

POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO (PLD/FT)

1. Objetivo

A presente Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (“Política PLD/FT”) estabelece os princípios, diretrizes, responsabilidades e procedimentos adotados pela empresa para prevenir a utilização de sua estrutura tecnológica, de seus produtos, de seus serviços ou de suas relações comerciais para práticas relacionadas à lavagem de dinheiro, ao financiamento do terrorismo, à fraude, à corrupção ou a quaisquer outras atividades ilícitas.

Embora a empresa atue como desenvolvedora de soluções tecnológicas para operadores do setor de apostas e jogos regulamentados, e não como operadora ou intermediadora financeira, reconhece que seu ambiente de negócios exige elevados padrões de integridade, governança e gestão de riscos.

Esta Política visa fortalecer a cultura de compliance, assegurar a conformidade com a legislação aplicável e proteger a reputação institucional da empresa perante clientes, parceiros, órgãos reguladores e autoridades competentes.

2. Abrangência

Esta Política aplica-se a:

- sócios e administradores;
- diretores;
- empregados;
- prestadores de serviços;
- desenvolvedores terceirizados;
- consultores;
- fornecedores estratégicos;
- parceiros comerciais;
- quaisquer terceiros que atuem em nome ou no interesse da empresa.

Todos deverão observar integralmente as disposições aqui previstas, independentemente do vínculo contratual existente.

3. Base Normativa

Esta Política foi elaborada considerando, entre outras, as seguintes referências:

- Lei nº 9.613/1998 (Prevenção à Lavagem de Dinheiro);
- Lei nº 12.846/2013 (Lei Anticorrupção);
- Lei nº 13.709/2018 (LGPD), quando aplicável ao tratamento de dados pessoais;
- Recomendações do Grupo de Ação Financeira Internacional (GAFI/FATF);
- boas práticas internacionais de Compliance;
- princípios de gestão de riscos corporativos.

Na hipótese de alteração da legislação ou da regulamentação aplicável, esta Política será revisada para garantir sua aderência ao novo cenário regulatório. POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E AO FINANCIAMENTO DO TERRORISMO (PLD/FT)

4. Princípios

A atuação da empresa será orientada pelos seguintes princípios:

- I – Integridade;
- II – Boa-fé objetiva;
- III – Transparência nas relações comerciais;
- IV – Gestão proporcional de riscos;
- V – Cooperação com autoridades competentes, quando legalmente exigível;
- VI – Registro e rastreabilidade das operações relacionadas à prestação dos serviços;
- VII – Proteção da reputação institucional;
- VIII – Tolerância zero à utilização da estrutura tecnológica para fins ilícitos.

5. Estrutura de Governança

A Diretoria é responsável pela implementação desta Política e pelo fortalecimento da cultura de integridade da organização.

Compete à Diretoria:

- aprovar esta Política;
- disponibilizar recursos compatíveis com os riscos da atividade;
- promover treinamentos periódicos;
- apoiar auditorias internas;
- assegurar que todos os colaboradores conheçam seus deveres.

O responsável técnico designado para Compliance terá, entre outras atribuições:

- acompanhar a efetividade desta Política;

- recomendar melhorias;
- receber comunicações internas de situações atípicas;
- coordenar revisões periódicas;
- elaborar relatórios destinados à Diretoria.

6. Avaliação de Riscos

A empresa adotará metodologia de avaliação contínua de riscos considerando, entre outros fatores:

- perfil dos clientes;
- natureza dos serviços contratados;
- localização geográfica dos parceiros;
- estrutura societária conhecida;
- riscos tecnológicos;
- riscos reputacionais;
- histórico de relacionamento comercial;
- exposição a ambientes regulados.

Os riscos serão classificados em níveis (baixo, médio e alto), permitindo que as medidas de controle sejam proporcionais à criticidade identificada.

7. Conhecimento de Clientes e Parceiros (Due Diligence)

A Empresa adotará procedimentos proporcionais de diligência prévia (“due diligence”) antes da formalização de relações comerciais relevantes, com o objetivo de reduzir riscos legais, reputacionais e operacionais.

A extensão da diligência será compatível com o nível de risco identificado.

Sempre que aplicável, poderão ser verificados:

- identificação da pessoa jurídica;
- situação cadastral perante a Receita Federal;
- composição societária e beneficiário final, quando disponível;
- existência de sanções públicas ou restrições legais;
- capacidade técnica e operacional para execução do contrato;
- histórico comercial e reputacional;
- compatibilidade entre a atividade econômica e os serviços contratados.

A Empresa poderá solicitar documentos adicionais quando entender necessário para melhor avaliação do risco.

8. Monitoramento Contínuo

Mesmo após o início da relação comercial, poderão ser realizados procedimentos periódicos de monitoramento destinados a identificar alterações relevantes que possam impactar o risco da relação contratual.

Serão considerados, entre outros fatores:

- alterações relevantes na estrutura societária;
- mudanças significativas no perfil operacional;
- notícias públicas envolvendo fraude, corrupção ou crimes financeiros;
- descumprimento contratual reiterado;
- utilização inadequada dos serviços tecnológicos fornecidos.

Sempre que forem identificadas situações incompatíveis com os padrões de integridade da Empresa, poderão ser adotadas medidas adicionais de verificação.

