

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

# Política de Prevenção a Fraude

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

## Sumário

|                                                                |          |
|----------------------------------------------------------------|----------|
| <b>1. Objetivo</b>                                             | <b>2</b> |
| <b>2. Abrangência</b>                                          | <b>2</b> |
| <b>3. Termos e Definições</b>                                  | <b>2</b> |
| <b>4. Princípios</b>                                           | <b>3</b> |
| <b>5. Tipologias de Fraude</b>                                 | <b>3</b> |
| <b>6. Avaliação de Risco de Fraude</b>                         | <b>4</b> |
| <b>7. Controles Preventivos</b>                                | <b>5</b> |
| 7.1 Onboarding e cadastro                                      | 5        |
| 7.2 Acesso e autenticação                                      | 5        |
| 7.3 Operações e transferências                                 | 5        |
| 7.4 Colaboradores e terceiros                                  | 5        |
| <b>8. Retenção Cautelar de Transferências</b>                  | <b>5</b> |
| <b>9. Detecção, Investigação e Resposta</b>                    | <b>6</b> |
| <b>10. Interfaces com PLD/FT e com Segurança da Informação</b> | <b>7</b> |
| <b>11. Compartilhamento de Dados sobre Indícios de Fraude</b>  | <b>7</b> |
| <b>12. Relacionamento com o Cliente e Remediação</b>           | <b>8</b> |
| <b>13. Treinamento e Conscientização</b>                       | <b>8</b> |
| <b>14. Revisão</b>                                             | <b>8</b> |
| <b>15. Normas de Referência</b>                                | <b>9</b> |
| <b>16. Vigência</b>                                            | <b>9</b> |
| <b>17. Controle e Histórico de Versões</b>                     | <b>9</b> |

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

## 1. Objetivo

Esta Política estabelece os princípios, as responsabilidades e os controles da Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. ("Trace Finance") para prevenir, detectar, conter, investigar e remediar fraudes e golpes relacionados aos seus produtos, serviços, canais e relacionamentos.

Constitui a política de prevenção a fraudes exigida pelo art. 43 da Resolução BCB nº 520/2025 e fixa as diretrizes para o registro e o compartilhamento de dados e informações sobre indícios de fraude, na forma da regulamentação aplicável.

## 2. Abrangência

Esta Política aplica-se aos administradores, colaboradores, estagiários, aprendizes e prestadores de serviço da Trace Finance e a todos os seus produtos, serviços, canais, sistemas e relacionamentos com clientes, contrapartes, parceiros e fornecedores, em moeda fiduciária e em ativos virtuais.

Alcança a fraude externa, praticada por clientes, contrapartes ou terceiros, a fraude interna, praticada por colaborador ou prestador de serviço, isoladamente ou em conluio, e os golpes aplicados a clientes que envolvam os serviços da Trace Finance.

A prevenção à lavagem de dinheiro, a segurança da informação e cibernética e a proteção de dados pessoais são disciplinadas em normativos próprios. Esta Política trata das interfaces com esses temas.

## 3. Termos e Definições

| <b>Termo</b>             | <b>Definição</b>                                                                                                                                                                                                                                               |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Fraude</b>            | Ato ardiloso, enganoso ou de má-fé, praticado por ação ou omissão, mediante inverdade, abuso de poder, quebra de confiança, burla de regras ou outro meio inidôneo, com o propósito de dissimular fatos ou obter vantagem indevida, para si ou para terceiros. |
| <b>Golpe</b>             | Fraude em que o próprio cliente é induzido, por engenharia social, a autorizar operação ou transferência em benefício do fraudador.                                                                                                                            |
| <b>Indício de fraude</b> | Fato, padrão ou informação que indique a ocorrência ou a tentativa de fraude, ainda não confirmada por investigação.                                                                                                                                           |

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

| <b>Termo</b>             | <b>Definição</b>                                                                                                        |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>Fraude interna</b>    | Fraude praticada por administrador, colaborador ou prestador de serviço, isoladamente ou em conluio com terceiros.      |
| <b>Tomada de conta</b>   | Acesso indevido à conta, à credencial ou ao canal de um cliente legítimo para realizar operações sem a sua autorização. |
| <b>Conta de passagem</b> | Conta ou carteira de interposta pessoa utilizada para receber e repassar recursos ou ativos de origem fraudulenta.      |
| <b>Retenção cautelar</b> | Retenção temporária de transferência de ativos virtuais para análise de risco, na forma desta Política.                 |
| <b>Perda por fraude</b>  | Valor efetivamente perdido pela Trace Finance ou por seus clientes em decorrência de fraude, líquido das recuperações.  |

