# Política de prevenção à lavagem de dinheiro, financiamento ao terrorismo e proliferação de armas de destruição em massa.

De acordo com os requisitos mínimos estabelecidos na Lei nº 14.790 de 2023 e demais regulamentações publicadas pelo Ministério da Fazenda.

| Versão | Descrição | Data | Autor |
|---|---|---|---|
| 1.0 | Versão inicial | 26/07/24 | Nae Alexandra |
| 2.0 | Atualização processo KYC | 24/02/25 | Nae Alexandra |
| 3.0 | Atualização de responsável | 23/10/25 | Augusto Cesar Piaskoski |

# Conteúdo do Documento

# 1. Introdução e Objetivo da Política

A lavagem de dinheiro e o financiamento ao terrorismo representam uma grave ameaça para as empresas que operam no setor de jogos de azar.

A política de Prevenção à Lavagem de Dinheiro, ao Financiamento ao Terrorismo e à Proliferação de Armas de Destruição em Massa descreve as medidas que a empresa adotará para mitigar e gerenciar os riscos relacionados à lavagem de dinheiro e ao financiamento ao terrorismo.

A política é projetada para garantir o cumprimento das leis e regulamentos brasileiros aplicáveis, incluindo os enumerados na seção 2 (Marco Legal e Regulatório) abaixo, para evitar que a empresa seja utilizada para fins de lavagem de dinheiro e o financiamento ao terrorismo.

A Lei nº 9.613/1998 tipifica o crime de “lavagem” ou ocultação de bens, amplamente conhecido como lavagem de dinheiro, que consiste no ato de ocultar ou dissimular a origem ilícita de bens ou valores que sejam resultado de crimes.

O termo “lavagem de dinheiro” surgiu porque o dinheiro adquirido ilegalmente é sujo e precisa ter aparência de legalidade; ou seja, é necessário “lavá-lo” para que pareça limpo.

Para as pessoas físicas, a pena é de 3 a 10 anos de prisão e multa. A Lei prevê penas maiores para os casos em que o crime ocorra de forma reiterada ou através de uma organização criminosa. Para as pessoas jurídicas, as sanções administrativas incluem advertência, multa, inabilitação temporária para os administradores e cassação ou suspensão da autorização de operação.

## 2. Marco Legal e Regulatório

Os requisitos de prevenção à lavagem de dinheiro, obrigações e possíveis sanções que a empresa deve cumprir em relação à sua oferta de jogo têm como fundamento as seguintes fontes do direito:

- Lei nº 9.613, de 3 de março de 1998
- Lei nº 13.260, de 16 de março de 2016
- Lei nº 13.810, de 8 de março de 2019
- Lei nº 14.790, de 29 de dezembro de 2023
- Lei nº 14.478, de 21 de dezembro de 2022
- Lei nº 14.597, de 14 de junho de 2023 (artigo 177)
- Lei nº 14.790, de 29 de dezembro de 2023
- Portaria SPA/MF nº 1.143, de 11 de julho de 2024
- Portaria SPA/MF nº 1.231, de 31 de julho de 2024
- Portaria MF nº 1.330, de 26 de outubro de 2023
- Outras normas regulamentares emitidas pelo Ministério da Fazenda
- Normas regulamentares emitidas pelo Conselho de Controle de Atividades Financeiras (COAF)

## 3. Estratégia e Princípios

A política se aplica a todos os usuários, colaboradores, diretores, fornecedores e prestadores de serviços da Versus, incluindo todas as plataformas de jogos e apostas online.

A estratégia de combate à lavagem de dinheiro tem como objetivo garantir que todos os requisitos e obrigações previstos em leis, regulamentos, orientações e diretrizes de melhores práticas sejam cumpridos. Isso também envolve combater o risco de uso indevido para fins de lavagem de dinheiro por meio de sistemas e controles adequados.

A empresa deve garantir que não esteja envolvida em atividades relacionadas a organizações criminosas e que implemente medidas para prevenir a participação dessas organizações no sistema de apostas.

A estratégia contra a lavagem de dinheiro estabelece os requisitos mínimos que devem ser cumpridos por todos os envolvidos na organização. Os elementos dessa estratégia são:

- Introduzir e cumprir processos eficazes e eficientes de combate à lavagem de dinheiro para a administração e o dia a dia, incluindo o desenvolvimento, implementação e execução de uma cultura organizacional de prevenção à lavagem de dinheiro e outros crimes relacionados, bem como de integridade, boa governança e agenda ESG (ambiental, social e de governança).

- Manter controles apropriados em conformidade com as leis e regulamentos aplicáveis, definindo funções e responsabilidades das pessoas envolvidas.

- Cumprir processos apropriados e eficientes para reportar atividades suspeitas de lavagem de dinheiro.

- Introduzir e apoiar processos com uma abordagem baseada no risco, que controlem a confiabilidade, a identificação e outros requisitos de KYC (Conheça seu Cliente), KYE (Conheça seu Empregado), KYP (Conheça seu Parceiro) e KYS (Conheça seu Fornecedor), bem como processos que exijam maiores obrigações de diligência com relação a pessoas de alto risco, como, por exemplo, pessoas politicamente expostas, diretores esportivos, treinadores esportivos e membros de comitês técnicos.

- Estabelecer processos pelos quais atividades suspeitas sejam notificadas internamente e, quando aplicável, às autoridades pertinentes (COAF).

- Atender às solicitações feitas pelo COAF ou pela Secretaria de Prêmios e Apostas do Ministério da Fazenda, seguindo a periodicidade, forma e condições estabelecidas por esses órgãos, sendo responsáveis por preservar a confidencialidade das informações fornecidas, conforme exigido por lei.

- Garantir treinamento e conscientização a todos os colaboradores, fornecedores e prestadores de serviços, com a realização periódica e contínua de atividades de informação e capacitação em matérias de prevenção à lavagem de dinheiro e outros

crimes relacionados.

- Fornecer informações suficientes à direção e aos reguladores sobre o cumprimento dos requisitos estabelecidos e/ou legais.

# 4. Estrutura Organizacional

Em cumprimento às diretrizes contidas na norma aplicável, a estrutura organizacional em matéria de prevenção à lavagem de dinheiro e financiamento ao terrorismo da empresa é composta pelos seguintes órgãos:

- Responsável por Integridade e Compliance
- Órgão de Administração

## 4.1 Responsável por Integridade e Compliance

De acordo com o disposto no artigo 6º, inciso XII, alínea "e" da Portaria MF nº 1.330/2023 e artigo 8º, § 2º, inciso IV da Portaria SPA/MF nº 827/2024, os agentes operadores devem designar um responsável por integridade e compliance (C*ompliance Officer*).

A Versus designou como **Responsável por Integridade e Compliance**, inclusive para assegurar a correta implementação das normas relacionadas à lavagem de dinheiro e ao financiamento ao terrorismo, o Sr. **Augusto Cesar Piaskoski**. O seu e-mail é: augusto.piaskoski@orenesgrupo.com e o seu telefone é +55 11 92160-0287.

Este cargo é fundamental para assegurar que as atividades da empresa estejam alinhadas com a legislação e regulamentação do país.

A Responsável assumirá as seguintes funções e competências:

**1. Implementação de Políticas e Procedimentos de Conformidade**

- Desenvolver e implementar políticas, procedimentos e controles internos de prevenção à lavagem de dinheiro e financiamento ao terrorismo, incluindo o Manual Específico de KYC a ser aprovado pelo Órgão de Administração, alinhados com as normas brasileiras e revisados anualmente.
- Realizar análises periódicas de risco para identificar se novos produtos, serviços ou tecnologias podem ser usados em práticas de lavagem de dinheiro ou crimes

relacionados. Além disso, garantir que todos os procedimentos estejam atualizados e sejam eficazes considerando os perfis de risco da empresa, dos clientes, do volume e quantidade de recursos envolvidos nas apostas, e dos colaboradores, fornecedores e prestadores de serviços.

- Realizar revisões periódicas da eficácia das políticas adotadas e da conformidade com as normas aplicáveis, incluindo a identificação e correção das deficiências detectadas.

**2. Supervisão e Monitoramento de Transações**

- Supervisionar a implementação de um sistema de monitoramento de transações para detectar atividades suspeitas, como apostas incomuns, grandes depósitos ou retiradas rápidas.

- Garantir que as transações que excedam os limites estabelecidos sejam reportadas ou revisadas.

**3. Estabelecimento de Processos KYC, KYE, KYP e KYS**

- Assegurar a existência de um processo KYC (Conheça seu Cliente) completo para a verificação de identidade dos clientes antes de permitir que realizem apostas ou transações, incluindo procedimentos de identificação que permitam verificar e validar a identidade dos clientes no momento de seu cadastro, e aprovar as categorias de risco a serem utilizadas para a classificação dos clientes.

- Implementar medidas de diligência reforçada para clientes de alto risco (por exemplo, pessoas politicamente expostas).

- Assegurar a existência de processos KYE (Conheça seu Colaborador), KYP (Conheça seu Parceiro) e KYS (Conheça seu Fornecedor) completos para a verificação de identidade de funcionários, fornecedores e prestadores de serviços, incluindo procedimentos de identificação e qualificação para avaliar e mitigar riscos.

- Adotar procedimentos para cumprir, prontamente, resoluções do Conselho de Segurança das Nações Unidas (CSNU) ou designações de seus comitês de sanções que determinem a indisponibilidade de ativos de titularidade, direta ou indireta, de pessoas físicas, de pessoas jurídicas ou de entidades sancionadas, incluindo o acompanhamento da lista mantida pelo CSNU e seus comitês de

sanções.

