto,

estruturado e eficaz para prevenção, detecção e combate à lavagem de dinheiro, financiamento do terrorismo, fraudes, corrupção, práticas ilícitas e uso indevido dos seus produtos.

A Política reflete:

As melhores práticas de instituições financeiras consolidadas, incluindo modelos de adquirentes líderes do mercado;

As recomendações do GAFI/FATF, incluindo metodologia de risco e efetividade;

A conformidade integral com COAF, Banco Central e demais órgãos reguladores;

O compromisso institucional com um ambiente seguro, ético e sustentável.

Esta Política orienta decisões estratégicas, define responsabilidades internas, padroniza procedimentos e integra-se com o Manual Operacional de PLD/FT, contendo os passo a passo específicos.

2. ABRANGÊNCIA

Aplica-se a todos os:

Colaboradores da empresa;

Diretores e gestores;

Terceirizados, consultores, prestadores e parceiros;

Correspondentes, representantes comerciais e prepostos;

Agentes de captura e sub-credenciadores ligados à operação;

Unidades, sistemas, canais, produtos e processos internos.

Abrange todo o ciclo operacional:

Credenciamento de estabelecimentos comerciais;

Onboarding digital;

Análise cadastral, societária e documental;

Classificação de risco (risk scoring);

Captura de transações;

Processamento e liquidação;

Gestão de chargebacks;

Relacionamento e suporte;

Encerramento de clientes.

3. VIGÊNCIA, APROVAÇÃO E ATUALIZAÇÕES

Esta Política:

Entra em vigor na data de aprovação pela Alta Administração;

Possui vigência por prazo indeterminado;

Deve ser revisada anualmente, ou sempre que houver:

Alterações regulatórias relevantes;

Mudanças no modelo de negócio;

Recomendações de auditoria;

Evolução tecnológica;

Riscos emergentes.

A revisão deve ser documentada, atualizada em repositório oficial e aprovada pela Diretoria.

4. BASES REGULATÓRIAS E NORMATIVAS

Lei nº 9.613/1998 (lavagem de dinheiro)

Lei nº 12.846/2013 (anticorrupção)

Lei nº 13.260/2016 (terrorismo)

Lei nº 13.709/2018 (LGPD)

Lei nº 13.810/2019 (sanções internacionais)

Circular BCB nº 3.978/2020

Resolução BCB nº 80/2021

Resolução BCB nº 119/2021

Normativos COAF aplicáveis ao setor de pagamentos

Recomendações internacionais GAFI/FATF

Padrões Wolfsberg e Basel

5. DEFINIÇÕES E TERMOS ESSENCIAIS

ABR – Abordagem Baseada em Riscos

Metodologia que orienta a empresa a direcionar esforços de prevenção conforme o risco identificado em clientes, parceiros, produtos, canais, segmentos (MCC) e regiões geográficas. A

ABR garante proporcionalidade na alocação de recursos, priorizando áreas mais expostas a riscos de lavagem de dinheiro, financiamento do terrorismo e fraudes.

AIR – Avaliação Interna de Riscos

Processo pelo qual a empresa identifica, mensura, classifica e documenta os riscos inerentes e residuais relacionados à PLD/FT. A AIR considera fatores como:

Avaliação de Efetividade

Processo regulatório que verifica se os controles internos, sistemas de monitoramento, políticas e procedimentos realmente funcionam na prática. Mede a eficiência, precisão e qualidade das medidas adotadas, garantindo aderência às normas do COAF e BACEN.

BCB – Banco Central do Brasil

Autoridade reguladora responsável por supervisionar instituições financeiras e empresas de pagamento, incluindo adquirentes, subcredenciadores e instituições que processam e liquidam transações.

Beneficiário Final (UBO – Ultimate Beneficial Owner)

Pessoa natural que exerce o controle final, direto ou indireto, sobre uma pessoa jurídica cliente. Inclui sócios ocultos, controladores de fato e pessoas que, mesmo sem constar formalmente no contrato social, exercem influência decisória relevante.

Cliente

Pessoa física ou jurídica que utiliza a infraestrutura de pagamentos da empresa para processar transações. Inclui estabelecimentos físicos, digitais, MEIs, autônomos, subcredenciadores e plataformas integradas.

COAF – Conselho de Controle de Atividades Financeiras

Unidade de inteligência financeira brasileira responsável por receber, examinar e identificar atividades suspeitas comunicadas pelas empresas obrigadas, incluindo empresas de pagamento.

