Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo

Última atualização: 03 de setembro de 2026 | Versão 1.0

Empresa	Mistic Tecnologias LTDA — CNPJ 53.626.720/0001-23
Nome de operação	MisticPay
Endereço	Avenida Portugal, 1148 - Quadra 29, Lote 1E, Sala C2501 - Edifício Orion Business - CEP 74150-030 - Goiânia/GO
Objeto	Prevenção, identificação, avaliação e mitigação de riscos de lavagem de dinheiro e financiamento do terrorismo nas atividades e relacionamentos da empresa.
Aprovação	Administração da Mistic Tecnologias
Revisão	No mínimo anual e sempre que houver alteração relevante no negócio, no perfil de risco ou na legislação aplicável.

A Mistic Tecnologias adota uma abordagem baseada em risco para prevenir a utilização de seus produtos, serviços, canais, contas, integrações e relações comerciais para fins de lavagem de dinheiro, financiamento do terrorismo ou outras práticas ilícitas. Esta política estabelece princípios, responsabilidades, controles e procedimentos mínimos a serem observados pela empresa e por terceiros que atuem em seu nome.

Nota de enquadramento: esta política foi estruturada considerando a legislação brasileira e, quando aplicável ao enquadramento regulatório da empresa, as normas do Banco Central do Brasil e do Conselho de Controle de Atividades Financeiras (Coaf). A existência desta política não constitui, por si só, declaração de autorização ou supervisão específica da empresa pelo Banco Central.

1. OBJETIVO E FINALIDADE

São objetivos desta política:

- prevenir a utilização da Mistic Tecnologias para ocultação ou dissimulação da origem, localização, disposição, movimentação ou propriedade de recursos de origem ilícita;
- reduzir a exposição da empresa a riscos de lavagem de dinheiro (LD) e financiamento do terrorismo (FT);
- estabelecer critérios de identificação, qualificação, classificação e monitoramento de clientes, parceiros, beneficiários e operações;
- definir mecanismos de escalonamento, análise, bloqueio, recusa ou encerramento de relacionamentos quando identificados riscos incompatíveis com o apetite de risco da empresa;
- promover cultura de integridade, conformidade, segurança e cooperação com autoridades competentes, respeitados o sigilo e a legislação aplicável.

2. ABRANGÊNCIA

Esta política aplica-se, na medida de sua pertinência, a:

- clientes pessoas físicas e jurídicas, inclusive seus representantes, procuradores, sócios e beneficiários finais;

- usuários, estabelecimentos, parceiros comerciais, prestadores de serviço e demais terceiros que mantenham relação relevante com a empresa;
- produtos, serviços, APIs, integrações, canais de atendimento, movimentações financeiras e demais operações processadas ou disponibilizadas pela Mistic Tecnologias;
- administradores, empregados, colaboradores e prestadores que participem de processos de cadastro, análise, monitoramento, pagamentos, saques, atendimento, tecnologia ou gestão de riscos.

3. BASE LEGAL E REGULATÓRIA

A política observa, conforme aplicabilidade ao modelo de negócio e ao enquadramento jurídico-regulatório da empresa, especialmente:

- Lei nº 9.613/1998, que dispõe sobre os crimes de lavagem ou ocultação de bens, direitos e valores e sobre a prevenção da utilização do sistema financeiro para ilícitos;
- Lei nº 13.260/2016, que disciplina o terrorismo e seu financiamento;
- Lei nº 13.810/2019, relativa ao cumprimento de sanções impostas pelo Conselho de Segurança das Nações Unidas e à indisponibilidade de ativos, quando aplicável;
- Lei nº 13.709/2018 (LGPD), no tratamento e proteção de dados pessoais;
- normas, circulares, resoluções e instruções do Banco Central do Brasil aplicáveis à atividade da empresa, inclusive as regras de PLD/FT/FTP pertinentes a instituições autorizadas, quando incidentes;
- orientações, resoluções e demais atos do Coaf aplicáveis às pessoas obrigadas, quando incidentes sobre a atividade desenvolvida.

A administração deverá acompanhar alterações legislativas e regulatórias e promover a atualização desta política e dos procedimentos internos sempre que necessário.

4. PRINCÍPIOS DE PLD/FT

- Abordagem baseada em risco: recursos de controle devem ser proporcionais aos riscos identificados.
- Conheça seu cliente: informações cadastrais, societárias e de atividade devem ser obtidas e validadas de acordo com o nível de risco.
- Rastreabilidade: operações e decisões relevantes devem manter registros suficientes para reconstrução dos fatos.
- Segregação de funções: quando compatível com o porte da empresa, atividades críticas de cadastro, monitoramento, análise e aprovação devem possuir controles independentes.
- Confidencialidade: informações sobre alertas, análises e comunicações às autoridades devem ser protegidas e compartilhadas apenas com pessoas autorizadas.
- Tolerância zero a ilícitos: atividades incompatíveis com a legislação, os termos da plataforma ou o apetite de risco poderão ser recusadas, suspensas ou encerradas.