- Promover a verificação periódica e o monitoramento de *compliance* das instituições de pagamento e financeiras com as quais mantém relação, assegurando que estejam autorizadas pelo Banco Central do Brasil para operar.

**5. Denúncia de Atividades Suspeitas**

- Implementar procedimentos de monitoramento, seleção e análise de transações para identificar aquelas que possam apresentar indícios de lavagem de dinheiro ou outros crimes correlatos, incluindo descrições das características das transações, das partes e demais envolvidos, dos valores, da modalidade de aposta e da forma de pagamento.

- Promover a observância ao prazo de 30 dias para o fechamento do procedimento de análise, contados a partir da data da transação, e documentar e registrar a análise e suas conclusões.

- Identificar e reportar transações suspeitas de lavagem de dinheiro ou financiamento ao terrorismo ao COAF e/ou outras autoridades pertinentes.

- Assegurar que os relatórios sejam apresentados dentro dos prazos estabelecidos pela legislação (conforme a Portaria SPA/MF nº 1.143/2024, até o dia útil seguinte à conclusão sobre a detecção).

- No caso de não identificação, ao longo de um ano-calendário, de transações que devam ser comunicadas ao COAF, enviar à Secretaria de Prêmios e Apostas a comunicação de não ocorrência.

**6. Capacitação e Sensibilização de Equipe**

- Capacitar toda a equipe da empresa em normas de conformidade e na identificação de possíveis atividades ilícitas, promovendo o treinamento anual dos funcionários.

- Assegurar que os colaboradores compreendam a importância de seguir as políticas de prevenção à lavagem de dinheiro e financiamento ao terrorismo, bem como seus papéis na prevenção dessas práticas.

**7. Coordenação com as Autoridades**

- Colaborar ativamente com as autoridades regulatórias e de *compliance*, fornecendo as informações requeridas para investigações sobre atividades ilícitas ou suspeitas.
- Garantir que sejam mantidos registros detalhados e completos das atividades de compliance, que estejam disponíveis para auditorias e revisões regulatórias.

**8. Avaliação de Riscos e Auditoria Interna**

- Promover avaliações periódicas dos riscos de lavagem de dinheiro e financiamento ao terrorismo dentro da empresa.
- Supervisionar auditorias internas para verificar a eficácia das medidas de compliance e implementar melhorias quando necessário.

**9. Retenção de Registros**

- Garantir que todos os registros de transações, documentos de verificação de clientes e relatórios de atividades suspeitas sejam retidos por pelo menos cinco anos, conforme a normativa vigente.

**10. Designação de um Comitê de Compliance / Órgão de Administração**

- Como boa prática de gestão de riscos e para assegurar que a empresa cumpre com os padrões internacionais e as melhores práticas do setor, a Responsável por Integridade e Compliance coordenará um Comitê de Compliance / Órgão de Administração, que o apoiará na tomada de decisões e na supervisão das políticas aplicáveis.

**11. Garantia de Cumprimento Regulatório**

- A Responsável garantirá o cumprimento contínuo de todas as normas locais relacionadas à lavagem de dinheiro e financiamento ao terrorismo.

Faculta-se à Responsável que outras pessoas a substituam pontualmente, assumindo suas funções e responsabilidades em caso de ausência ou indisponibilidade.

## 4.2 Órgão de Administração

O **Órgão de Administração** é responsável pela aprovação e aplicação das políticas,

procedimentos e controles internos de prevenção à lavagem de dinheiro e financiamento ao terrorismo, incluindo o Manual Específico de KYC.

As responsabilidades do Órgão de Administração são as seguintes:

**1. Cumprimento das Regulamentações e Leis Locais**

O Órgão de Administração deve assegurar que a empresa cumpre todas as leis e normativas relacionadas com apostas de quota fixa. Isso inclui:

- A Lei 13.756, de 12 de dezembro de 2018 e Lei 14.790, de 29 de dezembro de 2023, que regula a exploração de apostas de quota fixa no Brasil.
- Normas sobre a prevenção da lavagem de dinheiro e do financiamento ao terrorismo.
- Leis sobre combate à corrupção, incluindo a Lei nº 12.846, de 1º de agosto de 2013.
- Leis de proteção de dados pessoais, incluindo a Lei nº 13.709, de 14 de agosto de 2018.
- Requisitos sobre o jogo responsável e a prevenção do vício em jogos.

**2. Implementação de Políticas de Jogo Responsável**

O Órgão de Administração deve:

- Garantir que a empresa dispõe de políticas e mecanismos que estimulem o jogo responsável, protejam os menores de idade e promovam a integridade do processo de apostas. Isso inclui implementar limites nas apostas para evitar o jogo excessivo ou irresponsável e estabelecer medidas para identificar e tratar jogadores com problemas de vício.
- Fiscalizar a proibição do cadastro de pessoas impedidas de apostar, de acordo com o art. 26 da Lei nº 14.790/2023.
- Disseminar a cultura organizacional de prevenção à lavagem de dinheiro e outros crimes correlatos, bem como de integridade, boa governança e agenda ESG (ambiental, social e governança), inclusive nos termos da Lei nº 12.846/2013, para colaboradores, fornecedores e prestadores de serviços.

### 3. Prevenção e Monitoramento de Fraude e Lavagem de Dinheiro

O Órgão de Administração deve zelar pela implementação de políticas robustas de prevenção de fraude e lavagem de dinheiro. Isso implica:

- Conhecer adequadamente os riscos de lavagem de dinheiro e financiamento ao terrorismo aos quais a empresa está exposta em cada momento, bem como os processos utilizados para identificar, avaliar, monitorar e controlar esses riscos.
- Promover uma cultura de prevenção da lavagem de dinheiro e do financiamento ao terrorismo que abranja todos os colaboradores da empresa cujas funções sejam relevantes para a prevenção da lavagem de dinheiro e do financiamento ao terrorismo, baseada em elevados padrões de ética e integridade e, quando aplicável, na definição e aprovação dos oportunos códigos de conduta.
- Supervisionar e avaliar periodicamente a eficácia das políticas, procedimentos e controles, garantindo que sejam adotadas as medidas oportunas para corrigir as deficiências detectadas.
- Monitorar continuamente as transações financeiras e os procedimentos utilizados para analisá-las e classificá-las.
- Implementar sistemas de reporte de atividades suspeitas.
- Verificar a identidade dos clientes e realizar análises de riscos.

### 4. Proteção ao Consumidor

O Órgão de Administração é responsável por garantir que os direitos dos consumidores sejam protegidos, o que inclui:

- Assegurar que os termos e condições sejam claros e transparentes.
- Gerenciar corretamente os fundos dos clientes e garantir a transparência nas transações.

### 5. Auditoria e Transparência

Também é responsabilidade do Órgão de Administração assegurar que a empresa esteja sujeita a auditorias internas e externas periódicas. Isso inclui:

- Verificar as práticas financeiras e operacionais da empresa.
- Supervisionar os relatórios de auditoria e cumprir as recomendações dos auditores.
- Manter a transparência financeira nas operações da empresa.

**6. Compliance Fiscal**

Além da regulamentação específica do setor, o Órgão de Administração tem a responsabilidade de garantir que a empresa cumpra com as obrigações fiscais e tributárias, tanto a nível federal quanto estadual.

**7. Proteção de Dados e Privacidade**

Em virtude da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados), o Órgão de Administração deve assegurar que a empresa esteja cumprindo com as normativas sobre a privacidade dos dados dos usuários. Isso inclui:

- Coletar e tratar adequadamente os dados pessoais dos clientes, colaboradores e quaisquer outros.
- Implementar políticas para o armazenamento seguro e a proteção de dados pessoais, especialmente sensíveis (por exemplo, biometria).

**8. Observância à Regulamentação Específica do Setor**

O Órgão de Administração deve aderir às regulamentações e diretrizes emitidas pelos órgãos reguladores. À medida que o setor é objeto de mais regulações, os deveres nesse sentido podem aumentar e se diversificar.

# 5. Definições e Procedimentos

## 5.1 O Conceito de Lavagem de Dinheiro

A lavagem de dinheiro refere-se ao processo pelo qual uma pessoa ou entidade tenta ocultar, disfarçar ou transformar fundos obtidos de atividades ilegais (por exemplo, tráfico de drogas, corrupção, fraude, etc.) para que pareçam legítimos e sejam integrados ao sistema financeiro ou ao mercado legal.

Em seu artigo 1º, a Lei 9.613/1998, que trata sobre os crimes de lavagem de dinheiro, estabelece que a lavagem de dinheiro pressupõe as seguintes condutas:

- Ocultar ou disfarçar a natureza, a origem, a localização, a disposição, a procedência ou a titularidade de bens, direitos ou valores derivados direta ou indiretamente de um delito.
- Realizar transações financeiras ou comerciais com dinheiro obtido de delitos.
- Participar de um grupo, associação ou empresa sabendo que a sua atividade principal ou secundária está direcionada à prática das atividades mencionadas anteriormente.

**Normativas relevantes para o setor de apostas de quota fixa:**

No âmbito da Lei 9.613/1998 (sobre lavagem de dinheiro) e da legislação de aposta de quota fixa, as empresas do setor devem cumprir com as diretrizes do COAF, que supervisiona a prevenção da lavagem de dinheiro em todas as indústrias reguladas.

- **Monitoramento e denúncia de transações suspeitas**: Todas as transações financeiras devem ser monitoradas e, se detectadas atividades suspeitas, devem ser reportadas ao COAF.
- **Retenção de registros de transações**: Devem ser retidos registros detalhados de todas as transações realizadas pelos usuários, o que é crucial para as investigações de lavagem de dinheiro, por no mínimo cinco anos.