## 4. Princípios

- Abordagem baseada em risco.** Os controles são proporcionais à exposição demonstrada pela avaliação de risco de fraude.
- Prevenção antes da execução.** Controles preventivos atuam antes da ativação do relacionamento e da liquidação das operações sempre que possível.
- Contenção imediata.** Diante de indício relevante, a contenção prevalece sobre a conveniência operacional, sem prejuízo dos direitos do cliente.
- Segregação de funções.** Quem executa a operação não libera a operação retida nem investiga a própria atuação.
- Rastreabilidade.** Eventos, decisões, perdas, recuperações e compartilhamentos produzem registro verificável.
- Tolerância zero à fraude interna.** A fraude praticada por colaborador ou prestador é apurada e sancionada independentemente de cargo ou desempenho.
- Proteção de dados.** O tratamento e o compartilhamento de dados observam a finalidade de prevenção a fraudes, a necessidade e a Lei nº 13.709/2018.

## 5. Tipologias de Fraude

A Trace Finance mantém mapa de tipologias que contempla, no mínimo, as categorias abaixo:

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

| <b>Categoria</b>                             | <b>Exemplos</b>                                                                                                                                                                                                                                                                                          |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identidade e onboarding</b>               | Identidade sintética, documento falso ou furtado, uso de interposta pessoa, empresa de fachada e personificação de representante legal.                                                                                                                                                                  |
| <b>Comprometimento de conta</b>              | Tomada de conta, phishing, uso de credenciais vazadas, sequestro de sessão, troca de dispositivo e engenharia social.                                                                                                                                                                                    |
| <b>Instruções de pagamento e de carteira</b> | Comprometimento de e-mail corporativo, alteração indevida de dados bancários ou de endereço de carteira, ordens falsas em nome de cliente ou de contraparte.                                                                                                                                             |
| <b>Transferências e liquidação</b>           | Transferências não autorizadas, contas e carteiras de passagem, devolução indevida e liquidação contra recursos de origem fraudulenta.                                                                                                                                                                   |
| <b>Golpes contra clientes</b>                | Falso suporte, golpes de investimento, falsas promessas de rendimento e golpe de recuperação de perdas.                                                                                                                                                                                                  |
| <b>Fraude interna e de terceiros</b>         | Conluio, abuso de acesso privilegiado, manipulação de parâmetros, alteração indevida de registros e fraude de fornecedor.                                                                                                                                                                                |
| <b>Fraude de mercado</b>                     | Liquidez fictícia, negociação circular e manipulação de preços de ativos virtuais. A prevenção ao abuso de mercado e a comunicação de práticas espúrias ao Banco Central do Brasil observam a Política Integrada de Atividades Específicas e Custódia, na forma do art. 70 da Resolução BCB nº 520/2025. |

## 6. Avaliação de Risco de Fraude

O risco de fraude é avaliado por produto, canal, segmento de cliente e processo, considerando as tipologias mapeadas, os eventos e as perdas registrados e a efetividade dos controles. A avaliação utiliza a escala de quatro níveis (Baixo, Médio, Alto e Crítico) adotada na gestão de riscos da Trace Finance e é atualizada anualmente e diante de novo produto, novo canal, evento relevante ou mudança de tipologia.

Os resultados alimentam a calibragem das regras de detecção, a definição de limites e a avaliação prévia de novos produtos e serviços, e são considerados na avaliação de risco de PLD/FT quando houver sobreposição de tipologias.

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

## 7. Controles Preventivos

### 7.1 Onboarding e cadastro

- a. validação de identidade e de documentos por fontes independentes, inclusive biometria e verificação de dispositivo quando aplicável;
- b. confirmação da existência, da atividade e dos representantes de clientes pessoas jurídicas;
- c. consulta a bases de indícios de fraude e a listas internas de restrição antes da ativação.

### 7.2 Acesso e autenticação

- a. autenticação forte e baseada em risco para acesso a canais e para eventos sensíveis;
- b. controles reforçados para alteração de dados cadastrais, de dados bancários, de endereço de carteira, de dispositivo e de representantes;
- c. confirmação, por canal independente previamente cadastrado, de alteração de instrução de pagamento ou de carteira de destino.

### 7.3 Operações e transferências

- a. limites por cliente, por operação e por período, e controles de velocidade;
- b. listas de endereços de saque autorizados e período de espera para endereços novos;
- c. triagem on-chain de origem e destino dos ativos;
- d. revisão humana de operações fora do padrão do cliente ou com sinais de golpe.