5. GOVERNANÇA E RESPONSABILIDADES

A governança de PLD/FT será exercida de forma proporcional ao porte, complexidade e risco da empresa.

5.1 Administração

- aprovar esta política e assegurar recursos compatíveis para sua execução;
- definir e revisar o apetite de risco de PLD/FT;
- receber informações gerenciais sobre alertas relevantes, exposições, deficiências e medidas corretivas.

5.2 Responsável por PLD/FT / Compliance

- coordenar a implementação e atualização dos controles;
- acompanhar indicadores e casos de maior risco;

- assegurar que análises de operações suspeitas sejam documentadas;
- promover treinamentos e testes de efetividade dos controles;
- avaliar, quando cabível, a necessidade de comunicação a autoridades competentes.

5.3 Demais áreas e colaboradores

- cumprir procedimentos de identificação, validação e monitoramento;
- comunicar imediatamente sinais de irregularidade aos canais internos definidos;
- preservar evidências, documentos e informações relacionadas às análises;
- não alertar o cliente ou terceiro sobre eventual comunicação de operação suspeita quando isso for vedado pela legislação.

6. ABORDAGEM BASEADA EM RISCO

A Mistic Tecnologias deverá identificar e classificar riscos considerando, no mínimo:

- perfil e comportamento do cliente, incluindo atividade econômica, capacidade financeira declarada e finalidade de uso dos serviços;
- tipo de produto, serviço, fluxo financeiro e canal utilizado;
- volume, frequência, origem e destino das transações;
- localização geográfica e exposição a jurisdições de maior risco;
- estrutura societária, beneficiário final e eventual utilização de representantes;
- vínculos com pessoas politicamente expostas (PEP), sanções, listas restritivas ou outros fatores de risco;
- inconsistências entre o perfil cadastral e o comportamento transacional observado.

Os níveis de risco poderão ser classificados, por exemplo, como baixo, médio, alto ou crítico, com medidas de diligência e monitoramento proporcionais a cada nível.

7. CONHEÇA SEU CLIENTE — KYC/KYB

Antes ou durante a habilitação, conforme o produto e o risco, a empresa poderá coletar, validar e manter:

- nome completo ou razão social, CPF/CNPJ, data de nascimento ou constituição e dados de contato;
- documentos de identificação e comprovantes necessários à validação cadastral;
- atividade econômica, finalidade de uso da conta/serviço e informações de capacidade financeira quando pertinentes;
- para pessoas jurídicas: quadro societário, administradores, representantes e beneficiários finais;
- dados bancários e informações necessárias para validar titularidade e compatibilidade com o cadastro;
- informações adicionais quando houver alerta, inconsistência ou necessidade de diligência reforçada.

A empresa poderá solicitar documentação complementar, realizar validações automatizadas ou manuais e restringir o acesso a funcionalidades até a conclusão das verificações necessárias.

8. BENEFICIÁRIO FINAL, PEP E SANÇÕES

- A Mistic Tecnologias buscará identificar o beneficiário final de pessoas jurídicas e estruturas que apresentem complexidade relevante.
- Relacionamentos com Pessoas Expostas Politicamente (PEP) serão submetidos a procedimentos compatíveis com o risco e com a legislação aplicável.
- A empresa poderá realizar consultas a listas públicas, bases de sanções e fontes de informação confiáveis para fins de prevenção a ilícitos.

- Quando houver correspondência positiva ou dúvida relevante, a operação ou relacionamento poderá ser submetido a análise reforçada antes de sua continuidade.
- Medidas de indisponibilidade ou outras providências legalmente exigidas serão observadas quando aplicáveis.

9. MONITORAMENTO DE OPERAÇÕES

O monitoramento poderá utilizar regras, indicadores, análise comportamental e mecanismos automatizados ou manuais. Entre os sinais de alerta, incluem-se:

- movimentação incompatível com o perfil cadastral, atividade econômica ou capacidade declarada;
- operações fracionadas ou estruturadas para evitar controles, limites ou análises;
- rápida circulação de recursos sem finalidade econômica aparente;
- uso de múltiplas contas, dispositivos, pessoas ou empresas com vínculos suspeitos;
- transações com contrapartes, regiões ou atividades de risco elevado sem justificativa adequada;
- tentativas repetidas de cadastro, alteração de dados, saque ou transferência após alertas de segurança;
- divergências entre titularidade, origem dos recursos, beneficiário e finalidade informada;
- padrões associados a fraude, contas de passagem, engenharia social, interposição de terceiros ou outras condutas incompatíveis.