Colaboradores

Inclui todos os empregados, estagiários, jovens aprendizes e demais profissionais contratados diretamente pela empresa.

CSNU – Conselho de Segurança das Nações Unidas

Órgão emissor de listas de sanções internacionais, que devem ser observadas pela empresa no processo de onboarding e monitoramento.

Diretoria / Alta Administração

Órgãos decisórios máximos da empresa, responsáveis por assegurar recursos, aprovar políticas e supervisionar o Programa de PLD/FT.

Financiamento do Terrorismo (FT)

Ato de prover, receber, direcionar ou movimentar recursos (lícitos ou ilícitos) com a finalidade de apoiar atividades terroristas. Inclui ocultação de origem, repasses fragmentados e uso de empresas de fachada.

Financiamento à Proliferação de Armas de Destruição em Massa

Movimentação ou aporte de recursos destinados, direta ou indiretamente, ao desenvolvimento, aquisição ou disseminação de armas químicas, biológicas ou nucleares.

KYC – Know Your Customer (Conheça seu Cliente)

Processo de identificação, verificação e validação de clientes durante o onboarding, incluindo coleta documental, identificação do UBO, análise de risco e classificação inicial.

KYE – Know Your Employee (Conheça seu Funcionário)

Processo pelo qual a empresa monitora, verifica e avalia riscos relacionados a colaboradores.

KYP – Know Your Partner (Conheça seu Parceiro)

Diligência aplicada a parceiros comerciais, como subcredenciadores, correspondentes, plataformas integradas e agentes comerciais.

KYS – Know Your Supplier (Conheça seu Fornecedor)

Processo de avaliação de fornecedores que podem impactar a operação, especialmente aqueles ligados à tecnologia, captura e processamento dos pagamentos.

Lavagem de Dinheiro (LD)

Processo que envolve ocultação, dissimulação ou reintegração de recursos ilícitos na economia formal, normalmente dividida em três fases: colocação, ocultação e integração.

Canal de Denúncias

Ferramenta para comunicação de condutas suspeitas ou violação de regras. Deve permitir anonimato, preservar o denunciante e garantir tratamento independente de cada denúncia.

Parceiros

Entidades externas que prestam serviços complementares ou essenciais para a operação da empresa, como agentes de captura, subcredenciadores, correspondentes e integradores.

PEP – Pessoa Exposta Politicamente

Agentes públicos nacionais ou estrangeiros, bem como seus familiares e estreitos colaboradores, que exigem análise reforçada (EDD) e monitoramento contínuo.

PLD/FT / PLD-FTP

Programa e conjunto de práticas destinadas à prevenção à lavagem de dinheiro, financiamento do terrorismo e financiamento da proliferação de armas de destruição em massa.

Prestadores de Serviços Terceirizados (Terceiros)

Empresas ou indivíduos contratados para prestar serviços à empresa, especialmente quando atuam em processos sensíveis (ex.: onboarding digital, manutenção de POS, logística, tecnologia).

Programa de PLD/FT

Conjunto estruturado de políticas, processos, tecnologias, governança, controles, sistemas de monitoramento, indicadores, linhas de defesa e práticas adotadas para prevenir LD/FT.

Política de PLD/FT

Documento institucional que estabelece os compromissos estratégicos e diretrizes gerais adotadas pela empresa.

Perfil dos clientes;

MCC e ramo de atividade;

Nível de exposição do produto;

Volume transacional;

Canais de captura;

Histórico de alertas;

Controles existentes.

A AIR define o apetite de risco da empresa e fundamenta a criação dos controles do Programa de PLD/FT.

6. PRINCÍPIOS NORTEADORES

ÉTICA E TRANSPARÊNCIA

Definição: atuação pautada pela integridade, boa-fé, clareza e prestação de contas em todas as relações comerciais e operacionais.

Implicações operacionais:

Registro completo e legível de todas as decisões de compliance;

Justificativas documentadas para recusas, bloqueios e encerramentos;

Política de comunicação interna/externa sobre incidentes e medidas adotadas.

Exemplos práticos: publicar procedimentos de reporte interno, manter trilhas de auditoria (audit trails) em todas as análises.

Responsabilidades: Compliance (assegurar padrões), Operações (manter evidências), Jurídico (orientar comunicações).

KPIs sugeridos: percentual de casos com documentação completa; tempo médio de decisão justificada.

ABORDAGEM BASEADA NO RISCO (ABR)

Definição: priorização de controles e recursos conforme probabilidade e impacto dos riscos identificados.