A lavagem de dinheiro refere-se ao contrabando de ativos obtidos ilegalmente, independentemente da procedência de natureza delituosa, no circuito econômico lícito com o objetivo de ocultar a verdadeira origem desses fundos. Este processo geralmente é dividido em três etapas:

- **Colocação**

Os ativos provenientes de crimes antecedentes como, por exemplo, roubo, tráfico de drogas ou outras atividades criminosas, são introduzidos no sistema financeiro legítimo, convertidos em dinheiro contábil e utilizados para adquirir ativos que podem ser liquidados a curto prazo. Isso pode ser feito por meio de depósitos, normalmente em entidades de crédito.

- **Ocultação**

O objetivo desta etapa é diversificar os fundos colocados na primeira etapa para evitar o

rastreamento até as fontes de origem. Os fundos são movidos através de múltiplas transações para criar confusão e distanciá-los de sua origem criminosa.

Na prática, frequentemente são realizadas transações financeiras complexas com esse fim. No entanto, os fundos também podem ser obtidos por meio de uma variedade de transações confusas e aparentemente não relacionadas. Isso pode incluir transferências bancárias entre diferentes contas, compra e venda de ativos, ou movimentações através de empresas de fachada.

- **Integração**

Na terceira etapa da lavagem de dinheiro, os fundos ou ativos são reintegrados ao circuito econômico legítimo, aparentando ser obtidos de acordo com a lei. Aqui, a origem criminosa das transações financeiras torna-se difícil de identificar devido ao estágio avançado do processo de lavagem de dinheiro.

### 5.1.1 Padrões de Lavagem de Dinheiro

As práticas típicas de lavagem de dinheiro são, por exemplo:

- Tentativas de depósito e/ou retirada em diferentes contas ou cartões de débito.
- Solicitações de retirada antes que os fundos depositados tenham sido apostados ao menos uma vez.
- Ocultação de identidade mediante o uso de documentos falsificados ou roubados.
- Estratégias de jogo para minimizar o risco de perda.

Os colaboradores, especialmente aqueles que lidam com clientes, são capacitados para reconhecer comportamentos suspeitos. Os colaboradores também recebem documentos que informam sobre comportamentos suspeitos/sinais de alerta, se necessário.

### 5.1.2 Fases da Lavagem de Dinheiro e Medidas de Prevenção de Riscos

Com o objetivo de prevenir o uso indevido das plataformas de aposta de quota fixa para a lavagem de dinheiro, são indicadas diferentes medidas nas três fases da lavagem de dinheiro:

**Colocação**

- Identificação dos clientes.
- Limites de depósito/aposta.

**Ocultação**

- Capacitação dos colaboradores para o reconhecimento de comportamentos de jogo suspeitos.
- Autorização para retirada somente após a identificação completa do cliente.

**Integração**

- Identificação dos clientes.
- Regras claras para a transferência de ganhos a cartões de crédito/contas bancárias.

## 5.2 O Conceito de Financiamento ao Terrorismo

O **financiamento do terrorismo** está regulado principalmente pela **Lei 13.260/2016**, que estabelece medidas para prevenir e sancionar o financiamento a atividades terroristas. Como sujeito obrigado, a empresa deve tomar medidas para evitar que sua plataforma seja utilizada para canalizar fundos para atividades terroristas. As medidas incluem:

- **Monitoramento de fundos:** A empresa deve ser diligente em detectar qualquer padrão incomum nas transações que possa indicar que os fundos estão sendo canalizados para atividades terroristas.
- **Colaboração com autoridades:** Em caso de suspeitas de financiamento ao terrorismo, a empresa deve colaborar com as autoridades competentes, como o COAF e o Ministério Público.
- **Cumprimento com as sanções internacionais:** A empresa deve aderir às sanções internacionais emitidas por organismos como a ONU e o Departamento de Controle de Ativos Estrangeiros dos EUA (*Office of Foreign Assets Control* – OFAC), assegurando que não facilitem o financiamento a grupos terroristas.

O financiamento ao terrorismo tem como objetivo fornecer fundos para atividades terroristas. Esta arrecadação de fundos pode ocorrer de diferentes maneiras, incluindo fontes legais – como doações pessoais e ganhos de empresas e organizações

beneficentes – e fontes criminosas – como o tráfico de drogas, o contrabando de armas, bens e serviços tomados indevidamente mediante a força, fraude, sequestro e extorsão.

O financiamento ao terrorismo é o apoio financeiro, por qualquer meio, ao terrorismo ou àqueles que fomentam, planejam ou cometem atos de terrorismo.

O combate contra o financiamento ao terrorismo está intimamente ligado àquele contra a lavagem de dinheiro, já que as técnicas utilizadas para lavar dinheiro são essencialmente as mesmas empregadas para ocultar a origem e o destino dos recursos alocados ao terrorismo. Dessa forma, as fontes de financiamento continuam enviando dinheiro sem serem identificadas. Geralmente, essas transações financeiras ocorrem repetidamente, em pequenas quantias que passam por diferentes contas bancárias abertas em paraísos fiscais. Esse processo dificulta o trabalho das autoridades e evita a exposição dos patrocinadores ao terrorismo e combate à prática.

## 6. Identificação do Cliente

A empresa implementou um rigoroso processo de verificação de identidade para todos os apostadores. O processo de KYC (Conheça seu Cliente) é uma ferramenta fundamental que assegura que todas as operações sejam realizadas com clientes legítimos e dentro do marco da legalidade.

Para realizar este processo, a empresa utiliza a plataforma CAF, uma solução avançada e altamente confiável para a verificação de identidade e documentos e autenticação biométrica. A CAF é uma plataforma tecnológica que cumpre com as regulamentações de prevenção à lavagem de dinheiro e financiamento ao terrorismo, proporcionando um alto nível de segurança e eficiência na verificação dos usuários em tempo real.

O processo de KYC consiste em:

1. **Coleta de Dados Pessoais:** Em primeiro lugar, solicita-se que clientes, ao se registrarem, forneçam dados cadastrais, conforme enumerado na Seção 6.1 (Cadastro) desta Política, além de outros dados necessários para cumprir com a regulamentação aplicável. Essas informações são fundamentais para conhecer nossos clientes e garantir que as transações realizadas em nossa plataforma sejam legítimas.

2. **Verificação de Documentos de Identidade:** Em seguida, os clientes devem enviar uma cópia de seus documentos de identidade oficiais, como passaporte, carteira de identidade (RG), etc. A plataforma CAF valida automaticamente esses documentos para assegurar sua autenticidade, utilizando tecnologia de escaneamento avançado. Essa tecnologia compara a imagem dos documentos com bases de dados relevantes, garantindo a confiabilidade da verificação.

   O processo inclui a validação da autenticidade do documento, utilizando métodos avançados para verificar sua validade e assegurar que não se trata de um documento falsificado ou manipulado.

3. **Autenticação Biométrica:** Como etapa adicional de validação, implementa-se um sistema de verificação biométrica que compara a fotografia fornecida pelo cliente em seus documentos com sua imagem em tempo real (*selfie*) mediante reconhecimento facial. Esta camada adicional de segurança ajuda a prevenir fraudes e garante que a pessoa que se registra na plataforma seja quem diz ser, protegendo tanto o cliente quanto a integridade do sistema.

4. **Verificação de PPEs e Pessoas Sancionadas:** Uma vez que os dados do cliente são coletados, o sistema da CAF realiza uma comparação automática com as listas de Pessoas Politicamente Expostas (PPEs) e sanções. Isso inclui buscar correspondências exatas ou parciais com nomes, sobrenomes, endereços e outros dados relevantes, além de analisar variantes de nomes ou apelidos que possam ter sido utilizados por uma pessoa politicamente exposta ou sancionada. Se for detectada uma correspondência, gera-se um alerta para ser avaliado pelo departamento de Risco, Fraude e Regulamentação.

   A análise inclui verificar se o cliente é uma pessoa politicamente exposta (PPE), um familiar até o segundo grau, um representante ou um colaborador próximo dessa pessoa.

5. **Avaliação de Riscos:** Após a verificação de identidade, o sistema realiza uma análise de risco para avaliar o perfil do cliente com base nas informações coletadas. Essa análise ajuda a identificar transações suspeitas e a classificar os clientes de acordo com seu nível de risco, permitindo que implementemos medidas adicionais de monitoramento ou investigação, se necessário.

6. **Monitoramento Contínuo**: O processo de KYC não se limita à verificação inicial. O

sistema de monitoramento contínuo supervisiona as transações e comportamentos do cliente ao longo de sua atividade na plataforma. Isso nos permite detectar qualquer anomalia ou atividade suspeita e agir de maneira imediata para prevenir a lavagem de dinheiro ou o financiamento ao terrorismo.