Um alerta não significa, isoladamente, que tenha ocorrido crime. Cada caso deverá ser analisado considerando contexto, evidências disponíveis, histórico e justificativas apresentadas.

10. DILIGÊNCIA REFORÇADA

Clientes, operações ou situações classificadas como de maior risco poderão estar sujeitos a controles adicionais, tais como:

- solicitação de documentos e informações adicionais sobre origem e destino dos recursos;
- validação ampliada da atividade econômica e do beneficiário final;
- análise de vínculos, contrapartes e histórico transacional;
- aprovação por nível hierárquico superior, quando aplicável;
- redução de limites, bloqueio preventivo, recusa de operação ou encerramento do relacionamento, conforme o caso.

11. ANÁLISE E TRATAMENTO DE OPERAÇÕES SUSPEITAS

Alertas relevantes serão registrados e submetidos a análise compatível com seu risco. A análise deverá, sempre que possível, documentar:

- identificação do cliente e das contrapartes relacionadas;
- descrição das operações e do comportamento que originou o alerta;
- documentos e evidências analisados;
- justificativas apresentadas pelo cliente, quando solicitadas;
- conclusão da análise e fundamento para encerramento, monitoramento reforçado, restrição ou escalonamento.

Quando houver indícios suficientes e existir obrigação legal ou regulatória de comunicação, a empresa adotará os procedimentos necessários para comunicação às autoridades competentes, inclusive ao Coaf quando aplicável, observando os prazos, critérios e requisitos estabelecidos na regulamentação. A comunicação, quando devida, será tratada sob sigilo.

12. RECUSA, BLOQUEIO E ENCERRAMENTO

A Mistic Tecnologias poderá, conforme contrato, legislação e análise de risco:

- recusar cadastro, operação ou produto quando não for possível concluir adequadamente a identificação ou a análise de risco;
- solicitar informações e documentos adicionais;
- restringir temporariamente funcionalidades ou movimentações quando houver necessidade de análise ou determinação legal;
- encerrar relacionamentos quando identificada utilização incompatível com a legislação, com os termos da plataforma ou com o apetite de risco da empresa;
- preservar registros e evidências relacionados a medidas tomadas.

Medidas de bloqueio ou restrição deverão ser proporcionais, documentadas e submetidas aos responsáveis competentes, sem prejuízo do cumprimento de determinações judiciais ou administrativas.

13. ATIVIDADES E CONDUTAS PROIBIDAS

É vedada a utilização dos serviços para, entre outras hipóteses:

- lavagem ou ocultação de bens, direitos e valores;
- financiamento do terrorismo ou apoio material a atividades terroristas;
- fraudes, estelionato, uso de identidade de terceiros ou falsidade documental;
- operações destinadas a ocultar origem, propriedade, destino ou beneficiário de recursos;
- utilização de contas ou credenciais em nome de terceiros sem autorização legítima;
- atividades proibidas por lei, regulamentação, sanções aplicáveis ou pelos Termos de Uso da MisticPay.

14. REGISTROS E RETENÇÃO DE INFORMAÇÕES

A empresa manterá registros cadastrais, transacionais, análises, decisões e evidências necessárias ao cumprimento de suas obrigações legais, regulatórias, contratuais e de prevenção a ilícitos, pelo período exigido pela legislação aplicável.

- Os registros deverão ser íntegros, rastreáveis e acessíveis às pessoas autorizadas.
- Documentos e evidências de investigações internas deverão ser preservados contra alteração ou destruição indevida.
- O acesso será limitado conforme necessidade, função e princípios de segurança da informação e proteção de dados.

15. PROTEÇÃO DE DADOS E CONFIDENCIALIDADE

O tratamento de dados pessoais realizado no âmbito desta política deverá observar a Lei nº 13.709/2018 (LGPD), bem como princípios de necessidade, adequação, segurança, prevenção e responsabilização.

- Dados serão utilizados somente para finalidades legítimas e compatíveis com as atividades da empresa.
- Informações sobre alertas, investigações e comunicações a autoridades serão tratadas como confidenciais.
- Compartilhamentos com instituições parceiras, prestadores ou autoridades ocorrerão quando houver fundamento legal, contratual ou regulatório.
- A empresa adotará medidas técnicas e administrativas adequadas à proteção das informações sob sua responsabilidade.