Implicações operacionais:

Definição de critérios objetivos para classificação (score);

Políticas de diligência diferenciada (CDD / EDD) conforme nível de risco;

Revisão periódica de parâmetros e tolerâncias.

Exemplos práticos: aplicar limites transacionais dinâmicos a MIDs com score alto; exigir EDD para PEPs e certos MCCs.

Responsabilidades: AIR/Compliance (definir metodologia), TI (implementar scoring), Operações (executar medidas).

KPIs sugeridos: percentil de alertas por categoria de risco; redução de falsos positivos após tuning.

PREVENÇÃO ATIVA

Definição: medidas proativas que antecipam e evitam riscos antes que se concretizem.

Implicações operacionais:

Due diligence pré-lançamento em novos produtos e integrações (NPP – New Product Process);

Testes de cenário e stress test de regras de monitoramento;

Rotinas de revisão preditiva (ex.: análise de tendências de chargeback).

Exemplos práticos: simulação mensal de fraude em novos fluxos de pagamento; checklist de segurança para integrações de parceiros.

Responsabilidades: Produto (avaliar riscos), Risco & Fraude (testes), Compliance (emitir condições).

KPIs sugeridos: número de riscos mitigados antes do lançamento; tempo de resposta a alertas preditivos.

GOVERNANÇA ROBUSTA

Definição: estrutura clara de papéis, atribuições e escalonamentos que assegura supervisão, independência e responsabilização.

Implicações operacionais:

Definição formal das 3 linhas de defesa;

Políticas de alçada e critérios de aprovação de EDD/encerramento;

Comitês (risco/compliance) com reuniões periódicas e atas.

Exemplos práticos: regimento interno do Comitê de Risco, matriz de responsabilidades (RACI) para decisões críticas.

Responsabilidades: Alta Administração (aprovação), Compliance (governança), Auditoria (verificação).

KPIs sugeridos: frequência de reuniões do comitê; percentual de ações de compliance concluídas no prazo.

COOPERAÇÃO COM AUTORIDADES

Definição: compromisso de colaboração efetiva, tempestiva e precisa com COAF, BACEN e demais órgãos competentes.

Implicações operacionais:

Canal único e seguro para comunicações oficiais;

Processos internos de validação antes de envio de ROS;

Retenção e fornecimento de evidências conforme solicitação legal.

Exemplos práticos: playbook de comunicação para investigações, lista atualizada de contatos regulatórios.

Responsabilidades: Oficial de PLD/FT (envio), Jurídico (acompanha), Compliance (prepara material).

KPIs sugeridos: tempo médio de resposta a demandas regulatórias; número de solicitações atendidas com evidência completa.

CONTROLE CONTÍNUO E MONITORAMENTO INTELIGENTE

Definição: operação ininterrupta de monitoramento baseada em regras, modelos comportamentais e análises avançadas, com ajustes contínuos.

Implicações operacionais:

Atualização periódica de regras e thresholds;

Integração entre dados de onboarding, transacionais e externos;

Uso de analytics / ML para redução de falsos positivos (quando aplicável).

Exemplos práticos: regras que combinam MCC + ticket médio + frequência para gerar alertas; dashboards com heatmaps de risco geográfico.

Responsabilidades: TI (infraestrutura), Risco/Fraude (parametrização), Compliance (validação).

KPIs sugeridos: taxa de detecção de casos relevantes; proporção de alertas investigados vs. gerados.

PROPORCIONALIDADE E RAZOABILIDADE REGULADORA

Definição: adoção de medidas equilibradas — suficientes para mitigar risco, sem onerar desnecessariamente clientes legítimos.

Implicações operacionais:

Políticas de mitigação que consideram custo/benefício e impacto operacional;

Diferencial de tratamento para microempreendedores e grandes corporates;

Documentação robusta das decisões que adotam medidas restritivas.

Exemplos práticos: limites temporários escalonados (warnings → redução de limites → bloqueio) ao invés de bloqueio imediato; formulários simplificados para MEI com baixo risco.

Responsabilidades: Compliance (definir critérios), Operações (aplicar), Comercial (avaliar impacto cliente).

KPIs sugeridos: número de clientes impactados por medidas proporcionais; taxa de reversão de decisões após EDD.

7. GOVERNANÇA E ESTRUTURA DE RESPONSABILIDADES

A estrutura segue o modelo das Três Linhas de Defesa.

1ª Linha – Áreas Operacionais

Execução de controles;

Tratamento de alertas;

Cumprimento de KYC e onboarding.

