MERCGROUP

THINK GROWTH. THINK MERC.

AUDITORIA · GUIA TÉCNICO · SÉRIE ATIVOS VIRTUAIS

PLD/FT e *travel rule* na PSAV

Os controles de prevenção à lavagem de dinheiro e a regra de viagem da informação que o regulador cobra das prestadoras de ativos virtuais, e a trilha de evidência que o auditor testa.

NORMA BASE	PÚBLICO	EDIÇÃO	DATA
Lei 9.613 · FATF R.15/16 · Res. BCB 520	Diretor de PLD, compliance e auditoria interna	Guia técnico MERC · Série Ativos Virtuais	Agosto de 2026

SUMÁRIO · COMO LER ESTE GUIA

Índice

Guia em quatro partes. Parte I: o marco normativo e a abordagem baseada em risco. Parte II: os controles, do KYC à travel rule. Parte III: evidência, governança e o papel do auditor. Parte IV: implantação, perguntas frequentes e checklist.

PARTE I

I

O marco e a abordagem por *risco.*

Da Lei 9.613 às recomendações do FATF: o que se aplica à prestadora de ativos virtuais.

SEÇÃO 01 · PARTE I · MARCO NORMATIVO

A arquitetura *normativa.*

O programa de PLD/FT de uma prestadora de serviços de ativos virtuais responde a uma pilha de normas, não a uma regra isolada. A base é a Lei 9.613, que estrutura o sistema brasileiro de prevenção à lavagem de dinheiro e ao financiamento do terrorismo e ancora o dever de comunicar operações suspeitas ao COAF. Sobre ela, a Lei 14.478/2022 definiu o ativo virtual e a prestadora de serviços, o Decreto 11.563/2023 designou o Banco Central como órgão regulador e supervisor do setor, e as Resoluções BCB 519, 520 e 521, publicadas em 10/11/2025 e vigentes a partir de 02/02/2026, detalharam autorização, funcionamento, conduta e o tratamento cambial. Ler uma camada isolada produz leitura incompleta das exigências.

O efeito prático é um só. A PSAV deixa de operar sob regras próprias e passa a responder por controles típicos de instituições reguladas. Antes do marco legal, boa parte da atividade com ativos virtuais funcionava fora de um regime formal de prevenção. Com a vigência do novo regime, as prestadoras tornam-se sujeitas às obrigações de PLD/FT com controles equivalentes aos exigidos das demais instituições supervisionadas. A exigência não é de uma versão simplificada para um setor jovem. É de política equivalente à de instituição financeira, com governança dedicada, diretor responsável e rotina que produz evidência.

A pilha que *obriga*

CAMADA NORMATIVA	O QUE RESOLVE	EFEITO NA PRESTADORA
Lei 9.613	Estrutura o sistema de PLD/FT e o dever de comunicação	Fundamento das obrigações de prevenção e do reporte ao COAF
Lei 14.478/2022	Define ativo virtual e prestadora de serviços	Traz a atividade para o perímetro regulado
Decreto 11.563/2023	Designa o Banco Central como regulador	Sujeita a sociedade a autorização e supervisão
Res. BCB 519	Procedimento de autorização	Define a porta de entrada e o rito do pedido
Res. BCB 520	Constituição, funcionamento, governança e conduta	Abriga segregação, custódia e o núcleo de PLD/FT
Res. BCB 521	Operações submetidas ao mercado de câmbio	Cria obrigações de registro e reporte cambial
Recomendações do GAFI	**Padrão internacional de prevenção**	**Orientam a abordagem por risco e a travel rule**

A divisão de trabalho entre as resoluções organiza a leitura. A 519 cuida da porta de entrada: o rito de autorização e a instrução do pedido. A 520 cuida da vida da instituição autorizada: modalidades, governança, segregação patrimonial, custódia e prevenção à lavagem. A 521 cuida do câmbio, submetendo determinadas operações com ativos virtuais ao arcabouço cambial. As recomendações do GAFI atravessam as três camadas: são a referência internacional que orienta o padrão de prevenção do setor e que deu origem à travel rule.

> NÃO É REGIME SIMPLIFICADO
>
> A supervisão fala em elevar o setor ao nível das instituições autorizadas tradicionais em capital, controles e governança. Em PLD/FT, isso significa que a prestadora responde pelo mesmo padrão de um participante maduro do sistema financeiro. Programa enxuto demais para o risco da atividade é lacuna, não eficiência.

Os pilares do programa são conhecidos de quem atua no sistema financeiro: identificação e qualificação de clientes, abordagem baseada em risco, monitoramento contínuo de operações, comunicação de operações suspeitas e governança com responsabilidades definidas. A diferença está na natureza do ativo. Transações em blockchain são pseudônimas, cruzam fronteiras em minutos e podem envolver endereços sem qualquer instituição por trás. O programa precisa incorporar essa realidade técnica, sob pena de ser formalmente completo e operacionalmente cego. E há um mecanismo específico do universo cripto: a travel rule, a viagem da informação de originador e beneficiário nas transferências, que este guia trata em profundidade.

O calendário amarra tudo. As regras-base vigem desde 02/02/2026. As prestadoras em atividade têm janela de 270 dias, contada da vigência, para protocolar o pedido de autorização, com teto improrrogável em 30/10/2026. Depois dessa data, o perímetro se fecha para quem não protocolou. O programa de PLD/FT não é um anexo do pedido: é um dos requisitos centrais que a instrução precisa demonstrar em operação, com evidência.

SEÇÃO 02 · PARTE I · MARCO NORMATIVO

FATF R.15 e a regra de *viagem.*

A travel rule tem origem nas recomendações do GAFI, o organismo internacional que define o padrão global de combate à lavagem de dinheiro. A Recomendação 15 tratou das novas tecnologias e trouxe as VASPs, sigla internacional para prestadoras de serviços de ativos virtuais, para dentro do perímetro de prevenção. A Recomendação 16 estabeleceu a regra de transmissão de informação, historicamente aplicada às transferências eletrônicas de recursos e estendida às transferências de ativos virtuais. Juntas, as duas recomendações definem o padrão que o regime brasileiro incorporou.

O princípio é direto. Em uma transferência acima de um limiar definido, a instituição originadora deve transmitir dados do originador e do beneficiário, e a instituição beneficiária deve recebê-los. A informação viaja junto com a operação, permitindo que ambas as pontas saibam quem está de cada lado. Isso reconstitui, no ambiente cripto, uma capacidade que a intermediação bancária tradicional sempre teve: identificar as partes de uma transferência. Transferência de valor não pode ser anônima. A travel rule é a tradução desse princípio antigo para um ambiente que nasceu, tecnicamente, para funcionar sem esse elo.

Os dados envolvidos costumam incluir o nome do originador, a identificação de conta ou endereço de origem e o nome do beneficiário, entre outros elementos exigidos conforme o regime aplicável. Quando a mensagem chega incompleta, ou simplesmente não chega, a instituição beneficiária precisa de uma política clara: reter o ativo, questionar a contraparte, aplicar diligência reforçada ou recusar a operação. A ausência de tratamento definido para mensagens incompletas é uma fragilidade recorrente nos programas do setor e um ponto natural de teste em qualquer exame independente.