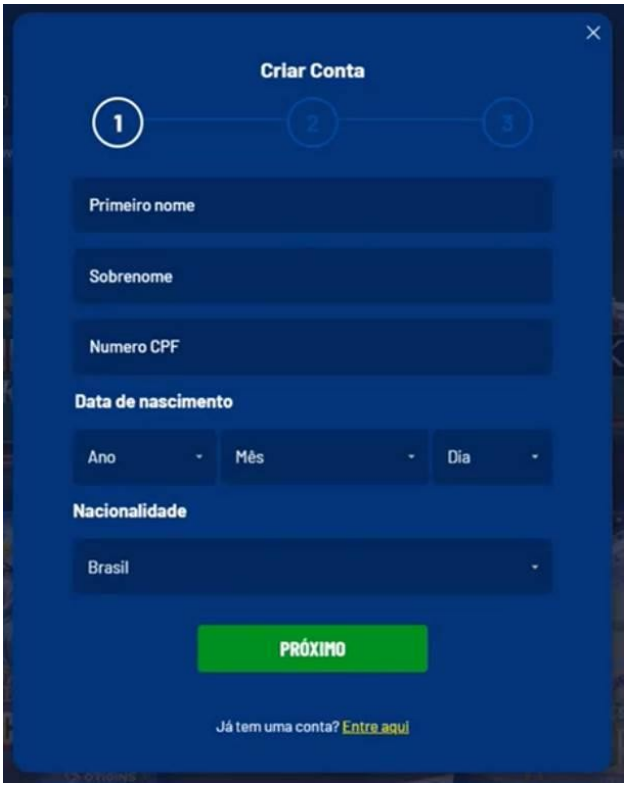
As informações coletadas durante a verificação devem **(i)** ser mantidas atualizadas, levando em consideração a evolução da relação com a pessoa qualificada e seu perfil de risco; **(ii)** ser utilizadas para a classificação dos apostadores e usuários da plataforma nas categorias de risco definidas nas avaliações internas de risco; e **(iii)** permitir avaliar a compatibilidade entre a capacidade econômica e financeira do apostador e as operações associadas a eles.

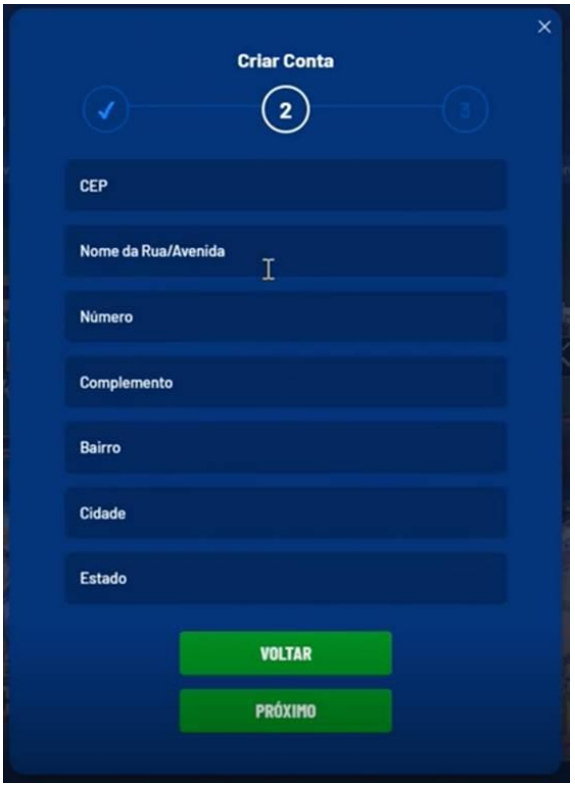
## 6.1 Cadastro

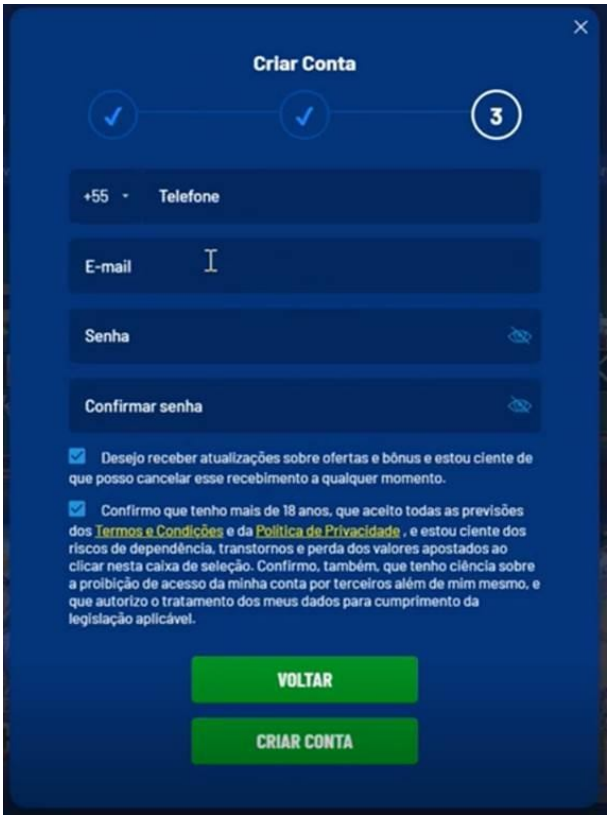
O cadastro do cliente deve conter as seguintes informações:

- Nome(s)
- Sobrenome(s)
- Número do documento de identidade (CPF / RMN)
- Data de Nascimento
- Nacionalidade
- Endereço (rua, número da casa, código postal, cidade, estado)
- Telefone móvel
- Endereço de e-mail
- Dados das contas de depósito ou de pagamento registradas
- Endereço IP registrado no momento da inscrição
- Senha

Como parte do processo de cadastro, será solicitado ao jogador, de forma obrigatória, as seguintes informações:



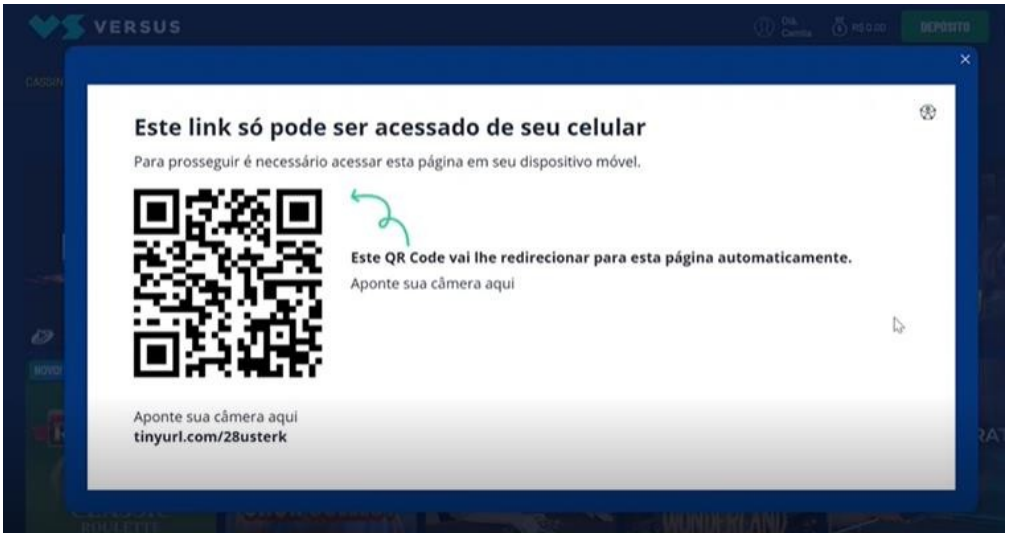




Após o envio dos dados de cadastro, a primeira etapa essencial que o cliente deve realizar

é fornecer seu documento de identidade. Para concluir essa etapa, a plataforma CAF fornece um código QR que o cliente deve escanear com seu celular e, seguindo as etapas fornecidas pela plataforma, concluir o processo de verificação do documento e a autenticação biométrica.

Sem concluir essa etapa, o usuário não poderá acessar a plataforma ou realizar qualquer outro gerenciamento dentro dela.




Uma vez que o cliente tenha enviado todos os documentos exigidos de maneira correta, o sistema de verificação da plataforma CAF inicia o processo automático de validação, cujas etapas são descritas acima.

Como parte do processo de cadastro, e para poder completar a verificação, a plataforma CAF solicita, na mesma sessão, a confirmação e verificação do e-mail e número de telefone. A plataforma envia dois códigos, um por e-mail para o endereço fornecido e outro por SMS para o número de telefone indicado no processo de cadastro. O cliente deve inserir os dois códigos e validá-los para poder completar a verificação. O processo é realizado na mesma sessão aberta com o celular. **Sem realizar esses passos e completar a verificação, a conta do usuário não será ativada.**

Para a gestão das contas de usuários, histórico de jogo, pagamentos, transações, etc., a Versus utiliza a plataforma **Playtech IMS** (Information Management System). A Playtech IMS permite à empresa realizar um acompanhamento detalhado dos dados dos clientes, criar regras automatizadas totalmente personalizadas, monitorar a atividade do usuário, revisar padrões de apostas e comportamentos suspeitos.

No momento do cadastro, antes que ele seja confirmado, é realizada uma verificação de contas duplicadas. Esse processo é realizado por meio das regras automatizadas da plataforma IMS e consiste em verificar se já existe uma conta de cliente com a mesma informação ou informações muito similares.

As duas plataformas utilizadas, CAF e IMS, estão completamente vinculadas e integradas. Dessa forma, ao detectar um usuário de alto risco, tentativa de falsificação de identidade, erro nos dados de cadastro, ou um usuário PPE, a plataforma CAF enviará instantaneamente e de forma automatizada a informação para a plataforma IMS. A plataforma IMS, por sua vez, atuará com base em regras personalizadas e tomará as medidas devidas de bloqueio preventivo. Além disso, enviará um alerta ao departamento de Risco, Fraude e Regulamentação, onde um técnico especializado avaliará e gerenciará o caso manualmente, revisando os dados.

Se for detectada uma conta duplicada, o cadastro será automaticamente rejeitado e, em caso de detectar uma conta com dados similares, a conta será temporariamente bloqueada e passará a ser revisada manualmente pelo departamento de Risco, Fraude e Regulamentação.

Em paralelo à verificação de duplicados, é realizada uma verificação do arquivo de bloqueio. Se houver uma proibição para o cliente nesse arquivo, o processo de cadastro será cancelado.