16. TREINAMENTO E CONSCIENTIZAÇÃO

A Mistic Tecnologias promoverá, de acordo com seu porte e exposição a risco:

- treinamento inicial para profissionais que atuem em áreas críticas;
- reciclagens periódicas e comunicações sobre alterações relevantes;

- orientações sobre identificação de sinais de alerta, tratamento de informações e escalonamento;
- registros de participação e, quando pertinente, avaliações de conhecimento.

17. TERCEIROS E PARCEIROS

Parceiros, prestadores e fornecedores que possam expor a empresa a riscos de PLD/FT serão avaliados de acordo com sua relevância e risco. Quando necessário, contratos poderão conter obrigações de cooperação, segurança, confidencialidade, fornecimento de informações e cumprimento da legislação aplicável.

A terceirização de determinada atividade não elimina a responsabilidade da Mistic Tecnologias de manter controles proporcionais aos riscos que permaneçam sob sua gestão.

18. INDICADORES E TESTES DE EFETIVIDADE

A administração poderá acompanhar, entre outros, os seguintes indicadores:

- quantidade de cadastros analisados, aprovados, recusados e submetidos a diligência reforçada;
- quantidade e natureza dos alertas transacionais;
- tempo médio de tratamento dos alertas;
- quantidade de relacionamentos restringidos ou encerrados por risco;
- incidentes, falhas de controle e respectivos planos de ação;
- treinamentos realizados e cobertura dos colaboradores envolvidos.

Os controles deverão ser periodicamente revisados e, quando possível, testados quanto à efetividade. Deficiências identificadas deverão gerar plano de correção com responsável e prazo compatíveis com a criticidade.

19. CANAL INTERNO E NÃO RETALIAÇÃO

Colaboradores e prestadores deverão comunicar, de boa-fé, suspeitas de fraude, lavagem de dinheiro, financiamento do terrorismo, falsidade cadastral ou descumprimento desta política aos canais internos disponibilizados pela empresa.

A empresa deverá buscar preservar a confidencialidade das comunicações e não tolerará retaliação contra pessoa que relate uma suspeita de forma legítima e de boa-fé, ressalvadas situações de má-fé ou uso indevido dos canais.

20. REVISÃO, APROVAÇÃO E VIGÊNCIA

Esta política entra em vigor em 03 de setembro de 2026 e permanecerá vigente até sua substituição ou revogação. Sua revisão deverá ocorrer, no mínimo, anualmente ou sempre que houver alteração relevante no modelo de negócio, nos produtos, no perfil de risco, na legislação ou na regulamentação aplicável.

A administração da Mistic Tecnologias é responsável por sua aprovação e por assegurar que os procedimentos internos necessários à sua implementação sejam mantidos atualizados.

ANEXO I — MATRIZ EXEMPLIFICATIVA DE FATORES DE RISCO

A matriz abaixo serve como referência para a construção e revisão do processo interno de classificação de risco. Os critérios e pesos poderão ser ajustados conforme a realidade operacional.

Fator	Indicadores de menor risco	Indicadores de maior risco
Cliente	Cadastro consistente; atividade compatível; histórico regular.	Inconsistências; estrutura opaca; dificuldade de validação; comportamento atípico.
Produto/serviço	Uso simples e previsível; baixa exposição.	Produto com maior velocidade, complexidade ou possibilidade de movimentação relevante.
Transações	Volume e frequência compatíveis com o perfil.	Fracionamento, circularidade, picos incomuns ou fluxos sem justificativa.
Geografia	Relacionamentos e fluxos em jurisdições de risco ordinário.	Exposição a jurisdições de maior risco ou com deficiências estratégicas relevantes.
PEP/sanções	Sem correspondências ou fatores adicionais.	PEP, correspondência em lista restritiva ou necessidade de diligência reforçada.
Comportamento	Uso estável e coerente.	Mudanças abruptas, tentativas de contornar controles ou múltiplos sinais de alerta.

REFERÊNCIAS NORMATIVAS PRINCIPAIS

Lei nº 9.613/1998; Lei nº 13.260/2016; Lei nº 13.810/2019; Lei nº 13.709/2018; Circular BCB nº 3.978/2020 e alterações, quando aplicável; Carta Circular BCB nº 4.001/2020, quando aplicável; Resolução BCB nº 44/2020, quando aplicável; e demais atos do Banco Central do Brasil e do Coaf pertinentes ao enquadramento da empresa e às atividades efetivamente exercidas.

Documento institucional. Esta política deve ser lida em conjunto com os Termos de Uso, Política de Privacidade, procedimentos internos de KYC/KYB, monitoramento transacional, prevenção a fraudes e demais normas internas da Mistic Tecnologias.