A regra por *dimensão*

DIMENSÃO	O QUE SE ESPERA	PONTO DE ATENÇÃO
Dados do originador	Transmitir a identificação de quem envia e do endereço de origem	Completude dos campos e consistência com o cadastro KYC
Dados do beneficiário	Receber e validar a identificação de quem recebe	Conferência do beneficiário e tratamento de divergências
Limiar de aplicação	Aplicar a regra às transferências acima do valor definido	Parametrização correta e teste de operações no entorno do corte
Mensagem incompleta	Reter, questionar ou recusar quando faltarem dados	Existência de política e registro das decisões tomadas
Interoperabilidade	Trocar mensagens com contrapartes em padrões diferentes	Cobertura de contrapartes e falhas de compatibilidade
Carteira autocustodiada	**Aplicar diligência quando não há instituição na outra ponta**	**Controles compensatórios e vínculo entre carteira e cliente**

Note o que a tabela revela: a travel rule não é um campo a mais no formulário de transferência. É um processo de ponta a ponta, com coleta, transmissão, recepção, validação e tratamento de exceção. Cada dimensão tem uma evidência própria, e o exame independente percorre todas. A dimensão mais difícil, a carteira autocustodiada, em que não existe contraparte institucional para trocar a mensagem, é tratada em detalhe na Parte II deste guia, junto com os controles compensatórios que a suprem.

> O PADRÃO É INTERNACIONAL
>
> A regra de viagem atravessa jurisdições. A contraparte da transferência pode estar em qualquer país, sujeita a um regime local diferente e a um protocolo técnico distinto. Cumprir a regra apenas no padrão doméstico, sem capacidade de dialogar com contrapartes estrangeiras, resolve metade do problema. A outra metade é exatamente onde o risco de lavagem internacional se concentra.

Para a prestadora, a consequência organizacional é clara. A travel rule é um requisito de sistema, não apenas de política. Exige capacidade técnica de capturar, transmitir, receber e validar dados, integrada à esteira de transferências e à arquitetura de segurança. Escrever a política é a parte rápida. Construir a integração com contrapartes, tratar exceções e guardar a trilha de cada mensagem é o trabalho que consome cronograma. Por isso a preparação começa antes do prazo, não no prazo.

SEÇÃO 03 · PARTE I · MARCO NORMATIVO

A abordagem por *risco.*

A abordagem baseada em risco é o princípio organizador de todo o programa: o esforço de controle acompanha o risco de cada cliente e de cada operação. Ela evita os dois erros simétricos que destroem programas de prevenção. O primeiro é tratar todos os clientes com a mesma intensidade, o que desperdiça diligência onde o risco é baixo e falta onde é alto. O segundo é calibrar controles por conveniência operacional, e não por avaliação fundamentada. A abordagem por risco exige que cada escolha de intensidade tenha uma justificativa documentada.

O instrumento central é a avaliação interna de risco. Ela não é peça de arquivo: é o documento que fundamenta as escolhas de controle, define onde aplicar diligência reforçada e justifica a calibragem dos cenários de monitoramento. Quando o supervisor ou o auditor pergunta por que determinado segmento de clientes recebe tratamento simplificado, ou por que determinado cenário de alerta usa certo parâmetro, a resposta precisa estar na avaliação interna de risco. Se a resposta não está lá, a calibragem é arbitrária, e controle arbitrário não se defende em exame.

Os fatores que *pesam*

FATOR DE RISCO	EXEMPLOS DE LEITURA	EFEITO NO CONTROLE
Cliente	Perfil sensível, atividade incompatível com o volume, pessoa jurídica de estrutura opaca	Define a classe de risco e a intensidade da diligência
Produto e serviço	Transferência para carteira externa, ativo com maior anonimato, operação de câmbio	Aciona controles específicos por modalidade
Canal	Onboarding totalmente remoto, intermediários, contas operadas por terceiros	Exige verificação adicional de identidade e titularidade
Jurisdição	Contrapartes em praças de maior risco ou com supervisão frágil	Eleva a diligência e o escrutínio da contraparte
Tecnologia	**Exposição on-chain a endereços de risco e a serviços de mistura**	**Alimenta escores, bloqueios e diligência reforçada**

A matriz de fatores produz a segmentação da carteira de clientes em classes de risco, e cada classe recebe um pacote de controles proporcional: periodicidade de atualização cadastral, profundidade da qualificação, limites operacionais, intensidade do monitoramento. O ponto que o exame independente verifica é a coerência do conjunto: os critérios de segmentação estão documentados, a classificação atribuída a cada cliente tem registro, e o pacote de controles aplicado corresponde de fato à classe atribuída. Segmentação que existe na política e não aparece no sistema é desenho sem eficácia.

REGRA DE OURO

Toda decisão de intensidade de controle nasce da avaliação interna de risco e volta para ela. Se um cenário de monitoramento foi calibrado, a justificativa está na avaliação. Se um segmento recebe diligência reforçada, o critério está na avaliação. O documento é vivo: risco muda, e a avaliação acompanha.

Dois erros práticos merecem alerta. O primeiro é a matriz genérica: uma avaliação de risco copiada de modelo de mercado, sem aderência à carteira real da prestadora, aos ativos listados e aos canais efetivamente usados. Ela reprova no primeiro confronto com os dados da operação. O segundo é a avaliação estática: aprovada uma vez, nunca revisitada, enquanto a prestadora lista novos ativos, abre novos canais e muda de perfil de cliente. A revisão periódica, com registro do que mudou e por quê, é o que mantém a abordagem por risco defensável ao longo do tempo. O programa inteiro se apoia nesse alicerce: KYC, monitoramento, travel rule e reporte herdam da avaliação interna de risco a sua régua de intensidade.

Um efeito colateral positivo merece registro. A abordagem por risco bem documentada reduz atrito comercial: clientes de baixo risco fluem por esteiras mais leves, com menos fricção de onboarding, enquanto o esforço analítico se concentra nos casos que de fato o exigem. O programa fica mais barato e mais defensável ao mesmo tempo. A régua, porém, precisa ser demonstrável: quando o supervisor pergunta por que determinado cliente recebeu tratamento leve, a resposta correta é a classe de risco documentada, nunca a conveniência da área de negócio.

PARTE II

II

Os controles em *operação.*

KYC, monitoramento, travel rule e sanções: o núcleo operacional do programa.

SEÇÃO 04 · PARTE II · CONTROLES

KYC e diligência *reforçada.*

O conhecimento do cliente é a base do programa, e o erro mais comum é tratá-lo como um cadastro único e estático. Um programa maduro faz duas coisas distintas. Identifica e qualifica o cliente na entrada, coletando e verificando informações que permitam entender quem é, qual atividade justifica as operações e qual a origem esperada dos recursos. E aplica diligência ampliada quando o risco é maior: clientes com perfil sensível, operações fora do padrão esperado, contrapartes em jurisdições de maior risco. O cadastro estabelece o perfil esperado; é contra esse perfil que o monitoramento vai comparar cada operação.

Identificação e qualificação não são sinônimos. Identificar é saber quem é a pessoa: dados de identidade verificados, documentos válidos, checagem de que o titular é quem diz ser. Qualificar é entender o cliente como agente econômico: atividade, capacidade financeira, propósito do relacionamento, volume e padrão de operação compatíveis com o que se declara. A qualificação é o que dá sentido ao monitoramento. Sem ela, o sistema compara operações contra o vazio, e todo alerta vira julgamento subjetivo do analista.

Três níveis de *diligência*

NÍVEL	QUANDO SE APLICA	O QUE MUDA NA PRÁTICA
Diligência simplificada	Clientes de baixo risco, conforme critérios da avaliação interna de risco	Coleta essencial, atualização menos frequente, limites operacionais menores
Diligência padrão	Carteira geral, sem fatores de agravamento	Identificação e qualificação completas, atualização periódica programada
Diligência ampliada (EDD)	**Perfil sensível, alto volume, jurisdição de risco, autocustódia relevante, estrutura societária opaca**	**Aprofundamento de origem de recursos, aprovação em alçada superior, revisão mais frequente**

A diligência ampliada não é burocracia extra por precaução genérica. É o aprofundamento reservado para onde o risco de fato está. O ponto que costuma faltar nos programas do setor é o regime de diligência ampliada para pessoas jurídicas de maior risco. Muitas prestadoras consolidam bem o conhecimento de pessoas físicas, com verificação de identidade robusta no onboarding digital, e deixam a diligência de clientes corporativos de alto risco sem procedimento definido: quem aprova, o que se examina do quadro societário e dos beneficiários finais, qual evidência fica guardada. Essa lacuna abre exatamente a porta que o regime quer fechar, porque estruturas societárias são o veículo clássico de ocultação.