2ª Linha – Compliance e PLD/FT

Definição de políticas;

Gestão dos riscos de LD/FT;

Monitoramento independente;

Comunicação ao COAF.

3ª Linha – Auditoria Interna

Avaliação da eficácia do programa;

Testes periódicos;

Recomendações estratégicas.

8. ABORDAGEM BASEADA NO RISCO (ABR) – METODOLOGIA COMPLETA

A metodologia utiliza variáveis específicas do mercado de pagamentos:

Perfil do cliente;

MCC;

Volume transacional;

Chargebacks;

Origem geográfica;

Tipo de canal (POS, e-commerce, link de pagamento);

Perfil societário e UBO.

Classificação: baixo, médio, alto risco.

Clientes de alto risco exigem due diligence reforçada (EDD).

9. IDENTIFICAÇÃO, CADASTRO E DUE DILIGENCE

Abrange:

Coleta documental;

Verificação automatizada;

Validação de identidade e autenticidade;

Análise societária e UBO;

Consultas a listas restritivas;

Compatibilidade entre faturamento e porte.

10. AVALIAÇÃO DE RISCO DE CLIENTES, PARCEIROS E PRODUTOS

Inclui:

Scoring automático;

Revisão periódica;

Análise de mudanças comportamentais;

Avaliação de produtos novos (NPP – New Product Process).

11. MONITORAMENTO DE TRANSAÇÕES

Modelos de alerta incluem:

Picos repentinos de volume;

Estruturação (fracionamento);

Circularidade;

Uso suspeito de múltiplos POS;

MCC incompatível;

Chargebacks excessivos;

Repasses suspeitos.

12. INVESTIGAÇÃO INTERNA

Fluxo:

1. Geração de alerta;
2. Coleta de evidências;
3. Contato sigiloso;
4. Escalonamento ao Compliance;
5. Decisão entre arquivamento, restrição ou reporte.

13. COMUNICAÇÃO AO COAF

O Oficial de PLD/FT reporta:

Operações suspeitas;

Operações automáticas previstas em norma;

Situações de recusa injustificada.

14. CONTROLES INTERNOS E TESTES DE EFETIVIDADE

Incluem:

Indicadores de eficiência do monitoramento;

KPIs e KRIs;

Testes semestrais;

Validação independente.

15. REGISTROS E SIGILO

Documentos são armazenados por 5 anos, com acesso restrito e controles LGPD.

16. TREINAMENTO E CAPACITAÇÃO

Treinamento obrigatório:

Na admissão;

Anualmente;

Em mudanças regulatórias.

17. AUDITORIA INTERNA E EXTERNA

Avalia conformidade, aderência, riscos e eficácia.

18. PENALIDADES E AÇÕES CORRETIVAS

Advertência;

Suspensão;

Bloqueio de produtos;

Descredenciamento;

Comunicação às autoridades.

19. MELHORIA CONTÍNUA

O programa é atualizado constantemente com base em:

Auditorias;

Evolução tecnológica;

Riscos emergentes;

Recomendações de reguladores.

20. DISPOSIÇÕES FINAIS

Esta Política integra o conjunto normativo da empresa e deve ser seguida por todos.

21. ANEXO – TERMO DE CIÊNCIA E COMPROMISSO

O colaborador ou parceiro assina declaração reconhecendo:

Ciência da Política;

Dever de cumprimento;

Responsabilidade individual.

CONTROLE DOCUMENTAL E GOVERNANÇA DA POLÍTICA

Esta Política constitui documento corporativo de diretrizes e deve ser mantida em repositório oficial, com controle de versão, acesso, histórico de alterações e evidência de aprovação. A versão vigente deverá ser disponibilizada às pessoas abrangidas, preservando-se as versões anteriores para fins de rastreabilidade.

Campo	Informação
Documento	Política Institucional de PLD-FTP
Empresa	Villet Pag Soluções de Pagamentos S.A.
CNPJ	53.183.086/0001-00
Versão	2.0 – Revisada e aprimorada
Classificação	Pública
Área proprietária	Compliance
Aprovação	Conselho de Administração ou Diretoria, conforme
Data de revisão	15/08/2025 – data de preparação desta versão;
Periodicidade de revisão	Anual ou diante de alterações legais, operacionais
Responsável formal por PLD-FTP	A preencher e formalizar pela Administração

21. RESPONSABILIDADES E DEVERES ESPECÍFICOS

A Administração deve assegurar que a Política seja efetivamente implementada, aprovada, revisada, divulgada e apoiada por recursos humanos, tecnológicos e financeiros adequados. A designação de responsável formal pelas obrigações de PLD-FTP deve ser documentada, observadas as exigências legais e regulatórias aplicáveis ao enquadramento da empresa.

