# POLITICAS DE COMPLIANCE

Ser cumpridora das leis, mantendo as melhores práticas de segurança e conduta, é o compromisso da RIBUS TECNOLOGIA junto aos nossos clientes, parceiros e toda a comunidade.

## Transparência e boas práticas

A missão RIBUS, é transformar o jeito como as pessoas lidam com nossa tecnologia, de forma segura e transparente.

O nosso mercado é descentralizado, por isso não está ligado a órgãos governamentais ou países. Porém, como existem transações financeiras de compra e venda de nossos tokens em nossa plataforma, ela está sujeita a políticas rígidas de controle associadas à Lei de Anticorrupção e às Leis de Combate à Lavagem de Dinheiro e Financiamento ao Terrorismo.

Investimos em estrutura e segurança da informação para garantir que todas as transações estejam em conformidade com a legislação

# SUMÁRIO



## 1.Objetivo

Esta política tem por objetivo estabelecer os conceitos, diretrizes e regras de gestão de riscos, visando a RIBUS TECNOLOGIA , os clientes e o público em geral.

## 2.Abrangência

Esta política aplica-se a todos os administradores, sócios, funcionários, estagiários e prestadores de serviços da RIBUS TECNOLOGIA (Empresa).

## 3.Conceitos

- Risco: ameaças ou ações que possam impactar os objetivos da Empresa.
- Apetite a Riscos: nível de exposição à riscos que a Empresa está disposta a aceitar.
- Controles: políticas, normas, procedimentos, atividades e mecanismos desenvolvidos para assegurar que os objetivos de negócios sejam atingidos e que eventos indesejáveis sejam prevenidos ou detectados e corrigidos.

- Atividades de Controles: Conjunto de ações, políticas, normas, procedimentos e sistemas, com os quais se visa salvaguardar os ativos, assegurando que seus riscos sejam conhecidos e mitigados adequadamente.

## 4.Diretrizes

Estabelecer as regras para gerenciamento de risco, baseada nas melhores práticas e regulações existentes, por meio da segregação das linhas de defesa e pelo monitoramento dos controles internos.

São consideradas “linhas de defesa” as segregações de funções, papéis, responsabilidades, áreas e práticas com o objetivo de mitigar a materialização dos riscos que possam acarretar prejuízos a Empresa.

1. Primeira linha de defesa:

   A primeira linha de defesa é a responsável direta por gerir, identificar, monitorar e mitigar a materialização dos riscos. Normalmente são associadas às funções, práticas e áreas que mantém os processos de negócios da Empresa. Desta forma, esta linha de defesa possui os objetivos:

   - Identificar, avaliar, controlar e mitigar os riscos;
   - Implementar ações para o tratamento dos riscos;
   - Manter controles internos eficazes;
   - Informar potenciais prejuízos.

2. Segunda linha de defesa:

   A segunda linha de defesa é a responsável pela monitoração dos níveis de riscos, de forma a assegurar que estejam dentro do “apetite de risco” estabelecido. Desta forma, esta linha de defesa possui os objetivos:

   - Implantar a estrutura de gerenciamento de riscos;
   - Fornecer orientação sobre gestão de riscos e práticas;
   - Assegurar o estabelecimento de limites e alçada de aprovação;
   - Monitorar os riscos e perdas operacionais;
   - Monitorar a eficácia dos controles internos e ações mitigadoras;

- Prover visibilidade aos gestores quanto a situação do ambiente de controle e riscos.

3. Terceira linha de defesa:

   A terceira linha de defesa é a responsável pela avaliação independente dos controles internos e riscos para à alta administração da Empresa. Desta forma, esta linha de defesa possui os objetivos:

   - Auditar os processos e controles internos de forma independente;
   - Prover avaliações sobre a eficácia do gerenciamento de riscos e dos controles internos.

## 5.Regras para gerenciamento de riscos

A estrutura de gerenciamento de risco deve ser segregada por linhas de defesa, capaz de avaliar periodicamente os processos, práticas e controles com o objetivo de identificar e mensurar vulnerabilidades que podem acarretar perdas e, consecutivamente, impactar os objetivos de negócio.

Os processos devem possuir atividades de controles que assegurem que seus riscos sejam conhecidos, controlados e mitigados adequadamente.

A mensuração do risco deve considerar a exposição à vulnerabilidade e ao impacto, com base nos limites descritos abaixo.