> O CADASTRO QUE ENVELHECE
>
> Conhecer o cliente é processo contínuo, não evento de entrada. A qualificação precisa ser atualizada em ciclos definidos pela classe de risco, e revisada fora do ciclo quando o comportamento muda. Cliente que entrou como pessoa física de movimentação modesta e passou a girar volume alto com carteiras externas não pode continuar com o cadastro da entrada. Cadastro desatualizado transforma o monitoramento em comparação contra um perfil que já não existe.

Para o exame independente, a evidência de KYC é objetiva: cadastros completos com documentos de identificação, registro da aprovação e da classificação de risco atribuída, trilha da atualização periódica e, nos casos de diligência ampliada, o registro do que foi aprofundado e de quem aprovou. O auditor seleciona uma amostra de clientes por classe de risco e verifica se o procedimento previsto na política aconteceu de fato, na data devida, com o rigor prometido. A distância entre a política escrita e o dossiê real do cliente é um dos achados mais frequentes em programas jovens: a política promete qualificação profunda e o dossiê contém apenas a identificação básica. Fechar essa distância antes do exame é mais barato do que explicá-la depois.

Um detalhe operacional fecha a seção. A qualificação precisa alcançar o beneficiário final nas estruturas societárias, com registro de quem foi identificado e por qual critério. E o vínculo entre o cadastro e as carteiras usadas pelo cliente, internas e externas declaradas, deve ficar registrado desde a entrada: é esse vínculo que a travel rule e a análise on-chain vão consumir adiante.

SEÇÃO 05 · PARTE II · CONTROLES

Monitoramento e análise *on-chain.*

O monitoramento de transações é o coração operacional do programa. Ele observa a operação depois que o cliente já está dentro, comparando o que o cliente faz com o que dele se esperava e levantando o que destoa. No mundo cripto, o monitoramento ganha uma camada adicional que não existe no sistema financeiro tradicional: a análise on-chain. Como o registro das operações está publicamente disponível na blockchain, a prestadora pode rastrear a origem e o destino dos recursos para além da própria fronteira, acompanhando o histórico das carteiras envolvidas.

A camada transacional clássica funciona por regras e cenários parametrizados: operações que fogem do padrão do perfil, fracionamento, movimentação incompatível com a capacidade declarada, uso atípico de canais. Cada cenário dispara alertas que entram em uma fila de tratamento. E aqui está a diferença entre um monitoramento que funciona e um que apenas existe: a governança dos alertas. Quem analisa, em que prazo, com que alçada de decisão e com que registro do desfecho. Alerta gerado e não tratado é pior do que alerta não gerado, porque cria a ilusão de controle e documenta a omissão.

As três frentes *on-chain*

FRENTE	O QUE FAZ	DECISÃO QUE ALIMENTA
Rastreamento de carteiras	Reconstitui o caminho dos ativos e identifica proximidade com endereços associados a atividade ilícita	Aprofundamento de diligência e abertura de caso
Checagem de sanções	Confronta endereços e contrapartes com listas restritivas, incluindo endereços designados por autoridades	Bloqueio, retenção e comunicação
Escore de exposição	**Mede a exposição dos recursos a endereços de risco conforme a origem dos fundos**	**Priorização de alertas e diligência reforçada**

Essas frentes não substituem o KYC nem o monitoramento transacional clássico. Elas se combinam. Um cliente com cadastro consistente pode, ainda assim, receber recursos de uma carteira com exposição elevada a endereços de risco. É o cruzamento entre o que se sabe do cliente e o que a cadeia revela sobre os recursos que produz os alertas mais relevantes. Para o auditor, importa verificar se essa integração existe de fato ou se as camadas operam isoladas, gerando pontos cegos: o time de KYC sem acesso ao escore on-chain, o analista de alertas sem visão do cadastro, a ferramenta de rastreamento desligada da esteira de transferências.

> A FILA QUE SE ACUMULA
>
> O padrão de falha mais comum não é a ausência de sistema. É a fila de alertas que cresce sem tratamento tempestivo e sem trilha do desfecho. O sistema gera, ninguém conclui, e o backlog vira passivo: cada alerta antigo não tratado é uma operação potencialmente suspeita que a prestadora detectou e ignorou. Em exame, isso pesa mais do que uma regra mal calibrada.

A cobertura do monitoramento também é objeto de teste. Verifica-se se as regras alcançam os riscos relevantes identificados na avaliação interna de risco ou se há tipologias sem cenário correspondente: um risco mapeado no papel, sem nenhuma regra que o detecte na prática, é lacuna de desenho. O caminho disciplinado é manter a rastreabilidade entre a avaliação interna de risco, a lista de tipologias e o inventário de cenários ativos, com registro das calibragens e das exclusões. O comitê acompanha os indicadores da esteira: volume de alertas por cenário, tempo médio de tratamento, taxa de conversão em comunicação e envelhecimento da fila. São números que contam, melhor do que qualquer política, se o monitoramento vive ou apenas existe.

Fecha a seção um teste simples de maturidade, aplicável em qualquer comitê: escolha um alerta encerrado no último trimestre e reconstrua o caminho completo, do disparo do cenário à decisão registrada, sem pedir nada a ninguém. Se a reconstrução exige memória de analista, mensagens avulsas ou planilhas paralelas, a esteira depende de pessoas, não de processo. O monitoramento auditável é o que qualquer terceiro percorre sozinho, do parâmetro ao desfecho, apenas com o que ficou registrado no sistema.

SEÇÃO 06 · PARTE II · CONTROLES

Os dados que *viajam.*

Na operação, a travel rule vira um processo de esteira: cada transferência de ativo virtual acima do limiar carrega uma mensagem com os dados de originador e beneficiário, e cada recebimento exige a validação da mensagem que chega. A prestadora precisa coletar e compartilhar informações sobre remetente e destinatário de modo que a operação seja rastreável, inclusive quando a outra ponta é uma carteira não custodiada. O desenho operacional tem quatro momentos: capturar, transmitir, receber e tratar a exceção. Falhar em qualquer um deles é falhar na regra.

A parametrização do limiar merece atenção específica. A regra se aplica às transferências acima do valor definido no regime aplicável, e o sistema precisa refletir exatamente esse corte. O teste clássico do auditor é selecionar operações no entorno do limiar e verificar o comportamento do sistema: as que estão acima carregam a mensagem completa, as que estão logo abaixo seguem o tratamento previsto, e não existe padrão de fracionamento para escapar do corte. Fracionamento recorrente logo abaixo do limiar é, ele próprio, uma tipologia que o monitoramento deve capturar.

Quando a mensagem *falta*

A mensagem incompleta é a exceção mais importante do processo. Quando a transferência chega sem os dados exigidos, ou com dados divergentes do que o cadastro indica, a instituição beneficiária precisa de uma política com opções definidas: reter o ativo até esclarecimento, questionar a contraparte, devolver, aplicar diligência reforçada antes de disponibilizar ou recusar. O que não pode acontecer é o ativo ser disponibilizado ao cliente sem tratamento, por falta de integração ou por pressa operacional. A dificuldade técnica de integração entre prestadoras não afasta a exigência. Deixar passar por não ter integração pronta é falha de controle, não limitação aceitável.