9. Situações Atípicas

Sem prejuízo da análise individual de cada caso, poderão ser consideradas situações de atenção:

- tentativa de ocultação da identidade dos reais controladores da empresa contratante;
 - fornecimento de informações falsas ou inconsistentes;
 - recusa injustificada em apresentar documentação necessária;
 - utilização da solução tecnológica para finalidade diversa daquela contratada;
 - indícios de utilização da plataforma para atividades ilícitas;
- solicitação de estruturas contratuais incompatíveis com a finalidade declarada;
- comportamento que possa indicar tentativa de ocultação de recursos ou identidade.

A simples ocorrência de qualquer dessas situações não caracteriza irregularidade, mas poderá justificar análise adicional.

10. Comunicação Interna

Qualquer colaborador que identifique situação potencialmente incompatível com esta Política deverá comunicar imediatamente o fato ao responsável designado pela Empresa.

As comunicações poderão ocorrer por meio dos canais internos definidos pela organização.

A identidade do comunicante será preservada sempre que possível, vedando-se qualquer forma de retaliação em razão de comunicação realizada de boa-fé.

11. Registro e Conservação de Informações

A Empresa manterá registros relacionados às verificações realizadas durante os processos internos de diligência, observados os princípios da necessidade, da confidencialidade e da proteção de dados pessoais.

Os documentos serão armazenados em ambiente seguro, com acesso restrito às pessoas autorizadas e pelo prazo definido na legislação aplicável ou nas normas internas de retenção documental.

12. Treinamento e Cultura de Integridade

A Empresa promoverá ações periódicas de conscientização destinadas aos colaboradores e prestadores de serviços, abordando temas relacionados à:

- ética empresarial;
- prevenção à lavagem de dinheiro;
- prevenção à fraude;
- segurança da informação;
- proteção de dados pessoais;
- reporte de irregularidades;
- boas práticas de compliance.

Os treinamentos poderão ocorrer presencialmente ou por meio eletrônico e deverão ser registrados para fins de controle interno.

A efetividade desta Política poderá ser avaliada periodicamente mediante revisões internas, auditorias ou outros mecanismos de verificação definidos pela Diretoria.

Sempre que identificadas oportunidades de melhoria, a Política poderá ser atualizada para refletir alterações legislativas, regulatórias, tecnológicas ou organizacionais.

14. Confidencialidade

Todas as informações obtidas durante procedimentos de diligência ou monitoramento serão tratadas com confidencialidade e utilizadas exclusivamente para finalidades legítimas relacionadas à gestão de riscos, observada a legislação aplicável, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD).

15. Medidas de Controle

A Empresa manterá controles internos compatíveis com a natureza de suas atividades e proporcionais aos riscos identificados, buscando prevenir a utilização de seus produtos, serviços ou infraestrutura tecnológica para fins ilícitos.

Sempre que aplicável, poderão ser adotadas as seguintes medidas:

- revisão periódica dos processos internos;

- segregação de funções críticas;
- controle de acessos às informações sensíveis;
- rastreabilidade das ações realizadas em sistemas corporativos;
- registro de evidências relevantes para fins de auditoria;
- gestão de terceiros com critérios mínimos de integridade;
- avaliação periódica da efetividade desta Política.

Os controles poderão ser aperfeiçoados continuamente conforme a evolução tecnológica, regulatória e operacional da Empresa.

16. Responsabilidades dos Colaboradores

Todos os colaboradores, administradores, prestadores de serviços e parceiros deverão:

- atuar de acordo com os princípios desta Política;
- comunicar imediatamente situações potencialmente incompatíveis com os padrões de integridade da Empresa;
- colaborar com auditorias internas;
- preservar o sigilo das informações obtidas em razão de suas atividades;
- participar dos treinamentos disponibilizados pela Empresa;
- cumprir as normas internas relacionadas à ética, segurança da informação e proteção de dados.

O desconhecimento desta Política não afasta a obrigação de seu cumprimento.

17. Medidas Disciplinares

O descumprimento desta Política poderá ensejar a adoção das medidas administrativas e contratuais cabíveis, observada a legislação vigente e o devido processo interno.

Dependendo da gravidade da conduta, poderão ser aplicadas, entre outras:

- orientação formal;
- advertência;
- suspensão de acessos ou atividades;
- rescisão contratual;
- comunicação às autoridades competentes, quando exigida por lei.

A aplicação das medidas observará os princípios da proporcionalidade, razoabilidade e ampla apuração dos fatos.

18. Gestão de Melhorias

Esta Política integra o Programa de Governança Corporativa da Empresa e deverá ser objeto de aperfeiçoamento contínuo.

Sempre que forem identificadas alterações relevantes na legislação, nas atividades da Empresa, nos riscos operacionais ou nas melhores práticas de mercado, a Diretoria poderá determinar sua revisão.

As sugestões de melhoria poderão ser apresentadas por qualquer colaborador ou parceiro da Empresa.

19. Revisão

Esta Política será revisada:

- anualmente; ou
- sempre que houver alteração legal, regulatória, tecnológica ou organizacional que justifique sua atualização.

As revisões serão registradas em controle próprio de versão.

20. Vigência

Esta Política entra em vigor na data de sua aprovação pela Diretoria e permanecerá vigente por prazo indeterminado, até que seja substituída por nova versão.

Elaboração e Revisão Jurídica

Everson Alessandro Pereira

Advogado – OAB/SC 12.470

Especialista em Direito Digital

Documento assinado digitalmente
 **EVERSON ALESSANDRO PEREIRA**
Data: 04/08/2026 17:08:08-0300
Verifique em <https://validar.iti.gov.br>