1. Identificação da vulnerabilidade.

   - Os riscos devem ser identificados, avaliados, documentados e formalizados de forma estruturada para que sejam conhecidos e tratados.
   - Os riscos devem ser avaliados e mensurados considerando o nível de exposição à vulnerabilidade frente ao impacto para Empresa

2. Mensuração de vulnerabilidade

   Abaixo a escala de vulnerabilidade que deve ser considerada para a mensuração do risco:

- Baixo: Existência de controles internos eficazes para mitigação dos riscos.
- Médio: Predominância de controles internos eficazes para mitigação dos riscos.
- Alto: Poucos controles eficazes para mitigação dos riscos.
- Extremo: Inexistência ou predominância de controles ineficazes para mitigação dos riscos.

3. Mensuração do impacto

   mensuração do risco deve ser realizada como base no impacto sob as perspectivas financeira, reputacional e regulatório.

4. Impacto financeiro

   Abaixo a escala de impacto financeiro que deve ser considerada para a mensuração do risco:

   - Baixo: Até R$ 30.000,00
   - Médio: Entre R$ 30.000,01 a R$ 100.000,00
   - Alto: Entre R$ 100.000,01 a R$ 500.000,00
   - Extremo: Acima de R$ 500.000,00

5. Impacto reputacional

   Abaixo a escala de impacto reputacional que deve ser considerada para a mensuração do risco:

   - Baixo: Impacto irrelevante na reputação, em pequeno grupo de cliente e com rápida remediação.
   - Médio: Impacto mínimo na reputação, atenção da mídia local e reversíveis no curto prazo.
   - Alto: Impacto relevante na reputação, atenção da mídia de forma generalizada e com possibilidade de remediação.
   - Extremo: Impacto relevante na reputação, atenção da mídia nacional e com improvável remediação.

6. Impacto regulatório

Abaixo a escala de impacto regulatório que deve ser considerada para a mensuração do risco:

- Baixo: Notificações legais, sem penalidades ou multa.
- Médio: Aplicação de multas ou sanções não significativas.
- Alto: Aplicação de multas ou sanções significativas que não impactam a continuidade das operações de negócio.
- Extremo: Aplicação de multas ou sanções que impactam a continuidade das operações de negócio.

7. Tratamento e monitoração

Os riscos devem ser tratados conforme sua exposição e prioridade. Desta forma, as medidas abaixo podem ser adotadas como tratamento do risco:

- Evitar: descontinuar atividades, produtos, negócios, práticas ou processos que acarretam os riscos identificados.
- Reduzir: adotar medidas ou ações para reduzir a vulnerabilidade ou impacto do risco identificado.
- Compartilhar: transferir a vulnerabilidade ou impacto para terceiros (ex.: seguros, hedging, etc.).
- Aceitar: nenhuma medida é adotada.

As ações, controles e processos relacionados ao tratamento do risco devem ser avaliados periodicamente com o objetivo de assegurar que as medidas adotadas foram eficazes.

8. Prazo de tratamento

Os responsáveis pelo risco, gestores da primeira linha de defesa, devem realizar o tratamento do risco conforme o nível de exposição e dentro dos prazos abaixo:

- Baixo: até 365 dias após a identificação.
- Médio: até 180 dias após a identificação.
- Alto: até 60 dias após a identificação.
- Extremo: até 30 dias após a identificação.

Os riscos que possuem impactos regulatórios devem ser tratados dentro dos prazos estipulados pelos órgãos reguladores e lei.

9. Alçada de aprovação

   Os tratamentos dos riscos devem ser aprovados pela alçada abaixo:

   - Baixo: Gestor direto, responsável pelo processo, prática ou negócio;
   - Médio: Líder ou Diretor do processo, prática ou negócio;
   - Alto: Diretor geral;
   - Extremo: Sócios.

10. Ocorrências e incidentes

    Os riscos materializados devem ser registrados, os prejuízos contabilizados e os tratamentos previstos para que a Empresa possa evitar, reduzir, compartilhar ou aceitar a recorrência desses eventos.

## 6.Papéis e responsabilidades

1. Sócios-Administradores
   Responsabilidades dos Sócios-Administradores:

   - Definir "interesse de risco" da Empresa;
   - Anuir os tratamentos de riscos extremos;
   - Acompanhar a evolução da estrutura de gerenciamento de riscos.

2. Diretores, Líderes e Gestores Diretos

   Responsabilidades dos Diretores, Líderes e Gestores:

   - Aprovar os tratamentos de riscos altos, médios e baixos;
   - Assegurar a implementação de controles internos para identificação e tratamento dos riscos;
   - Comunicar a identificação e a evolução do tratamento dos riscos;

- Acompanhar a evolução da estrutura de gerenciamento de riscos dentro de suas áreas, processos, práticas, produtos e negócios.