O segundo desafio estrutural é a interoperabilidade. O mercado desenvolveu diferentes padrões técnicos de troca de mensagens de travel rule, nem sempre compatíveis entre si. Duas prestadoras reguladas podem, cada uma, cumprir a regra em seu próprio padrão e ainda assim falhar em se comunicar. A cobertura de contrapartes torna-se, por isso, um indicador de gestão: com quantas contrapartes relevantes a mensagem flui de ponta a ponta, quantas exigem tratamento manual e quantas permanecem sem canal. As falhas de compatibilidade não resolvidas são objeto legítimo de avaliação.

> O PONTO CEGO DA AUTOCUSTÓDIA
>
> Quando uma das pontas é uma carteira autocustodiada, controlada diretamente pelo usuário, não há contraparte institucional para transmitir ou receber a mensagem. A prestadora identifica o cliente do seu lado e depende de mecanismos próprios para a outra ponta: comprovação de titularidade da carteira externa, diligência reforçada acima de determinados valores e uso intensivo da análise on-chain para suprir a ausência de informação transmitida. O vínculo entre a carteira externa e uma pessoa identificada é a evidência que o auditor procura.

O faseamento da *rastreabilidade*

2027 · doméstico

OPERAÇÕES NO PAÍS

O faseamento da regra de rastreabilidade prevê prazo até 2027 para as operações domésticas, conforme o cronograma do regime.

2028 · internacional

OPERAÇÕES COM O EXTERIOR

Para as operações internacionais, o prazo do faseamento vai até 2028, refletindo a complexidade adicional de contrapartes estrangeiras.

O faseamento é um dado de planejamento, não um alívio. Estruturar a coleta e o compartilhamento de dados de transferência exige tempo, integração técnica e acordo com contrapartes. A implementação segue um cronograma por etapas, começando pelo fluxo doméstico e avançando para o internacional, e a preparação começa antes do prazo, não no prazo. Tratar a travel rule como ajuste de última hora é subestimar a complexidade de integrar identidade e transferência em uma operação que nasceu

para funcionar sem esse elo. A prestadora que chega ao prazo com o processo desenhado, testado com contrapartes reais e com trilha de mensagens guardada transforma uma exigência difícil em vantagem de conformidade.

SEÇÃO 07 · PARTE II · CONTROLES

Sanções, listas e *bloqueios.*

A triagem de sanções é o controle que impede a prestadora de operar com pessoas, entidades e endereços restritos por listas nacionais e internacionais. No universo dos ativos virtuais, ela tem uma particularidade que não existe no sistema tradicional: além de nomes e documentos, as listas incluem endereços de blockchain designados por autoridades. A triagem precisa, portanto, operar em duas camadas: a camada de identidade, que confronta clientes e contrapartes com as listas, e a camada on-chain, que confronta os endereços envolvidos em cada transferência.

O controle opera em três momentos. Na entrada, todo cliente novo passa pela triagem antes da aprovação do cadastro. Na base, a carteira inteira de clientes é reprocessada periodicamente, porque as listas mudam: um cliente aprovado ontem pode constar de uma designação publicada hoje. E na transação, cada transferência confronta os endereços e as contrapartes envolvidas antes da liquidação. Os três momentos são complementares. Triagem só na entrada envelhece com a lista; triagem só na transação deixa a base cega entre atualizações.

Do alerta ao *desfecho*

ETAPA	O QUE O CONTROLE GARANTE	EVIDÊNCIA
Execução da triagem	Rodada com a frequência definida, sobre a base completa e as listas atualizadas	Log de execução com data, escopo e versão das listas
Tratamento do hit	Todo apontamento analisado, com distinção entre homônimo e correspondência real	Registro da análise e da conclusão, com responsável
Bloqueio e retenção	Correspondência confirmada gera bloqueio imediato e retenção de ativos	Registro da medida, do horário e da alçada que decidiu
Comunicação	**Situações previstas em norma são reportadas ao canal competente, no prazo**	**Comunicação efetuada com data e fundamentação**

O que a auditoria examina aqui não é a existência da política, mas a evidência de execução periódica: a triagem foi rodada, com que frequência, contra quais listas, e o que aconteceu com os resultados. Um sistema de triagem contratado e configurado, sem log que comprove as execuções e sem registro do tratamento dos apontamentos, não sustenta conclusão de eficácia. A pergunta do exame é sempre operacional: mostre a rodada de determinada data, mostre os apontamentos que ela gerou, mostre o desfecho de cada um.

> FALSO POSITIVO TAMBÉM DEIXA TRILHA
>
> A maior parte dos apontamentos de triagem é falso positivo: homônimos, coincidências parciais, dados incompletos. Descartar rápido é legítimo e necessário. Descartar sem registro é destruir a evidência do controle. Cada descarte precisa de um registro mínimo: quem analisou, que critério aplicou, por que concluiu pela não correspondência. É esse registro que diferencia uma fila bem tratada de uma fila esvaziada sem análise.

A camada on-chain merece destaque final. A checagem de endereços designados se integra ao escore de exposição tratado na seção anterior: um endereço pode não constar de lista, mas apresentar proximidade relevante com endereços designados, e essa proximidade alimenta a decisão de reter, aprofundar ou recusar. A calibragem dessa régua, que distância de um endereço sancionado dispara qual medida, é decisão de risco documentada na avaliação interna, não preferência da mesa de operações. E, como em todo o programa, a decisão registrada vale mais do que a intenção declarada: o exame independente reconstrói o que foi feito a partir do que ficou escrito.

Resta o ponto de fronteira com o câmbio. A Resolução BCB 521 submete determinadas operações com ativos virtuais ao tratamento do mercado de câmbio, e a triagem de sanções conversa diretamente com essa fronteira: operações que movem valor entre o país e o exterior carregam obrigações adicionais de identificação de partes, registro e reporte. A classificação

cambial na esteira, operação a operação, com o motivo registrado, evita que uma transferência internacional sancionável passe pelo crivo doméstico mais leve. As duas esteiras, sanções e câmbio, precisam se enxergar.

PARTE III

III

Evidência, COAF e *auditoria.*

A trilha que sustenta o programa, a governança que o mantém vivo e o exame que o testa.

SEÇÃO 08 · PARTE III · EVIDÊNCIA E GOVERNANÇA

A trilha de *evidência.*

Onde não há registro, não há evidência, e onde não há evidência, o auditor não pode concluir pela eficácia. Essa frase resume o que separa um programa de PLD/FT sólido de um programa apenas bem intencionado. A trilha de evidência é o conjunto de registros que permite a um terceiro independente reconstruir o que foi feito, quando, por quem e com qual autorização. Sem trilha, o controle pode até existir, mas não é testável, e o que não é testável não sustenta conclusão, nem no exame independente, nem perante a supervisão.

A trilha se organiza por controle. Para cada controle do programa, três perguntas definem a evidência: o que comprova que o controle operou, onde esse comprovante fica guardado e por quanto tempo. A resposta a essas três perguntas, escrita e mantida, é o que a auditoria e a supervisão vão percorrer. A tabela abaixo consolida a trilha esperada dos controles tratados neste guia.