Se todos os dados e documentos fornecidos estiverem corretos e não forem detectados riscos relacionados ao cliente, o processo de cadastro será concluído, permitindo que o usuário acesse e utilize sua conta de jogador.

Além disso, é necessário identificar e reportar às autoridades os clientes sancionados, investigados ou acusados de terrorismo, financiamento ao terrorismo ou atos similares, conforme sancionado pelo CSNU e seus comitês de sanções.

## 6.2 Identificação/Verificação/Autenticação

A identificação é realizada principalmente por meio de documentos oficiais de identificação. Sua finalidade é identificar o usuário, garantindo a sua individualidade.

Os dados contidos no documento de identificação podem variar de acordo com o órgão

responsável por sua emissão, mas geralmente contêm o nome do portador, filiação, naturalidade, data de nascimento, Cadastro de Pessoas Físicas (CPF), além de conter outros dados que identificam o titular e a data e o local de emissão do documento.

O documento pode ser encontrado em vários formatos, papel, cartão ou digital.

Como parte do processo de verificação de identidade, o usuário deve vincular e verificar o método de pagamento disponível.

CIN Papel

Frente e verso

CIN Cartão

Frente e verso em cartão

CIN Digital

Versão digital no GOV.BR

### 6.2.1 Cidadãos Estrangeiros Residentes

A Carteira de Registro Nacional Migratório (CRNM) é emitida nos seguintes casos:

- Registro de imigrantes portadores de visto temporário.
- Autorização de residência concedida.

- Refugiado, apátrida ou solicitante de asilo, já reconhecido pelos órgãos competentes.


### 6.2.3. Verificação Automática

A plataforma “CAF” permite a identificação por meio de um processo automatizado que compara dados biométricos.

Para iniciar o processo de identificação/verificação, o cliente deve primeiro tirar uma foto da frente e do verso do documento de identidade. Após ler os dados de identificação, a CAF verifica as características de segurança para determinar se se trata de um documento autêntico.

Em seguida, deve-se tirar uma *selfie*, cujos dados biométricos serão comparados com os dados biométricos da fotografia no documento de identidade.

Se todos os dados estiverem corretos e o documento de identidade não apresentar suspeitas de ser falsificado e passar nas verificações do software CAF, a identidade do cliente será verificada corretamente.

### 6.2.4. Verificação Manual

Em algumas ocasiões, pode ser necessário realizar a verificação de identidade do usuário de forma manual. Este processo pode ocorrer por vários motivos, mas entre os principais estão os seguintes:

- Durante o cadastro, ocorreu algum erro tipográfico e os dados do cliente não coincidem 100% com os do seu documento de identidade.

- O cliente não consegue tirar a foto do documento de identidade conforme os parâmetros da plataforma e este processo não pode ser finalizado.
- A plataforma CAF detectou que o usuário está registrado nas listas de PPEs e pessoas sancionadas.
- As regras da plataforma IMS detectam algum risco relacionado ao usuário e bloqueiam a conta.

Em todos os casos, se um usuário não puder finalizar a verificação de forma automática utilizando a plataforma CAF, ele será encaminhado para o atendimento ao cliente e seu caso será revisado minuciosamente por um técnico do departamento de Risco, Fraude e Regulamentação.

Para verificar corretamente a identidade do usuário e descartar a falsificação de identidade e/ou cadastro utilizando dados falsos, os técnicos de Risco, Fraude e Regulamentação solicitam ao usuário uma foto da frente e do verso do documento de identidade e uma *selfie* para verificar a identidade do cliente e corroborar que se trata da mesma pessoa.

Como parte do processo de revisão, os técnicos podem acessar a plataforma CAF para verificar a tentativa de verificação do cliente, podendo acessar todas as informações fornecidas e as verificações de risco de identidade.

Todos os documentos fornecidos pelo usuário devem ser claros e completos, permitindo a visualização dos quatro cantos e de todos os dados legíveis. Documentos que estejam muito deteriorados, ou que apresentem flash, holograma ou reflexo que impeçam a visualização de qualquer dado, NÃO serão aceitos.

Os documentos válidos para a verificação de identidade são:

- Usuário estrangeiro residente no Brasil:

- Foto da Carteira de Registro Nacional Migratório (CRNM)

- Usuário brasileiro e residente no Brasil:

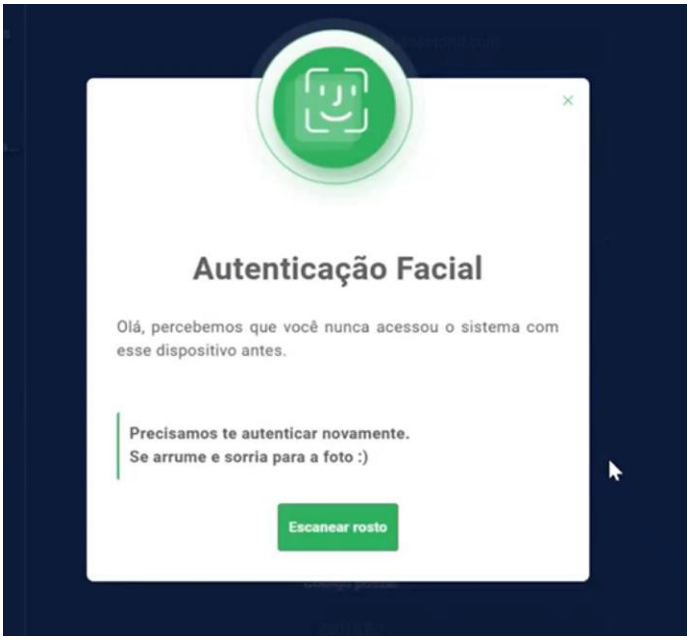
- Carteira de Identidade Nacional;

- Registro Geral - RG;

- Carteira Nacional de Habilitação - CNH; ou
- Passaporte.

### 6.2.5. Verificação Adicional

Como um processo adicional de verificação de identidade, toda vez que o cliente desejar fazer uma alteração relacionada aos seus dados pessoais (endereço, número de telefone, e-mail, conta bancária etc.), ele será solicitado a fazer uma verificação facial para verificar se é realmente o titular da conta que deseja fazer essas alterações.




Quando o processo de autenticação facial for concluído e verificado, a alteração feita será permitida.

## 7. Pessoas Jurídicas

A participação no jogo é reservada a pessoas físicas. As pessoas jurídicas estão proibidas de participar do jogo. Isso é feito por meio do cadastro e dos Termos e Condições, que estipulam que um jogador somente pode abrir uma conta de cliente se isso for feito em seu próprio nome e no seu próprio interesse, e não em nome de outra pessoa.

## 8. Pessoas Politicamente Expostas e Listas de Sanções

A verificação de PPEs (Pessoas Politicamente Expostas) e pessoas sancionadas é um componente essencial dentro do processo de KYC (Know Your Client) para garantir o cumprimento das regulamentações de prevenção à lavagem de dinheiro e financiamento ao terrorismo. Este processo é realizado utilizando tecnologia avançada para escanear e comparar os dados dos clientes com bases de dados globais que contêm listas de PPEs e pessoas ou entidades sancionadas.

A seguir, detalha-se como é realizada esta verificação de PPEs e pessoas sancionadas utilizando a ferramenta CAF:

**1. Integração de Bases de Dados de PPEs e Pessoas Sancionadas:**

A CAF se conecta com bases de dados globais e registros internacionais que contêm listas de PPEs e pessoas sancionadas. Essas bases de dados incluem fontes como:

- Listas da ONU
- Listas do OFAC
- Listas da União Europeia
- Listas de PPEs locais e regionais
- Outras listas de sanções nacionais e internacionais

**2. Comparação Automática de Dados do Cliente:**

- **Coleta de Dados:** Durante o processo de cadastro de um novo cliente, são coletados dados cadastrais como nome completo, endereço, data de nascimento e outros dados de identidade do cliente.
- **Verificação Automática:** Uma vez que os dados do cliente são coletados, o sistema realiza uma comparação automática com as listas de PPEs e pessoas sancionadas. Isso inclui buscar correspondências exatas ou parciais com nomes, sobrenomes, endereços e outros dados relevantes, além de analisar variantes de nomes ou apelidos que possam ter sido utilizados por uma pessoa politicamente exposta ou sancionada.

**3. Identificação de Correspondências:**

- **Alertas de Correspondências:** Se o sistema detectar uma correspondência entre

os dados de um cliente e as listas de PPEs ou pessoas sancionadas, gera uma alerta de correspondência. Estas alertas podem indicar que o cliente é potencialmente uma pessoa politicamente exposta ou que está associado a uma entidade sancionada.

- **Níveis de Correspondência:** O sistema avalia o nível de correspondência, levando em conta fatores como a exatidão do nome, a data de nascimento e outros detalhes de identidade. Se a correspondência for fraca (por exemplo, apenas uma semelhança parcial no nome), a plataforma pode realizar uma revisão manual ou gerar uma alerta de baixo risco.

**4. Avaliação de Risco:**

- **Avaliação de Risco**: Dependendo do grau de correspondência e do contexto (por exemplo, se a pessoa é uma figura política de perfil elevado ou se tem vínculos com governos ou empresas sancionadas), a plataforma atribui um nível de risco ao cliente. As pessoas identificadas como PPEs ou sancionadas podem ser classificadas como de alto risco.

- **Avaliação de Contexto:** No caso de identificação de uma PPE, é realizada uma etapa adicional de verificação manual do perfil da pessoa, como a sua exposição política ou as suas relações familiares, o que pode ajudar a determinar se a relação representa um risco significativo para a empresa ou se está na lista de pessoas proibidas de apostar.