Administração / Diretoria

aprovar a Política, suas revisões e o apetite de risco;

designar formalmente responsáveis e assegurar independência funcional adequada;

receber reportes periódicos sobre riscos, alertas relevantes, deficiências e planos de ação;

deliberar sobre medidas relevantes, inclusive suspensão de relacionamento, quando escalonadas.

Compliance / PLD-FTP

manter a Política, procedimentos e matriz de risco atualizados;

coordenar avaliação interna de risco e due diligence reforçada;

avaliar alertas e documentar decisões;

orientar comunicações legalmente exigidas e manter evidências;

promover treinamento e monitorar sua conclusão.

Operações / Atendimento / Comercial

cumprir os procedimentos de cadastro e validação sem contornar controles;

encaminhar alertas e indícios ao canal interno definido;

não prometer aprovação, liberação ou manutenção de operações sem validação competente;

preservar documentos, registros e evidências.

Tecnologia / Segurança da Informação

manter trilhas de auditoria e controles de acesso;

assegurar integridade, disponibilidade e confidencialidade dos dados;

implementar regras e parâmetros de monitoramento aprovados;

registrar alterações de configuração e permitir rastreabilidade.

Auditoria / Revisão Independente

avaliar desenho e efetividade dos controles;

registrar achados, responsáveis, prazos e recomendações;

acompanhar a remediação das deficiências.

22. AVALIAÇÃO INTERNA DE RISCO E MATRIZ DE CLASSIFICAÇÃO

A avaliação interna de risco deverá ser documentada, considerar os riscos inerentes e a qualidade dos controles mitigadores, e produzir classificação de risco residual. A metodologia deverá ser aprovada pela Administração, revisada periodicamente e ajustada quando houver alteração relevante no perfil de clientes, produtos, canais, parceiros, geografia ou volume.

Os fatores avaliados poderão incluir, conforme aplicável:

tipo, natureza, atividade econômica, estrutura societária, complexidade e transparência do cliente;

beneficiário final, representantes, procuradores, pessoas expostas politicamente e alertas em listas restritivas;

produto, serviço, canal de captura, modelo de liquidação, fluxo de recursos e possibilidade de movimentação por terceiros;

volume, frequência, ticket médio, velocidade, concentração, comportamento transacional e divergência entre atividade declarada e movimentação;

jurisdição, localização, origem e destino dos recursos, quando disponíveis e pertinentes;

histórico de fraude, chargebacks, reclamações, alertas, MED e eventos operacionais relevantes, sem tratar um indicador isolado como prova de ilícito;

risco de parceiros, fornecedores, agentes, plataformas, integradores e prestadores críticos;

efetividade dos controles, qualidade de dados, capacidade de monitoramento e evidências de execução.

A classificação deverá observar critérios documentados. Como referência operacional, poderá ser adotada a seguinte matriz, sujeita à aprovação e parametrização pela empresa:

Nível	Indicadores de referência	Diligência	Revisão sugerida
Baixo	Perfil transparente;	Diligência padrão e	Até 24 meses, ou conforme
Médio	Alguns fatores agravantes	Diligência adicional;	Até 12 meses
Alto	Fatores agravantes	Diligência reforçada	Até 6 meses, ou mais

Os prazos acima são parâmetros sugeridos para a política interna, não substituem prazos ou critérios regulatórios específicos. A empresa deverá definir e documentar os intervalos definitivos.

23. PROCEDIMENTOS DE KYC/KYB E BENEFICIÁRIO FINAL

Antes do início do relacionamento, e durante sua manutenção, devem ser obtidas, verificadas e atualizadas informações suficientes para identificar e qualificar clientes, representantes e beneficiários finais, conforme o risco e o tipo de relacionamento.

identificação e validação de CPF/CNPJ, razão social/nome, endereço, contatos e atividade;

documentos constitutivos, quadro societário e poderes de representação, quando aplicável;

identificação de beneficiário final e compreensão da estrutura de controle, inclusive indireta;

verificação de PEP, sanções, listas restritivas e mídias adversas conforme procedimento e critérios;

compatibilidade entre atividade declarada, canais, produtos, capacidade operacional, faturamento esperado e transações;

validação de conta de liquidação e titularidade, conforme fluxo e regras do parceiro/arranjo;

registro de data, fonte, resultado e responsável pelas verificações;

tratamento de divergências, documentos vencidos, suspeitas de falsidade e cadastro incompleto.