CONTROLE	EVIDÊNCIA QUE COMPROVA OPERAÇÃO
KYC e qualificação	Cadastros completos, documentos, registro de aprovação e da classificação de risco atribuída
Abordagem por risco	Avaliação interna de risco documentada, matriz de fatores e critérios de segmentação
Monitoramento	Regras parametrizadas, alertas gerados, fila de tratamento e registro de disposição de cada alerta
Análise on-chain	Consultas de rastreamento, checagens de sanções e escores de risco de endereços
Sanções	Logs de execução da triagem, tratamento dos apontamentos e medidas de bloqueio
Comunicação ao COAF	Comunicações efetuadas, data de detecção, data de envio e fundamentação da decisão
Travel rule	Registro de mensagens enviadas e recebidas, campos preenchidos e tratamento das incompletas
Governança	**Diretor designado, políticas aprovadas com data, atas e evidência de revisão periódica**

Repare que cada linha é um registro operacional, não um documento institucional. Política aprovada é necessária, mas é a evidência mais fraca da tabela: prova intenção, não operação. O que sustenta conclusão de eficácia são os registros que nascem da rotina: o alerta com sua disposição, a mensagem de travel rule com seus campos, a rodada de triagem com seu log. Um alerta tratado sem registro da decisão, uma comunicação sem data de detecção, uma transferência sem log da mensagem: todos são pontos em que o programa pode ser sólido na intenção e frágil na comprovação. A auditoria transforma essa distinção em achado.

EVIDÊNCIA CONTEMPORÂNEA VALE. RECONSTRUÇÃO NÃO CONVENCE

Registro feito no momento do fato tem força probatória. Planilha montada na véspera do exame, para explicar o que teria acontecido meses antes, não tem. A trilha precisa nascer com a operação. Guardar depois o que deveria ter sido registrado antes é a origem mais comum de ressalva em asseguração de controles.

Dois atributos completam a trilha: integridade e retenção. Integridade significa que o registro não pode ser alterado depois do fato sem deixar rastro; logs imutáveis ou com controle de versão são o padrão esperado para os registros críticos, como acessos, decisões de alerta e mensagens de travel rule. Retenção significa que a evidência permanece disponível pelo prazo exigido e recuperável em tempo razoável: evidência que existe mas não se localiza equivale, no exame, a evidência que não existe. A recomendação prática da MERC é manter um inventário de evidências por controle, com dono, local de guarda e prazo, revisado a cada ciclo. Esse inventário é a espinha da sala de dados que a Parte III detalha adiante e o antídoto contra a corrida de véspera que compromete exames e prazos.

Por fim, a retenção tem um dono. Cada evidência do inventário precisa de responsável nomeado pela guarda e pela recuperação, com prazo definido e teste periódico de que o registro se recupera íntegro. Evidência crítica guardada em ferramenta de terceiro exige atenção contratual: o histórico precisa permanecer acessível mesmo se o contrato terminar.

SEÇÃO 09 · PARTE III · EVIDÊNCIA E GOVERNANÇA

COAF e *governança.*

Nada do que este guia descreve funciona sem governança. O programa de PLD/FT precisa de um diretor responsável formalmente designado, de uma avaliação interna de risco que fundamente as escolhas de controle e de políticas aprovadas pela instância competente. E precisa de um ciclo que se fecha: quando o monitoramento detecta situação atípica sem justificativa econômica ou legal aparente, ou quando se configura hipótese prevista em norma, a prestadora comunica ao COAF. A comunicação é o desfecho que dá sentido a todo o resto.

Dois atributos são críticos na comunicação: a fundamentação e a tempestividade. Fundamentar é registrar por que a operação foi considerada suspeita, com os elementos objetivos que sustentam a conclusão. Ser tempestivo é comunicar no prazo, contado da detecção. Comunicar tarde, ou deixar de comunicar situação que exigia reporte, é falha de controle. O registro da data de detecção e da data de envio permite medir esse intervalo objetivamente, e é exatamente essa medição que o exame independente faz. A decisão de não comunicar também precisa de registro e fundamentação: é ela que sustenta a posição da instituição perante a supervisão quando o caso é revisitado.

> O SILÊNCIO QUE DENUNCIA
>
> Um programa que nunca comunica nada, em um mercado de risco elevado, é em si um sinal de alerta. Ou o monitoramento não detecta, ou a fila não é tratada, ou a régua de decisão está deslocada. O número de comunicações não é meta, mas a ausência total delas, combinada com volume relevante de operações, convida a supervisão a perguntar o que o programa está deixando passar.

Quem responde pelo *quê*

ATIVIDADE	RESPONSÁVEL	APROVA	ACOMPANHA
Política de PLD/FT e avaliação interna de risco	Diretor de PLD	Conselho ou diretoria	Controles internos
Tratamento de alertas e casos	Equipe de prevenção	Diretor de PLD	Comitê, por indicadores
Comunicações ao COAF	Equipe de prevenção	Diretor de PLD	Controles internos
Travel rule nas transferências	Operações e tesouraria	Diretor de PLD	Controles internos
Trilha de evidência e guarda	**Cada dono de controle**	**Diretoria**	**Auditoria interna, independente de tudo**

A matriz é ponto de partida, ajustável à estrutura de cada casa, mas com duas regras de coerência inegociáveis: cada atividade tem um único aprovador claro, e quem executa não aprova a própria execução. A auditoria interna fica informada de tudo e independente de tudo, na lógica das três linhas: a operação executa os controles, a função de prevenção e os controles internos supervisionam, e a auditoria interna avalia com independência. Essa segregação é requisito de governança do regime e um dos primeiros pontos que o exame verifica.

O comitê mantém o programa vivo por indicadores: volume de alertas por cenário, tempo de tratamento, número de comunicações efetuadas, casos de informação de viagem ausente, resultado das rodadas de sanções, envelhecimento da fila. Indicador acompanhado em ata, com decisão registrada quando o número foge da meta, é evidência de supervisão ativa. A avaliação interna de risco fecha o ciclo de governança: revisada periodicamente, ela incorpora o que os indicadores revelam e recalibra os controles. Governança de PLD não é organograma: é esse circuito de detecção, decisão, registro e ajuste operando em ciclo contínuo, com nomes e alçadas definidos.

Um último ponto de disciplina: a governança também responde pelo que muda. Toda alteração relevante do programa, um cenário desligado, um limiar ajustado, uma classe de risco redefinida, passa por aprovação registrada, com justificativa e data. É

essa disciplina de mudança que permite ao exame independente confiar no período: sem ela, o auditor não sabe qual versão do controle operava em cada mês, e a conclusão de eficácia perde base. Programa maduro versiona seus controles como a tecnologia versiona seus sistemas.

SEÇÃO 10 · PARTE III · EVIDÊNCIA E GOVERNANÇA

Tecnologia e *ferramentas.*

A travel rule e o monitoramento on-chain deixam explícito o que sempre foi verdade em PLD: o programa é um requisito de sistema, não apenas de política. A prestadora precisa de capacidade técnica de capturar, transmitir, receber e validar dados, de rastrear fluxos na blockchain e de sustentar logs íntegros. A arquitetura de PLD é, portanto, decisão de engenharia tanto quanto de conformidade, e entra na conversa de segurança cibernética e de arquitetura de dados da casa.

Os componentes da *arquitetura*

COMPONENTE	FUNÇÃO	RISCO SE OPERAR ISOLADO
Cadastro e KYC	Identidade, qualificação e classe de risco do cliente	Monitoramento compara operações contra perfil desatualizado
Motor de monitoramento	Cenários, regras e geração de alertas	Alertas sem contexto de cadastro e de cadeia
Ferramenta on-chain	Rastreamento, escores de exposição e checagem de endereços	Escore que ninguém consome nas decisões
Protocolo de travel rule	Troca de mensagens de originador e beneficiário com contrapartes	Transferência liquidada sem mensagem ou sem validação
Triagem de sanções	Confronto de identidades e endereços com listas restritivas	Base envelhecida entre rodadas, hit sem tratamento
Gestão de casos	**Fila, alçadas, prazos e registro de desfecho**	**Decisões dispersas, sem trilha unificada**

O valor está menos em cada componente e mais nas integrações. O alerta relevante nasce do cruzamento: o cadastro diz quem é o cliente, a cadeia diz de onde vem o recurso, o motor cruza os dois e a gestão de casos garante o desfecho registrado. Quando as camadas operam isoladas, cada uma pode funcionar bem e o conjunto ainda assim falhar. O exame independente testa exatamente as costuras: o escore on-chain chega ao analista de alertas, a classe de risco do cliente calibra os cenários, a mensagem de travel rule bloqueia a liquidação quando falta.