## 7.Referências

- Contrato Social
- Código de Conduta
- COSO – ERM: Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management Framework

# POLÍTICA DE PREVENÇÃO À LAVAGEM DE DINHEIRO



## 1.Introdução

A presente Política de Prevenção e Combate à Lavagem de Dinheiro e ao Financiamento do Terrorismo ("Política") do RIBUS TECNOLOGIA visa a promover a adequação das atividades operacionais da Empresa com as normas pertinentes aos crimes de lavagem de dinheiro e financiamento do terrorismo ("LDFT").

Todos os estagiários, funcionários, prestadores de serviços, exchanges e sócios devem adotar as melhores práticas no cadastramento de clientes e dedicar especial atenção aos conceitos e atividades que auxiliam na prevenção e combate à LDFT. As leis e regulamentos atrelados a este delito, bem como as regras desta Política devem ser obrigatoriamente cumpridas.

A Política identificará o conceito de lavagem de dinheiro, as etapas que configuram o delito e as características de pessoas e produtos suscetíveis a envolvimento com este crime.

Além disso, serão tipificadas as operações de lavagem de dinheiro, identificados os controles utilizados pelo RIBUS TECNOLOGIA e definidas as regras para aplicação dos formulários "Conheça seu cliente". O conhecimento de algum indício de lavagem de dinheiro deverá ser comunicado ao departamento de Controles Internos e Compliance("Compliance"), sendo este responsável por averiguar as informações reportadas e, caso aplicável, comunicar aos órgãos reguladores.

O Compliance será igualmente responsável por disponibilizar aos colaboradores da RIBUS TECNOLOGIA, treinamentos e palestras que promovam a conscientização sobre o crime de lavagem de dinheiro e desenvolver campanhas/atividades que auxiliem na detecção de operações que caracterizem indícios deste crime.

## 2.Conceitos

- Definição:

A expressão “lavagem de dinheiro” consiste na realização de operações comerciais ou financeiras com a finalidade de incorporar recursos, bens e serviços obtidos ilicitamente.

- Etapas do crime e lavagem de dinheiro:

O processo de lavagem de dinheiro envolve três etapas, são elas: colocação, ocultação e integração. A colocação é a etapa em que o criminoso introduz o dinheiro obtido ilicitamente no sistema econômico mediante depósitos, compra de instrumentos negociáveis ou compra de bens. Trata da remoção do dinheiro do local que foi ilegalmente adquirido e sua inclusão, por exemplo, ao mercado financeiro.

A ocultação é o momento que o agente realiza transações suspeitas e caracterizadoras do crime de lavagem. Nesta fase, diversas transações complexas se configuram para desassociar a fonte ilegal do dinheiro.

Na integração, o recurso ilegal integra definitivamente o sistema econômico e financeiro. A partir deste momento, o dinheiro recebe aparência lícita.

## 3.Normas Reguladoras

As atividades desenvolvidas pelo RIBUS TECNOLOGIA não se encontram reguladas, deforma direta e específica. Entretanto, para fins de prevenção e combate à lavagem de3 dinheiro, pode-se aproveitar dispositivos presentes em normas disciplinadoras do mercado financeiro, dentre as quais vale mencionar:

- Lei no 9613/98 - Dispõe sobre os crimes de “lavagem” ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os respectivos ilícitos e cria o COAF - Conselho de Controle de AtividadesFinanceiras;

- Instrução CVM n. 617/19 - Dispõe sobre a identificação, o cadastro, o registro, as operações, a comunicação, os limites e a responsabilidade administrativa referente aos crimes de lavagem de dinheiro e financiamento do terrorismo;

- BACEN Circular n. 3.978/20 - Dispõe sobre os procedimentos a serem adotados na prevenção e combate às atividades relacionadas com os crimes previstos naLei no 9.613/98; e

- Normas emitidas pelo COAF – Conselho de Controle de Atividades Financeiras.

Em 2012, a Lei no 9.613 foi alterada pela Lei no 12.683 que trouxe importantes avanços para a prevenção e combate à lavagem de dinheiro, tais como:

1. a extinção do rol taxativo de crimes antecedentes, admitindo-se agora como crime antecedente da lavagem de dinheiro qualquer infração penal;

2. a inclusão das hipóteses de alienação antecipada e outras medidas assecuratórias que garantam que os bens não sofram desvalorização ou deterioração;

3. inclusão de novos sujeitos obrigados tais como cartórios, profissionais que exerçam atividades de assessoria ou consultoria financeira, representantes de atletas e artistas, feiras, dentre outros;

4. aumento do valor máximo da multa para R$ 20 milhões.

## 4.Cadastro de Clientes

O cadastro de clientes é elemento essencial na prevenção e combate ao crime deLDFT, o que torna indispensável o cumprimento de todos os preceitos contidos na Política de Regras e Procedimentos do departamento de Cadastro (“Cadastro").