### 7.4 Colaboradores e terceiros

- a. segregação de funções e gestão de acessos privilegiados, com revisão periódica;
- b. diligência reforçada para funções e prestadores com acesso a sistemas, parâmetros ou movimentação de ativos;
- c. monitoramento de acessos e de alterações em registros e parâmetros sensíveis.

## 8. Retenção Cautelar de Transferências

A partir de 1º de janeiro de 2027, as transferências de ativos virtuais destinadas a prestadora de serviços de ativos virtuais no exterior ou a carteira autocustodiada são retidas pelo prazo de até 24 horas, para análise de risco, quando o valor superar USD 10.000 ou equivalente, considerado

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

individualmente ou pelo total do cliente no dia, e nas demais situações definidas pela avaliação de risco da Trace Finance, na forma da Resolução BCB nº 142/2021, com a redação dada pela Resolução BCB nº 584/2026.

O cliente é informado da retenção. A transferência pode ser liberada antes do prazo quando a análise, documentada, concluir que os elementos de risco não justificam a retenção, considerados os perfis de risco do cliente, da operação, da contraparte e da jurisdição. A inclusão do endereço de destino na lista de carteiras previamente validadas pela Trace Finance (whitelist), com verificação de titularidade, constitui critério de liberação antecipada e não dispensa da retenção. A decisão de liberação é registrada por operação, ainda que de forma sistematizada, e a liberação antecipada é afastada diante de sinais de tomada de conta, de alteração recente de credenciais, de dispositivo ou de dados cadastrais, de comportamento atípico do cliente ou de valor elevado definido pela Gestão de Riscos, caso em que depende de dupla aprovação. As transferências destinadas a prestadoras de serviços de ativos virtuais autorizadas a funcionar no País não estão sujeitas à retenção cautelar. A retenção não substitui o bloqueio decorrente de sanções nem a análise de PLD/FT.

## 9. Detecção, Investigação e Resposta

| Fase                     | Ações mínimas                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Detecção</b>          | Regras e modelos de detecção, relatos de clientes, de colaboradores e de parceiros, inteligência externa, bases de indícios de fraude e monitoramento on-chain. |
| <b>Classificação</b>     | Severidade, valor envolvido, clientes afetados, risco sistêmico e obrigações de registro e comunicação.                                                         |
| <b>Contenção</b>         | Suspensão de acesso, restrição de saque, retenção ou bloqueio de operação, bloqueio de beneficiário ou de endereço e aviso a parceiros.                         |
| <b>Investigação</b>      | Análise de contas, dispositivos, carteiras, contrapartes, trilhas de acesso e cadeia transacional, com dossiê do caso.                                          |
| <b>Decisão</b>           | Remediação do cliente, recuperação de valores, encerramento do relacionamento, medidas disciplinares e comunicações devidas.                                    |
| <b>Lições aprendidas</b> | Análise de causa raiz e ajuste de regras, limites, produto, comunicação e treinamento.                                                                          |

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

Os eventos são classificados na escala de quatro níveis. Os eventos Altos são reportados ao Diretor de Riscos e os Críticos também à Diretoria e ao Comitê de Compliance. A investigação de fraude interna é conduzida por área independente da envolvida, com preservação das evidências.

## 10. Interfaces com PLD/FT e com Segurança da Informação

- PLD/FT:** todo evento de fraude confirmado ou com indício relevante é comunicado a Compliance em até 24 horas da sua identificação, para avaliação de comunicação ao Coaf. Os fluxos são cumulativos, vedada a substituição de um pelo outro, e os prazos de PLD/FT contam da data em que o indício foi identificado. A decisão de comunicar é do Diretor responsável por PLD/FTP.
- Relacionamento:** quando o evento envolver indício de LD/FT, a decisão sobre a continuidade do relacionamento e a comunicação ao parceiro bancário que realiza a operação cabem a Compliance, na forma do programa de PLD/FT.
- Vedação de ciência:** a comunicação ao cliente sobre retenção, bloqueio ou encerramento não revela a existência de análise ou de comunicação ao Coaf.
- Sanções:** correspondência em lista de sanções identificada durante a investigação segue o fluxo de indisponibilidade de ativos, que prevalece sobre as medidas desta Política.
- Incidentes de segurança:** a fraude decorrente de incidente de segurança da informação é tratada também no fluxo de resposta a incidentes, inclusive quanto às comunicações a autoridades e a titulares de dados.