A contratação de ferramentas de mercado, comum e legítima em análise on-chain e em protocolos de travel rule, não transfere a responsabilidade. A governança de terceirização exige contrato formal, avaliação do prestador, entendimento da metodologia da ferramenta e monitoramento do serviço. A prestadora precisa saber explicar como o escore é construído, que listas a triagem consome e com que atualização, e o que acontece quando o serviço fica indisponível. A responsabilidade não se terceiriza: perante a supervisão, quem responde pelo controle é a instituição autorizada, não o fornecedor.

> PARAMETRIZAÇÃO É DECISÃO DE RISCO
>
> Limiar da travel rule, régua de escore que dispara diligência, sensibilidade dos cenários, frequência da triagem: cada parâmetro dessas ferramentas é uma decisão de risco, com dono e justificativa na avaliação interna. Parâmetro herdado do padrão de fábrica, sem análise, é calibragem de conveniência. O exame pergunta quem decidiu, quando e com que fundamento.

Dois requisitos transversais fecham a arquitetura. O primeiro é a integridade dos logs: registros de acesso, de decisão e de mensagem precisam ser imutáveis ou versionados, porque são a matéria-prima da trilha de evidência. O segundo é a resiliência: o programa de PLD depende dos mesmos sistemas que a cibersegurança da casa protege, e o diretor responsável por segurança responde por um plano de resposta a incidentes testado, não apenas documentado. Uma indisponibilidade prolongada da esteira de monitoramento é, ela própria, um evento a registrar, com avaliação do período descoberto. Arquitetura madura é a que continua produzindo evidência mesmo quando algo falha.

O teste final da arquitetura é o da reconstrução: um terceiro, com acesso aos sistemas, consegue reconstituir qualquer decisão do programa, do parâmetro que disparou o alerta à alçada que o encerrou, sem depender de memória de pessoas. Quando a resposta é sim, a tecnologia cumpriu seu papel: transformou o programa de PLD em um processo que produz a própria prova.

SEÇÃO 11 · PARTE III · EVIDÊNCIA E GOVERNANÇA

PLD na asseguração e na *auditoria.*

O trabalho de auditoria ou de asseguração sobre um programa de PLD/FT avalia duas dimensões: o desenho dos controles e a sua eficácia operacional. Desenho é saber se o controle, tal como concebido, é capaz de mitigar o risco. Eficácia é saber se ele operou de forma consistente ao longo do período. Uma política bem escrita que não é seguida na prática reprova no segundo teste. A distinção importa porque os dois exames usam evidências diferentes: o desenho se avalia lendo e confrontando; a eficácia se testa em amostras da operação real.

No regime das prestadoras, esse exame deixou de ser opcional. O processo de autorização exige relatório de asseguração independente sobre os controles, emitido por firma registrada na CVM, exigível nos pedidos a partir de junho de 2026. PLD/FT e sanções são o núcleo desse trabalho: não basta ter política, é preciso evidência de que o controle opera. O padrão técnico dos trabalhos de asseguração é o das normas NBC TO 3000 e ISAE 3000, que disciplinam como o auditor independente obtém segurança sobre um objeto que não é demonstração financeira: no caso, o programa de prevenção e seus controles.

O que o auditor *pede*

FRENTE	DOCUMENTO OU EVIDÊNCIA
Governança	Designação do diretor, políticas aprovadas com data, atas do comitê e indicadores acompanhados
Risco	Avaliação interna de risco, matriz de fatores e critérios de segmentação da carteira
KYC	Amostra de dossiês por classe de risco, com aprovação, classificação e atualização
Monitoramento	Inventário de cenários, trilha de alertas com disposição e indicadores da fila
Sanções	Logs de execução da triagem e tratamento dos apontamentos
Travel rule	Amostra de transferências com informação de originador e beneficiário e tratamento das incompletas
COAF	**Comunicações com data de detecção e de envio, e decisões fundamentadas de não comunicar**

Os testes de eficácia seguem a lógica da amostra dirigida ao risco. Em travel rule, o auditor seleciona transferências acima do limiar e verifica a mensagem completa; seleciona operações no entorno do corte e verifica a parametrização; seleciona casos de mensagem incompleta e verifica o tratamento. Em monitoramento, percorre alertas da fila até o desfecho registrado. Em sanções, reexecuta a lógica sobre a base e compara com os apontamentos tratados. Em KYC, confronta o dossiê real com o que a política promete para aquela classe de risco. O fio condutor é sempre o mesmo: da política ao registro, do registro à operação.

> O PEDIDO NÃO É SURPRESA
>
> Toda linha da tabela acima é previsível. A instituição que a trata como checklist vivo, mantido durante o ano, entrega o exame em dias. A que a trata como corrida de fim de ciclo entrega tarde, com lacuna, e paga em ressalva e em prazo. A diferença entre as duas não é competência técnica. É antecipação.

A preparação prática recomendada é a sala de dados por frente: evidência organizada e nomeada, conciliações e logs por período, políticas com data de aprovação, amostras de mensagens de travel rule, atas e indicadores. Sala de dados pronta encurta o campo do auditor e reduz o custo do trabalho. E há um efeito de segunda ordem que as administrações maduras percebem: o mesmo material que instrui a asseguração serve à supervisão, ao conselho e à auditoria das demonstrações financeiras. A evidência de PLD não é um custo do exame; é o ativo de credibilidade da prestadora no novo regime, construído na rotina e colhido no pedido de autorização.

Uma nota de calendário fecha a seção. A exigência de asseguração no pedido e o teto de protocolo em 30/10/2026 se combinam: o trabalho de asseguração precisa de período de operação para testar eficácia, e período de operação não se improvisa. A

prestadora que deixa o exame para o fim descobre que não há o que testar, porque os controles acabaram de nascer. O cronograma realista posiciona a asseguração depois de alguns meses de operação evidenciada, com folga antes do protocolo.

PARTE IV

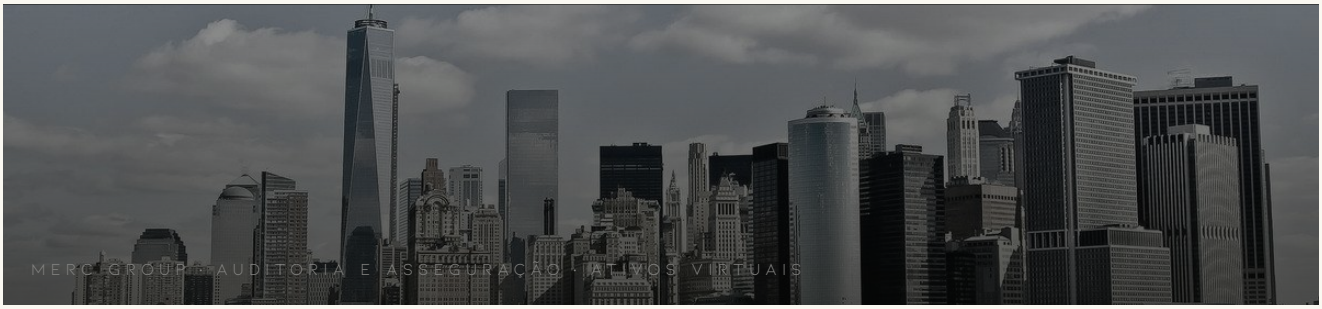
IV

Implantar, responder e *manter.*

O programa auditável, as dúvidas mais comuns e o checklist de implantação.