**5. Monitoramento e Atualização Contínuos:**

- **Monitoramento Contínuo:** O sistema não apenas executa a verificação inicial, mas também fornece monitoramento contínuo dos bancos de dados de PPE e pessoas sancionadas. Isso significa que, se um cliente verificado anteriormente se tornar uma PPE ou for colocado em uma lista de sanções após o cadastro, o sistema detectará isso e gerará um alerta em tempo real.

- **Atualização Automática:** As listas de PPE e de pessoas sancionadas são constantemente atualizadas, de modo que o sistema mantém o processo de verificação atualizado, garantindo que as listas mais recentes e precisas estejam sempre sendo usadas.

**6. Procedimentos Posteriores à Correspondência:**

- **Revisão Manual:** Quando uma correspondência significativa é identificada com uma PPE ou com uma pessoa ou entidade sancionada, a equipe de Risco, Fraude e Regulamentação da empresa realiza uma revisão manual dos resultados. Isso pode envolver a solicitação de informações adicionais do cliente para confirmar a sua identidade e status.

- **Decisão sobre a Continuidade do Relacionamento Comercial:** Dependendo da avaliação de risco, o Órgão de Administração decide se deve continuar, suspender ou encerrar o relacionamento com o cliente, de acordo com as políticas internas de compliance. Se o cliente estiver vinculado a sanções internacionais, medidas adicionais poderão ser tomadas, como a comunicação da transação às autoridades competentes.

**7. Relatórios e Auditorias:**

- **Geração de Relatórios:** O sistema gera relatórios detalhados de PPEs e pessoas sancionadas, que podem ser usados para auditorias internas ou externas. Esses relatórios são fundamentais para demonstrar o cumprimento das normas locais.

- **Documentação de Compliance:** Todas as informações sobre PPEs e pessoas sancionadas são armazenadas com segurança e podem ser acessadas de forma transparente a qualquer momento, fornecendo um histórico completo da conformidade da plataforma com as normas de combate à lavagem de dinheiro e ao financiamento ao terrorismo.

## 9. Participantes Excluídos

Em virtude do artigo 26 da Lei nº 14.790/2023, fica proibida a participação, direta ou indireta, inclusive por meio de intermediário, como apostador, de:

- Menor de 18 (dezoito) anos de idade;

- Proprietário, administrador, diretor, pessoa com influência significativa, gerente ou funcionário do agente operador;

- Agente público com atribuições diretamente relacionadas à regulação, ao controle e à fiscalização da atividade no âmbito do ente federativo em cujo quadro de pessoal exerça suas competências;

- Pessoa que tenha ou possa ter acesso aos sistemas informatizados de loteria de apostas de quota fixa;
- Pessoa que tenha ou possa ter qualquer influência no resultado de evento real de temática esportiva objeto de loteria de apostas de quota fixa, incluídos:
    - Pessoa que exerça cargo de dirigente desportivo, técnico desportivo, treinador e integrante de comissão técnica;
    - Árbitro de modalidade desportiva, assistente de árbitro de modalidade desportiva, ou equivalente, empresário desportivo, agente ou procurador de atletas e de técnicos, técnico ou membro de comissão técnica;
    - Membro de órgão de administração ou de fiscalização de entidade de administração de organizadora de competição ou de prova desportiva;
    - Atleta participante de competições organizadas pelas entidades integrantes do Sistema Nacional do Esporte;
- Pessoas diagnosticada com ludopatia, por laudo de profissional de saúde mental habilitado;
- Pessoas impedidas de apostar por decisão administrativa ou judicial específica, quando formalmente notificado.
- Outras pessoas previstas na regulamentação do Ministério da Fazenda.

Segundo o § 1º do artigo 26 da referida Lei, as apostas realizadas em desacordo com as essas disposições são nulas de pleno direito.

As proibições previstas anteriormente se estendem aos cônjuges, companheiros e parentes em linha direta e colateral, até o segundo grau, inclusive, das pessoas impedidas de participar, direta ou indiretamente, como apostador.

Cabe à empresa implementar mecanismos que impeçam o cadastro daqueles que estão impedidos de apostar.

## 10. Diligência Reforçada

Em conformidade com a norma vigente sobre a prevenção de lavagem de dinheiro e financiamento ao terrorismo, bem como as regulações específicas, devem ser adotadas

medidas de diligência reforçada para certos casos considerados de alto risco. Essas medidas visam prevenir atividades ilícitas, garantindo a integridade do sistema financeiro e o cumprimento das leis locais e internacionais.

As medidas de diligência reforçada são essenciais para garantir que a empresa cumpra com as rigorosas normas de prevenção de lavagem de dinheiro e financiamento ao terrorismo. Essas medidas permitem mitigar riscos associados à lavagem de dinheiro e atividades fraudulentas, protegendo tanto os clientes quanto a empresa de possíveis implicações legais e financeiras. A implementação eficaz dessas medidas é crucial para garantir um ambiente de jogo seguro e em conformidade com a legislação vigente.

## 10.1 Classificação dos Clientes em Categorias de Risco

Com o objetivo de proporcionar um acompanhamento coerente, apropriado e sustentável, todos os clientes são classificados nas categorias de risco adequadas. A classificação pode ser manual, automatizada ou semiautomática, dependendo da responsabilidade do empregado/agente ou do sistema, entre outros fatores.

Em particular, o Departamento de Risco, Fraude e Regulação é responsável por verificar se há anomalias ou notificações de possíveis casos de lavagem de dinheiro e revisar a atividade da conta do cliente correspondente.

Posteriormente, os técnicos do Departamento de Risco e Fraude ajustarão imediatamente a classe de risco do cliente se houver uma suspeita razoável confirmada e implementarão as medidas definidas a seguir.

O procedimento de qualificação inclui:

- Avaliação da compatibilidade entre a capacidade econômica e financeira do apostador e as operações associadas a ele.
- Verificação da condição do apostador ou usuário da plataforma como pessoa politicamente exposta (PPE), familiar até o segundo grau, representante ou colaborador próximo de uma pessoa nessa condição.
- Avaliação cuidadosa das informações necessárias e relevantes coletadas e armazenadas no processo de cadastro.

Será dada especial atenção às apostas e operações associadas que indiquem:

- Falta de fundamento econômico ou jurídico.
- Incompatibilidade com atividades habituais ou práticas de mercado.
- Possível evidência de lavagem de dinheiro e financiamento ao terrorismo ou outro delito conexo.

Também serão analisadas com especial atenção as apostas e operações associadas nas quais estejam envolvidas:

- Pessoas envolvidas ou suspeitas de estarem envolvidas em atividades tipificadas como delito de lavagem de ativos e delitos contra o sistema financeiro.
- Pessoas que tenham cometido ou tentado cometer, facilitar ou participar em terrorismo, proliferação de armas de destruição em massa ou seu financiamento.
- Pessoas domiciliadas em jurisdições consideradas pelo Grupo de Ação Financeira (GAFI) como de alto risco ou com deficiências estratégicas em matéria de prevenção da lavagem de dinheiro e financiamento ao terrorismo, ou em países ou dependências qualificadas pela Receita Federal como regime fiscal favorecido ou privilegiado (https://www.gov.br/coaf/pt-br/assuntos/informacoes-as-pessoas-obrigadas/avisos-e-alertas/comunicados-do-gafi/jurisdicoes-sujeitas-a-monitoramento-intensificado-2013-fevereiro-de-2024).
- Resistência do usuário em fornecer informações adicionais quando solicitadas pela empresa.
- Fornecimento de informações falsas ou difíceis de verificar, especialmente para formalizar o cadastro, abrir uma conta, registrar uma aposta ou outra operação na plataforma de apostas.
- Pagamento de um prêmio suspeito de ser utilizado para prevenção de lavagem de dinheiro e financiamento ao terrorismo ou fraude.
- Pagamento do prêmio de uma aposta cujo resultado seja suspeito de manipulação (por exemplo, conluio).
- Incompatibilidade entre as operações realizadas por um cliente e seu padrão habitual de atividades.

- Movimentação atípica de valores que possa sugerir o uso de uma ferramenta automatizada pelo cliente.
- Depósito ou retirada de fundos em um curto período que possa sugerir fracionamento ou ocultação da operação.
- Retirada, ou tentativa de retirada, de fundos da conta transacional do cliente, imediatamente após fazer um depósito, sem realizar uma aposta.
- Uso indevido de uma conta por pessoa distinta de seu titular.
- Evidência de que a conta está sendo utilizada por um intermediário que realiza apostas para outras pessoas.
- Qualquer característica que indique, especialmente devido à sua natureza incomum ou atípica, possíveis indícios de lavagem de dinheiro, financiamento ao terrorismo ou qualquer outro delito relacionado.

## 10.2 Classificação dos Empregados, Fornecedores e Prestadores de Serviço

Em conformidade com o capítulo II, seção 1 da Portaria SPA/MF n° 1.143/2024, a empresa adota e implementa políticas, procedimentos e controles internos de prevenção à lavagem de dinheiro e financiamento ao terrorismo, observando as disposições da Lei 9.613/1998, da Lei 13.260/2016 e da Lei 13.810/2019, bem como a prevenção de outros delitos conexos, de acordo com a legislação aplicável. As políticas internas de prevenção à lavagem de dinheiro e financiamento ao terrorismo incluem as seguintes diretrizes:

- Desenvolvimento, implementação e execução de um programa de *compliance* que promova a difusão de uma cultura organizacional para prevenir a lavagem de dinheiro, financiamento ao terrorismo e outros delitos relacionados, bem como a integridade, a boa governança e a agenda ESG (ambiental, social e de governança), para empregados, fornecedores e prestadores de serviços.
- Realização periódica e contínua de atividades de informação e capacitação em matéria de prevenção à lavagem de dinheiro, financiamento ao terrorismo e outros delitos conexos, abrangendo empregados, fornecedores e prestadores de serviços.