O relacionamento não deverá ser iniciado ou mantido quando informações essenciais não puderem ser verificadas ou quando o risco não puder ser adequadamente mitigado, salvo decisão formalmente autorizada e juridicamente admissível.

24. DUE DILIGENCE REFORÇADA (EDD)

A diligência reforçada deverá ser aplicada a clientes, parceiros, operações ou situações classificados como de maior risco. Poderá incluir, conforme o caso:

documentação adicional e confirmação independente de informações;

esclarecimento da origem dos recursos, patrimônio, finalidade e natureza da relação;

análise ampliada do beneficiário final, grupo econômico e pessoas relacionadas;

avaliação aprofundada de PEP, sanções e notícias relevantes;

aprovação por alçada superior ou Compliance antes de ativação, continuidade ou alteração material;

limites, monitoramento e revisão mais frequentes;

registro da justificativa, evidências, decisão e prazo de reavaliação.

A classificação de risco elevado, por si só, não representa conclusão de ilícito; exige controles proporcionais e decisão fundamentada.

25. MONITORAMENTO TRANSACIONAL – CONTROLES E ALERTAS

O monitoramento deverá ser compatível com os produtos, canais e fluxos de recursos efetivamente oferecidos. As regras devem possuir responsável, justificativa de risco, parâmetros, teste, aprovação, registro de alterações e revisão de efetividade.

alteração abrupta de volume, frequência, ticket médio ou padrão de horário;

movimentação incompatível com cadastro, atividade, faturamento ou capacidade declarada;

transações fracionadas, repetitivas, circulares ou com sinais de tentativa de evitar controles;

concentração de pagamentos, múltiplas origens/destinos, uso de contas ou dispositivos correlacionados, quando tais dados forem disponíveis;

divergências entre pagador, recebedor, titularidade e finalidade, conforme fluxo aplicável;

repasses rápidos, movimentação atípica de saldo ou comportamento incompatível com o modelo de negócio;

chargebacks, contestações, MED, reclamações e sinais de fraude em patamar ou padrão atípico;

atividade, MCC, produto, checkout, URL, canal ou descrição incompatível com cadastro;

alterações de cadastro, conta de liquidação, sócios, representantes ou dados críticos próximas a eventos de risco.

Alertas deverão ser priorizados por severidade e risco. Parâmetros numéricos, limites, regras e janelas temporais devem constar em documento operacional restrito, evitando que a Política pública exponha mecanismos sensíveis.

26. TRATAMENTO DE ALERTAS E INVESTIGAÇÃO

Cada alerta ou caso deverá possuir identificador, data de abertura, origem, classificação de prioridade, analista responsável, evidências, histórico de diligências, conclusão e aprovação quando exigida.

1. Receber e registrar o alerta;
2. Realizar triagem e verificar dados cadastrais, transacionais e contexto disponível;
3. Solicitar informações ou documentos por canal seguro, quando necessário e permitido;
4. Escalonar casos críticos, suspeitas de ilícito, sanções ou risco iminente ao responsável de PLD-FTP e à Administração;
5. Documentar conclusão, fundamento, medidas aplicadas e necessidade de comunicação às autoridades;
6. Monitorar pendências e assegurar que o caso seja encerrado por pessoa autorizada;
7. Preservar sigilo, restringir acesso e evitar alertar o cliente sobre eventual comunicação às autoridades quando proibido.

As decisões de liberar, restringir, suspender, encerrar ou reportar deverão ser fundamentadas, proporcionais, documentadas e adotadas conforme alçadas e obrigações legais, contratuais e regulatórias.

27. COMUNICAÇÕES AO COAF E AUTORIDADES

A empresa deverá avaliar e efetuar, quando legalmente obrigada e aplicável ao seu enquadramento, comunicações de operações ou situações suspeitas às autoridades competentes, especialmente ao COAF, observando prazos, canais, critérios e sigilo previstos na legislação e regulamentação.

manter procedimento formal para identificação, análise, aprovação e envio de comunicações;

documentar a decisão de comunicar ou não comunicar, com fundamentação e evidências;

observar comunicações automáticas ou obrigações específicas previstas em norma, quando aplicáveis;

manter registro de comunicações, protocolos, responsáveis e controles de acesso;

proibir divulgação indevida ao cliente ou a terceiros sobre comunicações suspeitas, nos termos legais.