SEÇÃO 12 · PARTE IV · PRÁTICA

Um programa *auditável.*



Um programa de PLD auditável não nasce de uma compra de sistema nem de uma política bem redigida. Nasce de uma sequência de implantação que respeita as dependências entre os controles e que produz evidência desde o primeiro dia. A ordem importa: avaliação de risco antes de calibragem, cadastro antes de monitoramento, processo antes de ferramenta. Quem inverte a ordem instala tecnologia sobre o vazio e descobre, no exame, que tem sistema sem controle.

1. **Avaliação interna de risco.** Mapear clientes, produtos, canais, jurisdições e tecnologia da operação real. É o alicerce de todas as calibragens.
2. **Governança.** Designar o diretor responsável, aprovar as políticas, definir alçadas, indicadores e a matriz de responsabilidades.
3. **KYC e segmentação.** Implantar identificação, qualificação e classes de risco, com o regime de diligência ampliada operacionalizado, inclusive para pessoas jurídicas sensíveis.
4. **Monitoramento e sanções.** Ativar cenários rastreáveis à avaliação de risco, integrar a análise on-chain e disciplinar a governança de alertas e as rodadas de triagem.
5. **Travel rule.** Desenhar o processo de captura, transmissão, recepção e exceção, seguindo o cronograma do faseamento: doméstico primeiro, internacional na sequência.
6. **Trilha e exame.** Consolidar o inventário de evidências, montar a sala de dados e submeter o conjunto à asseguração independente antes do protocolo.

Um caso anonimizado ilustra o padrão de falha. Considere uma plataforma que sempre teve política de PLD/FT escrita e um sistema de monitoramento contratado, e que por isso se considerava preparada. Quando a asseguração independente se aproxima, o exame revela: a diligência ampliada para clientes corporativos de alto risco nunca foi operacionalizada; a fila de alertas se acumula sem tratamento tempestivo e sem trilha do desfecho; a triagem de sanções está configurada, mas não há evidência de que foi rodada com regularidade; e a estrutura para a travel rule não foi montada, porque o prazo parecia distante. Nenhum desses pontos indica má-fé. Indicam que ter política não é ter controle. O programa se prova pela execução evidenciada, não pelo documento arquivado.

ERRO FREQUENTE	CONSEQUÊNCIA	CORREÇÃO
Tratar PLD como manual de gaveta	Estrutura sem evidência e sem capacidade de travel rule	Governança dedicada, monitoramento vivo e capacidade técnica de viagem da informação
EDD de pessoa jurídica sem procedimento	Porta aberta para estruturas de ocultação	Regime de diligência ampliada definido, com alçada e evidência
Fila de alertas sem tratamento	Ilusão de controle e omissão documentada	Prazos, alçadas e registro de desfecho por alerta
Triagem de sanções sem log	Controle não comprovável em exame	Log de execução por rodada e trilha de cada apontamento
		Reter, devolver ou analisar antes de disponibilizar

ERRO FREQUENTE	CONSEQUÊNCIA	CORREÇÃO
Deixar passar transferência sem mensagem	Falha de prevenção e exposição de conduta	
Evidência reconstruída na véspera	**Ressalva por falta de registro contemporâneo**	**Trilha nascendo com a operação, guardada de forma íntegra**

02/02/2026
VIGÊNCIA
Entrada em vigor das Resoluções BCB 519, 520 e 521 e das obrigações do regime.

270 dias
JANELA
Janela de protocolo do pedido de autorização, contada da vigência das resoluções.

30/10/2026
PRAZO FINAL
Teto improrrogável para o protocolo pelas prestadoras em atividade.

O ERRO CARO É O DE TEMPO

Quase todo erro da tabela é barato se corrigido cedo e caro se descoberto tarde. Trilha, governança de alertas e travel rule não se reconstroem depois do fato: o período sem registro fica descoberto para sempre. Comece pelos controles que, se faltarem no período, não têm conserto retroativo.

A síntese da implantação cabe em uma linha: comece pela avaliação de risco, faça cada controle nascer com a sua evidência e trate o calendário como restrição de engenharia, não como referência distante. O restante deste guia, o checklist adiante em particular, transforma essa síntese em itens verificáveis.

SEÇÃO 13 · PARTE IV · PRÁTICA

Perguntas *frequentes.*

As perguntas abaixo concentram as dúvidas mais frequentes de diretores de PLD, compliance e auditoria interna sobre o programa de prevenção e a travel rule no regime das prestadoras. As respostas resumem o que o guia desenvolve em profundidade nas seções anteriores e servem de material de apoio para comitês, treinamentos internos e conversas com a administração sobre as prioridades do programa.

A partir de quando as PSAVs precisam cumprir as regras de PLD/FT?

O marco foi estabelecido pela Lei 14.478/2022 e regulamentado pelo Decreto 11.563/2023. As Resoluções BCB 519, 520 e 521, publicadas em 10/11/2025, entram em vigor em 02/02/2026, quando passam a valer plenamente as obrigações de prevenção para as prestadoras, com protocolo do pedido de autorização até 30/10/2026.

O programa pode ser mais simples que o de um banco?

Não. A exigência é de política equivalente à de instituição financeira: conhecimento do cliente proporcional ao risco, monitoramento de operações, triagem de sanções e comunicação de suspeitas ao COAF. O regime traz o mercado de cripto para o mesmo patamar de prevenção das instituições reguladas.

O que é a travel rule e de onde ela vem?

É a regra que exige a viagem da informação de originador e beneficiário nas transferências de ativos virtuais acima de um limiar definido. Tem origem na Recomendação 16 do GAFI, complementada pela Recomendação 15, que trouxe as prestadoras de ativos virtuais para o perímetro internacional de prevenção.

Por que a travel rule é difícil de implementar?

Porque integra identidade e transferência em uma operação que nasceu, tecnicamente, para funcionar sem esse elo. Exige capacidade de capturar, transmitir, receber e validar dados, integração com contrapartes em protocolos nem sempre compatíveis e tratamento definido para mensagens incompletas.

Como funciona o faseamento da rastreabilidade?

Há prazos distintos por tipo de operação: o faseamento prevê prazo até 2027 para operações domésticas e até 2028 para operações internacionais. Isso pede um cronograma de implementação por etapas, com a preparação começando antes do prazo, porque a integração técnica consome tempo.

Por que as carteiras autocustodiadas são um problema?

Porque não têm instituição por trás. Quando uma das pontas é uma carteira controlada diretamente pelo usuário, não existe contraparte institucional para trocar a mensagem exigida. A prestadora precisa de controles compensatórios: comprovação de titularidade, diligência reforçada por valor e análise on-chain intensiva.

Qual a diferença entre testar desenho e testar eficácia?

Testar o desenho é avaliar se o controle, como concebido, mitiga o risco. Testar a eficácia é verificar se ele operou de forma consistente no período, com amostras da operação real. Uma política adequada no papel reprova no teste de eficácia se não for seguida na prática.

Que evidência sustenta o cumprimento das obrigações?

A trilha: logs do monitoramento, alertas com disposição registrada, decisões fundamentadas, comunicações ao COAF com datas de detecção e envio, logs das rodadas de sanções e registros da travel rule, incluindo o tratamento das mensagens incompletas. Onde não há registro, o auditor não conclui pela eficácia.

A comunicação ao COAF tem meta de volume?