Além disso, os procedimentos internos de prevenção à lavagem de dinheiro e financiamento ao terrorismo incluem:

- Identificação, qualificação e classificação de risco de empregados, fornecedores e prestadores de serviços.
- Avaliação e classificação de riscos em suas atividades comerciais, contratação e desenvolvimento de produtos, operações com ativos financeiros e imobiliários.
- Avaliação e classificação de riscos na contratação de empregados, fornecedores e prestadores de serviços.

### 10.3 Pessoas Politicamente Expostas

Quando se trata de pessoas politicamente expostas (PPEs), cumprem-se as obrigações de diligência reforçada em conformidade com a lei contra a lavagem de dinheiro, conforme o artigo 12 A, § 2º da Lei 14.478/2022.

Para isso, são solicitados documentos que comprovem a origem dos fundos, o que pode incluir, entre outros, recibos de salário, certificados de herança, extratos bancários e, se aplicável, outros documentos.

Além da procedência dos fundos, também deve haver um maior acompanhamento da relação comercial até cinco anos a partir da data em que a pessoa deixa de ocupar um cargo que a habilite nessa condição.

## 11. Transações de Pagamento

A empresa somente aceita métodos de pagamento não anônimos e os identifica claramente como parte da oferta de jogo. Não é possível o uso de outros métodos de pagamento.

As contribuições e retiradas de recursos financeiros por parte dos clientes, bem como o pagamento de prêmios por parte da empresa, devem ser realizados exclusivamente por meio de transferência eletrônica entre uma conta registrada e verificada previamente pelo cliente e a conta transacional da empresa, ambas mantidas em instituições financeiras ou de pagamento autorizadas a operar pelo Banco Central do Brasil.

Segundo a Portaria SPA/MF n° 615/2024, só é permitido o uso dos seguintes métodos de pagamento/serviços de pagamento:

- Transferência mediante Pagamento Instantâneo – PIX

- Transferência Eletrônica Disponível – TED
- Cartão de débito ou pré-pago
- Transferência nos próprios livros.

Como a empresa não permite métodos de pagamento anônimos, cada um dos métodos de pagamento mencionados acima deve sempre corresponder ao titular da conta de jogo e ao titular da conta de pagamento ou ao usuário do método de pagamento.

No contexto do uso de um cartão de débito ou pré-pago, tanto a empresa quanto a plataforma de pagamento recebem apenas os dados do titular (sobrenome, nome) do cartão de débito ou apenas os dados do proprietário (sobrenome, nome, etc.) do cartão pré-pago. As informações sobre a conta de pagamento à qual o cartão está vinculado para fins de faturamento estão fora do alcance de acesso da empresa ou do provedor de serviço de pagamento (PSP) e, portanto, não podem ser verificadas.

A empresa de cartão de crédito ou o fornecedor também não têm a obrigação de transmitir essas informações ao PSP. No entanto, se um cartão de débito puder ser usado como método de depósito e retirada, normalmente é garantido que se trate apenas de uma conta de pagamento. O banco emissor do cartão de crédito garantirá que o titular do cartão de crédito ou pré-pago e o titular da conta de pagamento (conta bancária) designada para a liquidação respectiva sejam idênticos.

O uso dos seguintes métodos de pagamento é completamente vedado:

- Dinheiro
- Comprovantes de pagamento
- Cheques
- Ativos virtuais ou outros tipos de criptoativos
- Pagamentos ou transferências de contas que não tenham sido previamente registradas pelo apostador
- Pagamentos ou transferências de terceiros
- Cartões de crédito ou qualquer outro instrumento de pagamento pós-pago

- Qualquer alternativa de transferência eletrônica não prevista anteriormente

## 11.1 Verificação do Método de Pagamento

A empresa deve garantir que o titular da conta de jogo e o titular da conta de pagamento coincidam nas transações de pagamento e que um cliente não utilize contas de pagamento diferentes para ocultar a origem e o destino dos fundos apostados.

Portanto, o cliente deve ter o método de pagamento verificado antes de solicitar a retirada de fundos.

Todas as solicitações de reembolso de fundos dos clientes serão analisadas de forma automatizada e passarão por uma série de regras automáticas criadas na plataforma IMS antes de serem completamente validadas.

Dependendo do valor da retirada a ser processada, as retiradas passarão por diferentes níveis de regras e aprovações automáticas antes de serem validadas e emitidas para o método de pagamento previamente registrado e verificado pelo cliente.

Se necessário, devido ao risco do cliente ou suspeitas de transações fraudulentas, pode ser realizada uma verificação adicional pelo departamento de Risco, Fraude e Regulação. Nesse caso, os técnicos terão a tarefa de verificar que uma pessoa é o titular de uma conta bancária e, geralmente, poderão solicitar ao usuário um dos seguintes documentos:

- Comprovante de residência recente (como uma fatura de serviços públicos ou um contrato de aluguel).
- Cartão de débito ou crédito associado à conta.
- Documentos relacionados à conta bancária onde conste o Código de Identificação Bancária (CIB) e os dados do titular.

Para verificar o comprovante de conta em que apareça a assinatura do usuário, o documento deve atender aos seguintes requisitos:

- Data de emissão.
- Código de Identificação Bancária (CIB).
- Código BIC/SWIFT do banco.

- Nome completo do usuário como titular da conta bancária.
- Identificação/logotipo do banco.
- Se for um documento impresso da web, deve estar datado e conter a URL/link para o site do banco.
- Se for um comprovante em papel, deve estar carimbado e assinado pelo banco, e deve ser enviada uma fotografia legível com as 4 bordas visíveis.

NÃO são aceitos:

- Capturas de tela.
- Scans.
- E-mails reenviados do banco (nem mesmo em .pdf).
- Provas em preto e branco.
- Documentos ilegíveis, cortados e sem as 4 bordas visíveis

Em caso de suspeita de documento falsificado ou se for identificado que um documento pertence a um terceiro, o departamento de Risco, Fraude e Regulação fará uma identificação minuciosa do usuário aplicando as medidas de diligência reforçada.

## 12. Treinamento de Equipe

Uma peça essencial na aplicação dessa Política e na implementação das medidas preventivas e de controle estabelecidas pela empresa é o treinamento de equipe.

Para isso, um exemplar dessa Política será fornecido a todos mencionado a seguir, por serem responsáveis pela aplicação das medidas de diligência nele contidas:

- Órgão de Administração.
- Equipe de gestão.
- Colaboradores encarregados de executar o pagamento e/ou verificar a identidade do usuário.

- Todos aqueles que ocupam uma posição compatível com a identificação de eventos ou operações que possam estar relacionados à lavagem de dinheiro.
- Todos os colaboradores que forem determinados pelo Órgão de Administração, após consulta à Responsável por Integridade e Compliance.

Com base nisso, o plano de treinamento será implementado por meio de cursos e circulares internos, cada um dos quais será aprovado pelo Órgão de Administração sob proposta da Responsável.

Todos os indivíduos mencionados anteriormente deverão participar dos treinamentos. Deve-se dar especial atenção ao treinamento das pessoas encarregadas do pagamento de prêmios e/ou verificação da identidade do usuário, devido à natureza da atividade que desenvolvem.

As novidades legislativas que surgirem, bem como qualquer outra inovação relevante, serão comunicadas à equipe por meio de treinamentos de apoio ou circulares dirigidas aos departamentos afetados.

Os treinamentos serão ministrados pela Responsável, salvo se for considerada necessária a participação de algum especialista externo contratado para esse fim.

O conteúdo do treinamento básico contemplará as seguintes matérias:

- Explicação do fenômeno da lavagem de dinheiro e do financiamento ao terrorismo na atualidade.
- Principais obrigações a serem cumpridas no setor.
- Estrutura interna: os órgãos de controle.
- O conceito de paraíso fiscal.
- As operações de risco no setor de jogos.
- Procedimentos de comunicação de operações de risco.
- Crimes relacionados com a lavagem de dinheiro.

### 12.1 Documentação de Treinamentos Realizados

Os treinamento são documentados e os dados armazenados de forma a serem auditáveis.

A documentação deve incluir, no mínimo, para cada colaborador e cada treinamento realizado:

- Data da atividade formativa.
- A natureza e o objetivo do treinamento.
- Identidade dos empregados treinados.
- Resultados das avaliações de aprendizagem realizadas para cada empregado.

### 12.2 Classificação de Riscos dos Empregados

De acordo com a legislação aplicável, a empresa adota as seguintes políticas e procedimentos internos de prevenção à lavagem de dinheiro e financiamento ao terrorismo:

- Identificação, qualificação e classificação de risco de empregados, fornecedores e prestadores de serviços.
- Desenvolvimento, implementação e execução de um programa de *compliance* que promova a difusão de uma cultura organizacional para prevenir a lavagem de dinheiro, financiamento ao terrorismo e outros delitos relacionados, bem como a integridade, a boa governança e a agenda ESG (ambiental, social e de governança), inclusive sob os termos da Lei n.º 12.846/2013, para empregados, fornecedores e prestadores de serviços.
- Realização periódica e contínua de atividades de informação e capacitação em matéria de prevenção à lavagem de dinheiro, financiamento ao terrorismo e outros delitos conexos, abrangendo empregados, fornecedores e prestadores de serviços.