28. FRAUDES, MED, CHARGEBACKS E RISCOS CORRELATOS

Eventos de fraude, MED, chargebacks, reclamações, disputas e indícios de uso indevido devem ser considerados como informações relevantes para a avaliação e monitoramento de risco, sem que sua ocorrência isolada implique automaticamente suspeita de lavagem de dinheiro.

registrar eventos, valores, identificadores de transação, evidências, origem do alerta e providências;

identificar padrões, reincidência, correlação entre clientes, recebedores, parceiros e canais, quando disponíveis;

avaliar impacto sobre perfil de risco, limites, diligência e continuidade do relacionamento;

escalar eventos materiais, recorrentes ou com indícios de ilícito;

preservar evidências e respeitar os procedimentos de contestação, comunicação e resposta definidos para cada produto e parceiro.

29. GESTÃO DE PARCEIROS, FORNECEDORES E TERCEIROS

Parceiros e terceiros que possam afetar a integridade da operação deverão ser avaliados antes da contratação e durante o relacionamento, de acordo com sua criticidade e exposição.

identificar empresa, representantes, beneficiários finais e estrutura de controle;

avaliar reputação, capacidade técnica, segurança, compliance e aderência ao serviço contratado;

formalizar responsabilidades, direitos de auditoria, obrigações de cooperação, confidencialidade e proteção de dados;

monitorar mudanças relevantes, incidentes, falhas, reclamações e riscos;

estabelecer plano de contingência e critérios de suspensão ou encerramento.

30. REGISTROS, RETENÇÃO, SIGILO E LGPD

Registros cadastrais, transacionais, de alertas, análises, decisões, comunicações, treinamentos, auditorias e controles deverão ser mantidos em ambiente seguro, íntegro, rastreável e com acesso baseado em necessidade. Os prazos de guarda deverão observar a legislação e regulamentação aplicáveis, inclusive obrigações específicas, e não poderão ser reduzidos por esta Política.

controle de acesso por perfil e autenticação;

registro de consulta, alteração, exportação e compartilhamento, quando tecnicamente possível;

proteção contra alteração, perda, destruição ou acesso indevido;

descarte seguro após o término do prazo de retenção, ressalvadas obrigações de preservação;

tratamento de dados pessoais limitado à finalidade, necessidade e base legal aplicável;

procedimento para incidentes de segurança e solicitações de titulares, conforme legislação.

O prazo de cinco anos mencionado no texto-base deverá ser validado para cada categoria documental e obrigação aplicável; prevalecerá prazo legal ou regulatório específico quando superior ou diferente.

31. TREINAMENTO, COMUNICAÇÃO E CULTURA DE CONFORMIDADE

A empresa deverá manter programa de capacitação compatível com funções, exposição e responsabilidades. Os treinamentos devem ser registrados, possuir conteúdo atualizado e permitir comprovação de participação e avaliação, quando adotada.

treinamento inicial antes ou próximo do início das atividades, conforme risco e função;

reciclagem periódica e em mudanças relevantes de normas, procedimentos ou produtos;

conteúdo sobre sinais de alerta, cadastro, sigilo, escalonamento, fraude, sanções e proteção de dados;

treinamento específico para áreas de maior exposição;

registro de presença, conteúdo, data, avaliação e ações para participantes pendentes.

32. INDICADORES, TESTES E PLANO DE REMEDIAÇÃO

A Administração e Compliance deverão acompanhar indicadores adequados à operação e ao risco. Os indicadores devem ser interpretados em conjunto, com metodologia consistente, histórico e análise de tendências.

alertas gerados, analisados, pendentes e encerrados, por prioridade e tempo de tratamento;

casos escalonados, decisões, medidas aplicadas e comunicações, quando aplicáveis;

cadastros incompletos, revisões vencidas, diligências reforçadas e pendências documentais;

treinamentos realizados e pendentes;

achados de auditoria, incidentes, deficiências e ações corretivas vencidas;

taxas de falso positivo e efetividade de regras, quando mensuráveis;

eventos de fraude, MED e chargeback usados como indicadores correlatos, com análise contextual.

Deficiências deverão ser registradas em plano de ação com causa, risco, medida corretiva, responsável, prazo, prioridade e evidência de conclusão. A efetividade da remediação deverá ser verificada.

33. INCIDENTES, CONTINUIDADE E ESCALONAMENTO

Incidentes que possam comprometer controles PLD-FTP, dados, sistemas de monitoramento, integridade de registros, cumprimento de obrigações ou segurança da operação devem ser comunicados imediatamente ao canal e responsáveis definidos. A empresa deverá manter procedimento de contingência para falhas críticas, assegurando registro de decisões, recuperação de dados e revisão posterior do incidente.