Não há meta, mas há leitura de coerência. Um programa que nunca comunica nada, em um mercado de risco elevado, é em si um sinal de alerta: ou o monitoramento não detecta, ou a fila não é tratada. A decisão de não comunicar também precisa ficar registrada e fundamentada.

Contratar ferramenta de análise on-chain resolve o monitoramento?

Não sozinha. A ferramenta entrega rastreamento, escores e checagem de endereços, mas a responsabilidade permanece da prestadora: parametrização justificada na avaliação interna de risco, integração com o cadastro e a esteira, governança dos alertas e trilha das decisões. Responsabilidade não se terceiriza.

SEÇÃO 14 · PARTE IV · PRÁTICA

Checklist de *implantação.*

Use o checklist antes do protocolo do pedido de autorização e a cada ciclo de revisão do programa. Cada item é acionável e verificável: ou a evidência existe e se localiza, ou o item está aberto. A ordem segue a lógica do guia, da governança à trilha.

GOVERNANÇA E RISCO

- ✓ Diretor responsável por PLD/FT formalmente designado, com atribuições documentadas
- ✓ Política de PLD/FT aprovada pela instância competente, com data e versão controlada
- ✓ Avaliação interna de risco documentada, aderente à carteira real e revisada periodicamente
- ✓ Matriz de responsabilidades com aprovador único por atividade e segregação entre execução e aprovação
- ✓ Indicadores do programa acompanhados em comitê, com decisões registradas em ata

KYC E DILIGÊNCIA

- ✓ Identificação e qualificação implantadas, com perfil esperado e origem de recursos registrados
- ✓ Segmentação por classe de risco refletida no sistema, não apenas na política
- ✓ Regime de diligência ampliada operacionalizado, inclusive para pessoas jurídicas de maior risco
- ✓ Atualização cadastral periódica por classe de risco, com trilha de execução

MONITORAMENTO E SANÇÕES

- ✓ Cenários de monitoramento rastreáveis às tipologias da avaliação interna de risco
- ✓ Governança de alertas com prazos, alçadas e registro de desfecho por alerta
- ✓ Análise on-chain integrada: rastreamento, escores de exposição e checagem de endereços
- ✓ Triagem de sanções na entrada, na base e na transação, com log de cada rodada
- ✓ Tratamento de apontamentos registrado, inclusive o descarte de falsos positivos
- ✓ Fila de alertas sem backlog envelhecido; envelhecimento medido e reportado

TRAVEL RULE

- ✓ Processo de captura, transmissão, recepção e validação de dados implantado na esteira
- ✓ Limiar parametrizado conforme o regime, com teste de operações no entorno do corte
- ✓ Política de mensagem incompleta definida: reter, questionar, devolver ou recusar, com registro
- ✓ Controles compensatórios para carteiras autocustodiadas, com comprovação de titularidade
- ✓ Cronograma do faseamento cumprido: fluxo doméstico até 2027, internacional até 2028
- ✓ Cobertura de contrapartes mapeada e falhas de interoperabilidade tratadas

COAF E TRILHA

- ✓ Comunicações ao COAF com data de detecção, data de envio e fundamentação
- ✓ Decisões de não comunicar registradas e fundamentadas
- ✓ Inventário de evidências por controle: o que comprova, onde guarda, por quanto tempo
- ✓ Logs críticos íntegros e imutáveis: acessos, decisões e mensagens de travel rule

- ✓ Sala de dados organizada por frente, pronta para asseguração e supervisão

CÂMBIO E FRONTEIRA

- ✓ Operações classificadas na esteira quanto ao tratamento cambial da Res. BCB 521, com motivo registrado
- ✓ Identificação de partes, registro e reporte das operações classificadas como câmbio
- ✓ Conciliação de fechamento entre operações classificadas como câmbio e operações reportadas

Item marcado significa evidência que existe e se localiza; a lista inteira marcada não significa programa perfeito, significa programa demonstrável. O item aberto identificado antes do exame é tarefa; o mesmo item descoberto pelo auditor é achado, e descoberto pela supervisão é problema. A diferença entre os três cenários é apenas quem encontrou primeiro.

SEÇÃO 15 · PARTE IV · PRÁTICA

Próximos passos com a *MERC.*

Quando o programa de PLD/FT precisa resistir ao exame do regulador e do auditor, a MERC Group atua na avaliação independente de programas de prevenção no contexto das prestadoras de serviços de ativos virtuais. O trabalho combina o conhecimento da norma com o entendimento técnico do ambiente cripto, o que permite testar não apenas a formalidade das políticas, mas a operação real dos controles.

A atuação segue uma sequência lógica. O **diagnóstico** compara o programa existente com as exigências do regime e devolve um mapa objetivo de lacunas, priorizado por risco e por prazo. A **prontidão** acompanha a remediação: operacionalizar a diligência ampliada, disciplinar a governança de alertas, montar o processo de travel rule dentro do cronograma do faseamento e construir a trilha de evidência que faltava. A **asseguração independente**, conduzida sob NBC TO 3000, testa desenho e eficácia dos controles e produz o relatório que instrui o pedido de autorização. E a **auditoria** das demonstrações financeiras completa o ciclo, com a visão integrada de quem examina a prestadora como instituição regulada.

- Revisão de desenho dos controles de PLD frente às exigências regulatórias aplicáveis
- Testes de eficácia operacional do KYC, do monitoramento, das sanções e da travel rule
- Avaliação da trilha de evidência que sustenta comunicações ao COAF e decisões sobre alertas
- Análise da cobertura do monitoramento e da integração com a análise on-chain
- Asseguração NBC TO 3000 sobre o programa, no padrão exigido no processo de autorização

O objetivo é oferecer à administração e à governança uma visão objetiva sobre onde o programa está sólido e onde a evidência precisa ser fortalecida, antes que a supervisão o faça. A disciplina é a de quem já examinou programas de prevenção em instituições reguladas: da política ao registro, do registro à operação.

O formato do trabalho se ajusta ao estágio da prestadora. Quem está no início da adequação normalmente contrata o diagnóstico e o acompanhamento de prontidão, com entregas periódicas sobre o avanço das lacunas. Quem já opera os controles contrata a asseguração para o pedido de autorização, precedida de uma pré-avaliação que evita submeter ao exame um programa ainda verde. E quem já foi autorizado mantém ciclos recorrentes de avaliação independente, porque o programa de PLD/FT envelhece: listas mudam, tipologias evoluem, o faseamento da travel rule avança e a avaliação interna de risco precisa acompanhar. Em todos os formatos, o compromisso é o mesmo: conclusões escritas, baseadas em evidência, sem complacência e sem alarmismo.

> FALE COM A MERC
>
> Para agendar uma conversa técnica sobre diagnóstico, prontidão ou asseguração do programa de PLD/FT da sua prestadora: www.mercgroup.com.br/contato · contato@mercgroup.com.br. Think growth. Think MERC.

MERCGROUP

Controle bom deixa *trilha.*

Quando o programa de PLD/FT precisa resistir ao exame do regulador e do auditor, os sócios da MERC avaliam desenho, efetividade e trilha de evidência, do KYC à comunicação ao COAF.

CONTATO	contato@mercgroup.com.br
TELEFONE E WHATSAPP	+55 11 98196 1447
CONTEÚDO TÉCNICO	www.mercgroup.com.br/insights
ENDEREÇO	Av. Adolfo Pinheiro, 1001 · Alto da Boa Vista · São Paulo SP

Guia técnico **MERC Group · Série Ativos Virtuais** · Material informativo de caráter geral: não constitui opinião de auditoria, parecer jurídico ou recomendação para caso concreto. Não cita instituições nominalmente; exemplos são ilustrativos e anonimizados.
Edição Agosto de 2026 · Think Growth. **Think MERC.**