## 13. Comunicações de Boas Práticas e Operações de Risco

Como agente operador de apostas, a Versus deve cumprir as normativas de prevenção à lavagem de dinheiro e financiamento ao terrorismo, o que inclui a apresentação de diversos relatórios periódicos ao COAF. A seguir, detalham-se os relatórios que devem ser apresentados:

**1. Relatório Anual de Boas Práticas**

- **Frequência:** Anual (até 1º de fevereiro do ano seguinte).
- **Conteúdo:** Este relatório deve resumir as boas práticas adotadas durante o ano em termos de políticas, procedimentos e controles de prevenção à lavagem de dinheiro e financiamento ao terrorismo. Inclui detalhes sobre as políticas implementadas, as atividades de capacitação realizadas, os sistemas de monitoramento utilizados e as medidas adotadas para prevenir riscos, entre outros. O relatório deve ser apresentado diretamente à Secretaria de Prêmios e Apostas.
- **Fundamento Jurídico:**
    - Portaria SPA/MF n.º 1.143/2024 (Art. 11)

**2. Relatório de Operações Suspeitas**

- **Frequência:** Conforme necessário (quando uma operação suspeita for identificada).
- **Conteúdo:** Este relatório deve apresentar qualquer operação que seja considerada suspeita de estar vinculada a atividades ilícitas, como lavagem de dinheiro ou financiamento ao terrorismo. As operações devem ser reportadas ao COAF assim que identificadas. Se uma transação apresentar características de atividade suspeita (por exemplo, padrões incomuns, repetitivos, sem justificativa clara ou com fundos de procedência duvidosa), deve ser reportada.
- **Fundamento Jurídico:**
    - Lei nº 9.613/1998 (Art. 10, 11 e Art. 14): Estabelece a obrigação dos sujeitos obrigados de reportar operações suspeitas ao COAF.
    - Portaria SPA/MF n.º 1.143/2024 (Art. 27).

Em virtude da Lei n° 9.613/1998, a empresa tem a obrigação de comunicar ao COAF, abstendo-se de dar ciência de tal ato a qualquer pessoa, inclusive àquela à qual se refira a informação, no prazo de 24 (vinte e quatro) horas, a proposta ou realização:

- De todas as transações em moeda nacional ou estrangeira, títulos e valores mobiliários, títulos de crédito, metais, ativos virtuais ou qualquer ativo suscetível de ser convertido em dinheiro, que excedam o limite fixado pela autoridade competente, acompanhadas da identificação do usuário.

- As operações que, de acordo com instruções emitidas pelas autoridades competentes, possam constituir sérios indícios dos delitos previstos na Lei n° 9.613/1998, ou estar relacionadas a eles.

- Devem comunicar ao órgão regulador ou supervisor de sua atividade ou, na falta deste, ao COAF, dentro da periodicidade, forma e condições estabelecidas por ele, a não ocorrência de propostas, transações ou operações.

O COAF colocará as comunicações recebidas à disposição dos respectivos órgãos encarregados de regular ou fiscalizar as pessoas sujeitas ao mecanismo de controle a que se refere o art. 9º da Lei n° 9.613/1998.

O prazo para completar o procedimento de análise é de 30 (trinta) dias, contados a partir da data da aposta ou da operação associada a ela.

A análise e a conclusão devem ser documentadas e seu registro deve ficar disponível para efeitos demonstrativos da Secretaria de Prêmios e Apostas, independentemente de terem dado origem ao envio de comunicação ao COAF.

**As comunicações ao COAF devem:**

- Conter uma indicação dos elementos nos quais a análise relevante foi baseada e explicar as razões para concluir que havia indícios de lavagem de dinheiro e financiamento ao terrorismo ou outra infração.

- Mencionar a possível existência de um intermediário no contexto dos fatos relatados.

- Detalhar as características da aposta ou outra transação associada relatada, como categoria ou tipo de jogo ou aposta, forma de pagamento e origem e destino dos fundos envolvidos.

- Apresentar informações obtidas nos procedimentos de identificação, qualificação e classificação de risco do apostador, do usuário da plataforma ou de outros envolvidos, que sejam relevantes para esclarecer a suspeita ou reconhecer a natureza incomum ou atípica do que está sendo denunciado.

É terminantemente proibido o compartilhamento de quaisquer informações sobre as comunicações ao COAF com qualquer pessoa que não seja o próprio COAF e a Secretaria de Prêmios e Apostas, incluindo apostadores, usuários da plataforma, demais envolvidos ou

quaisquer terceiros, sob pena de responsabilização.

## 14. Comunicação de Não Ocorrência à Secretaria de Prêmios e Apostas

A **obrigação de realizar um relatório anual de "Comunicação de Não Ocorrência"** está vinculada principalmente às normativas derivadas da **Lei 13.756/2018** e da Portaria SPA/MF 1.143/2024, além de ser complementada pelas **normas do COAF** sobre prevenção à lavagem de dinheiro. Este relatório deve ser apresentado à Secretaria de Prêmios e Apostas para garantir o cumprimento das obrigações legais e normativas.

Este relatório deve ser apresentado para confirmar que, no período respectivo, não foi detectada nenhuma atividade fora das normativas estabelecidas, nem ocorreram eventos ou situações de risco relacionadas à lavagem de dinheiro ou ao financiamento ao terrorismo.

## 15. Retenção de Registros e Documentos

A Versus deve reter os registros e documentos relacionados ao cumprimento das disposições da Portaria SPA/MF 1.143/2024, por pelo menos 5 (cinco) anos, sem prejuízo dos demais deveres previstos na legislação.

## 16. Procedimentos de Comunicação Interna e Relatórios

O empregado deve enviar à Responsável um relatório contendo os seguintes dados:

- Dados da(s) pessoa(s) envolvida(s) na operação.
- Atividade conhecida da(s) mesma(s).
- Relação de operação(ões) considerada(s) de risco.
- Indicação das gestões efetuadas pelo empregado para investigar a(s) operação(ões).

Deve ser remetida também a documentação adicional existente relativa à referida operação, tudo com a máxima confidencialidade e diligência.

Após analisar os dados, o Responsável decidirá se a operação efetivamente apresenta ou não risco ou se está relacionada à lavagem de dinheiro.

Se concluir que a operação pode estar relacionada à lavagem de dinheiro e/ou ao financiamento ao terrorismo, a operação será comunicada imediatamente ao COAF.

Caso contrário, se concluir que a operação não apresenta indícios de lavagem de dinheiro e/ou financiamento ao terrorismo, nenhuma ação será tomada.

Para fins dessa Política, sem prejuízo de outras situações que a Versus pode vir a identificar como suspeita, deve resultar na análise com especial atenção as apostas e operações a elas associadas que envolvam:

- Pessoa envolvida ou suspeita de envolvimento em atividades tipificadas como crime de lavagem de dinheiro e crimes contra o sistema financeiro;
- Pessoa que tenha cometido ou tentado cometer, facilitar ou participar de práticas de terrorismo, proliferação de armas de destruição em massa ou seu financiamento;
- Pessoa domiciliada em jurisdição considerada pelo Grupo de Ação Financeira Internacional (Gafi) como de alto risco ou com deficiências estratégicas em matéria de PLD/FTP ou em países ou dependências qualificados pela Secretaria Especial da Receita Federal do Brasil (RFB) como de tributação favorecida ou regime fiscal privilegiado;
- Resistência do apostador ou usuário da plataforma em fornecer informações adicionais solicitadas pelo agente operador de apostas;
- Prestação de informações falsas ou de difícil verificação, notadamente para a formalização de cadastro, abertura de conta, registro de aposta ou outra operação na plataforma de apostas;
- Aporte de valores sobre os quais recaia suspeita quanto à sua origem;
- Pagamento de prêmio sobre o qual recaia suspeita de utilização para LD/FTP ou fraude;
- Pagamento de prêmio de aposta sobre o qual recaia suspeita de manipulação de resultados;
- Incompatibilidade entre as operações realizadas por apostador e seu padrão habitual de atividades, suas informações ocupacionais ou sua aparente situação financeira;
- Movimentação atípica de valores de forma que possa sugerir o uso de ferramenta automatizada por parte do apostador;

- Aporte ou retirada de valores, em um curto tempo, que possa sugerir fracionamento ou dissimulação de operação;
- Retirada, ou tentativa de retirada, de recursos da conta transacional de apostador, logo após a realização de depósito, sem a efetivação de aposta;
- Utilização indevida de conta por outra pessoa que não seu titular;
- Indício da utilização de conta por intermediador que realize apostas para outras pessoas;
- Aportes em quantidade que possa sugerir a prática de intermediação de apostas;
- Aposta na categoria bolsa de apostas (bet exchange) na qual haja indício de arranjo por dois ou mais apostadores em apostar em resultados diferentes, com a finalidade de realizar transferência de valores entre si, visando a prática de LD/FTP;
- Contas abertas em nome de pessoa exposta politicamente (PEP);
- Dificuldade ou inviabilidade de coletar, verificar, validar ou atualizar informações cadastrais de apostadores ou usuários da plataforma; e
- Quaisquer características que sinalizem, notadamente por seu caráter não usual ou atípico, possível indício de prática de LD/FTP ou outro delito correlato.

Esta Política e seus procedimentos devem ser avaliados periodicamente. A avaliação da eficácia deverá ser devidamente documentada em um relatório específico a ser preparado anualmente, com data base de 31 de dezembro e, posteriormente, submetido ao Órgão de Administração para avaliação. O relatório deverá conter informações que descrevam a metodologia adotada na avaliação da eficácia, os testes aplicados, as classificações dos avaliadores e as deficiências identificadas.