34. REVISÃO, APROVAÇÃO E EXCEÇÕES

Esta Política deverá ser revisada ao menos anualmente e sempre que ocorrer alteração regulatória, mudança significativa do modelo operacional, introdução de produto ou canal, incidente relevante, recomendação de auditoria ou mudança no perfil de risco. Exceções deverão ser justificadas, documentadas, aprovadas por alçada competente, possuir prazo e controles compensatórios, e não poderão afastar obrigações legais.

A aprovação formal desta versão deve ser registrada em ata, termo ou sistema corporativo de aprovação, com indicação dos aprovadores e data efetiva.

ANEXO I – CHECKLIST MÍNIMO DE ONBOARDING (REFERENCIAL)

Identificação e validação da pessoa física ou jurídica;

Documentos de constituição e representação, conforme aplicável;

Identificação de sócios, controladores e beneficiário final;

Atividade econômica, produtos/serviços e canais;

Endereço, contatos e informações de localização;

Perfil de volume, ticket, frequência e finalidade da operação;

Verificações de PEP, sanções e listas restritivas, conforme procedimento;

Análise de risco e classificação;

Verificação de conta de liquidação/titularidade, conforme fluxo;

Pendências, diligências adicionais, aprovação e registro de decisão.

ANEXO II – CHECKLIST DE INVESTIGAÇÃO DE ALERTA (REFERENCIAL)

Identificador do caso e data;

Cliente, envolvidos, beneficiário final e relacionamentos relevantes;

Transações e período analisado;

Motivo do alerta e regra acionada;

Dados cadastrais e perfil esperado;

Origem e destino dos recursos, quando disponíveis;

Documentos, justificativas e evidências obtidas;

Resultado de consultas e diligências;

Conclusão fundamentada;

Decisão, alçada, medidas e responsável;

Necessidade de comunicação e registro da análise;

Data de encerramento e revisão futura, quando necessária.

ANEXO III – MATRIZ DE RESPONSABILIDADES (RESUMO)

Atividade	Executa	Supervisiona/Aprova	Evidência
Política e revisão	Compliance	Administração/Diretoria	Versão aprovada/ata
Onboarding e cadastro	Operações/KYC	Compliance, conforme risco	Cadastro e documentos
Classificação de risco	Compliance/Risco	Responsável	Avaliação e score
Monitoramento	Risco/Fraude/Operações	Compliance	Alertas e logs
Investigação	Analista designado	Compliance/Alçada	Dossiê do caso
Comunicação externa	Responsável designado	Alçada competente	Protocolo/decisão
Treinamento	Compliance/RH	Administração	Registro de conclusão
Auditoria	Auditoria/revisor	Administração	Relatório e plano de ação

ANEXO IV – REFERÊNCIAS NORMATIVAS E FONTES OFICIAIS

A área de Compliance deverá manter a relação normativa atualizada e avaliar a aplicabilidade de cada norma ao enquadramento e às atividades efetivamente exercidas pela empresa. Referências indicativas:

Lei nº 9.613/1998;

Lei nº 13.260/2016;

Lei nº 13.709/2018 (LGPD);

Lei nº 13.810/2019, relativa a sanções e indisponibilidade de ativos, conforme aplicável;

Circular BCB nº 3.978/2020 e alterações vigentes, quando aplicável ao enquadramento da empresa;

Resolução BCB nº 119/2021 e demais alterações pertinentes;

Resolução BCB nº 591/2026, que altera a Circular nº 3.978/2020, com vigência indicada pelo BCB a partir de 1º/10/2026;

Carta Circular BCB nº 4.001/2020 e alterações, como referência de sinais de alerta, quando aplicável;

Normas e orientações COAF pertinentes ao setor e à atividade.

Fontes oficiais consultadas para atualização normativa:

Banco Central do Brasil – Circular nº 3.978/2020 e histórico de alterações: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=3978&tipo=Circular

Banco Central do Brasil – página de legislação relacionada à PLD/FTP: https://www.bcb.gov.br/estabilidadefinanceira/lavagemdinheiro

Banco Central do Brasil – Resolução BCB nº 588/2026 A inclusão de referências não representa, por si só, declaração de que a VILLET PAG SOLUÇÕES DE PAGAMENTOS S.A. esteja autorizada, supervisionada ou sujeita a todos os dispositivos citados. A aplicabilidade deve ser confirmada juridicamente e de acordo com o modelo operacional e status regulatório.