## 11. Compartilhamento de Dados sobre Indícios de Fraude

A Trace Finance registra e compartilha dados e informações sobre indícios de fraude na forma da Resolução Conjunta nº 6/2023 e da Resolução BCB nº 343/2023, conforme estendida às prestadoras de serviços de ativos virtuais pela Resolução BCB nº 552/2026, com implementação até 30 de outubro de 2026. O registro contempla, quando aplicável, a identificação de quem executou ou tentou executar a fraude, a descrição dos indícios e os dados da conta ou da carteira destinatária.

O compartilhamento observa a Lei nº 13.709/2018 e os princípios de finalidade, necessidade, qualidade e segurança. Cada registro identifica origem, conteúdo, destinatário, finalidade, data e responsável, com controle de acesso e trilha de consulta.

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

As informações recebidas de terceiros são insumo de risco e não produzem, isoladamente, decisão adversa automática contra o cliente, sem análise contextual e tratamento de falso positivo.

A Trace Finance mantém contrato com o provedor do sistema eletrônico de compartilhamento de dados e informações sobre indícios de fraudes e encaminha ao Banco Central do Brasil a declaração mensal de conformidade, inclusive quando não houver registros no período, nos prazos da Resolução BCB nº 343/2023.

## 12. Relacionamento com o Cliente e Remediação

O cliente afetado é informado das medidas que o atingem, por canal oficial, sem divulgação de informações protegidas por sigilo. As reclamações e os relatos de fraude recebem protocolo, prazo de resposta e tratamento prioritário quando houver risco de nova perda.

A remediação ao cliente, a recuperação de valores junto a parceiros e o eventual ressarcimento são decididos com base na investigação, com registro da fundamentação.

## 13. Treinamento e Conscientização

Os colaboradores recebem treinamento anual sobre prevenção a fraudes, com conteúdo específico para as áreas de operações, atendimento, tecnologia e para funções com acesso a movimentação de ativos ou a parâmetros sensíveis. Os conteúdos são atualizados diante de novas tipologias identificadas. A conclusão observa o prazo, a nota mínima e o escalonamento aplicáveis aos treinamentos obrigatórios da Trace Finance, com registro de conclusão e de aproveitamento.

A Trace Finance divulga a clientes, usuários e fornecedores informações sobre boas práticas e sobre os riscos de fraudes e golpes, nos termos do art. 43, §2º, III, da Resolução BCB nº 520/2025.

## 14. Revisão

Esta Política é revisada anualmente, com aprovação pela Diretoria, formalizada em ata, após deliberação prévia do Comitê de Compliance, e de forma extraordinária diante de alteração normativa, de evento Crítico, de nova tipologia relevante ou de mudança nos produtos, canais ou modelo de negócio.

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

## 15. Normas de Referência

Lei nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais.

Lei nº 14.478/2022: diretrizes para a prestação de serviços de ativos virtuais.

Resoluções BCB nº 519, 520 e 521/2025: autorização, funcionamento e operações no mercado de câmbio das prestadoras de serviços de ativos virtuais.

Resolução Conjunta nº 6/2023 e Resolução BCB nº 343/2023: compartilhamento de dados e informações sobre indícios de fraudes.

Resolução BCB nº 142/2021 (alterada pela Resolução BCB nº 584/2026): procedimentos e controles de prevenção a fraudes, inclusive retenção cautelar de transferências de ativos virtuais, com vigência a partir de 1º de janeiro de 2027.

Resolução BCB nº 85/2021, aplicável por força da Resolução BCB nº 552/2026: política de segurança cibernética.

Circular BCB nº 3.978/2020: prevenção à lavagem de dinheiro e ao financiamento do terrorismo, quanto às interfaces com a prevenção à lavagem de dinheiro.

## 16. Vigência

Esta Política entra em vigor na data de sua publicação, após a aprovação pela Diretoria da Trace Finance, formalizada em ata, com deliberação prévia do Comitê de Compliance, e permanece vigente até sua revisão ou revogação expressa. As regras de retenção cautelar de transferências aplicam-se a partir de 1º de janeiro de 2027.

## 17. Controle e Histórico de Versões

| Versão | Data       | Histórico de Alterações/Inclusões | Resp. Aprovação                                     |
|--------|------------|-----------------------------------|-----------------------------------------------------|
| 1.0    | 15/10/2026 | Emissão inicial.                  | Diretoria, após deliberação do Comitê de Compliance |

|                                                                                   |                                       |                        |
|-----------------------------------------------------------------------------------|---------------------------------------|------------------------|
|  | <b>Política de Prevenção a Fraude</b> | <b>RSC-POL-001-FIN</b> |
| Data da Publicação:<br>15/10/2026                                                 | <b>Gestão de Riscos</b>               | Público                |

---