A ficha cadastral do RIBUS TECNOLOGIA é clara, objetiva e segregada em pessoas físicas e jurídicas. Toda a documentação deve ser cuidadosamente analisada para fins de confirmação do cadastro.

Considerando as principais diretrizes e regras existentes no mercado financeiro e de negociação de criptoativos, bem como, a análise dos principais casos de lavagem de

dinheiro, é possível relacionar as pessoas mais sensíveis de envolvimento com o crime de lavagem de dinheiro. Estas devem ser classificadas como de Alta Sensibilidade.

Todos os colaboradores do RIBUS TECNOLOGIA devem dedicar atenção aos clientes classificados como politicamente expostos ou “suspeitos”.

1. Pessoas Politicamente Expostas.

   Em conformidade com as normas em vigor, o RIBUS TECNOLOGIA e seus colaboradores devem dedicar especial atenção às pessoas politicamente expostas.

   São consideradas politicamente expostas aquelas pessoas que desempenham ou tenham desempenhado, nos últimos 5 (cinco) anos, cargos, empregos ou funções públicas relevantes, no Brasil ou em outros países, territórios e dependências estrangeiros, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

   Além disso, são exemplos de situações que caracterizam relacionamento próximo e acarretam o enquadramento de cliente permanente como pessoa politicamente exposta:

   - Constituição de pessoa politicamente exposta como procurador ou preposto;
   - Controle, direto ou indireto, cliente pessoa jurídica por pessoa politicamente exposta;

   Todo cliente da RIBUS TECNOLOGIA é obrigado a se autodeclarar como pessoa politicamente exposta, no momento do cadastramento. Além disso, o sistema de prevenção à lavagem de dinheiro contratado pela Empresa confronta a sua base de clientes com uma lista de pessoas politicamente expostas. Assim, caso um cliente que seja identificado como politicamente exposto, ainda que não se tenha autodeclarado, será assim considerado nas análises de indícios de lavagem de dinheiro.
   Todos os clientes politicamente expostos são definidos pelo sistema como de alto risco de envolvimento com ilícitos associados a lavagem de dinheiro. O Compliance analisa os dados da ocorrência e, caso aplicável, solicita os esclarecimentos necessários ao assessor responsável ou ao próprio cliente sobre

suas operações. Caso os indícios sejam consistentes, o Compliance é responsável por comunicar aos órgãos reguladores, respeitando o fluxo operacional conforme trataremos neste documento.

2. Pessoas "Suspeitas".

   Os estagiários, funcionários, prestadores de serviços, incluindo os agentes autônomos e sócios devem ter atenção com pessoas classificadas como “suspeitas”.
   Segundo parâmetros aplicados no mercado financeiro, as pessoas que trabalham nos setores turismo, jogos, transporte aéreo, companhias de seguros, casas de câmbio, distribuidoras, factoring, entre outros, são mais suscetíveis de envolvimento intencional(ou não) em crimes de lavagem de dinheiro. Cabe destacar que pessoas residentes em locais fronteiriços devem ser igualmente identificadas como de alta suscetibilidade para a participação em atividades atreladas àLDFT.

   Por sua vez, o RIBUS TECNOLOGIA igualmente dedica atenção especial aos clientes maiores de 70 (setenta) e menores de 18 (dezoito) anos e aos clientes que, no momento do cadastramento, indicarem procurador/representante.

   Por fim, podem ser caracterizados como clientes “suspeitos”, as pessoas físicas ou jurídicas já envolvidas com crime de lavagem ou que receberam qualquer tipo de publicidade negativa. Para fins de controle, o Compliance desenvolve uma lista interna contendo os dados de pessoas divulgadas pela mídia ou pelos órgãos reguladores que tenham relação direta ou indiretamente com o crime de lavagem de dinheiro.

3. Conheça Seu Cliente (Know Your Client).

   A aplicação da política “Conheça seu cliente” é mais uma das formas utilizadas pelaEmpresa na prevenção e combate ao crime de lavagem de dinheiro. A identificação do perfil dos clientes e informações precisas sobre a atuação profissional, ramo da atividade e a situação financeira patrimonial dos clientes protege a reputação daEmpresa e afasta a possibilidade de sanções administrativas ou perdas financeiras.

Os formulários de “Conheça seu cliente” devem ser aplicados aos clientes pessoas físicas e jurídicas. Todos os campos devem ser preenchidos com seriedade e clareza, permitindo a exata definição do perfil do cliente.

Sempre que necessário, os responsáveis pelo preenchimento dos formulários devem realizar visitas aos clientes e, quando aplicável, aos seus estabelecimentos comerciais.Tais visitas podem ser periodicamente refeitas e visitas especiais deverão ser efetuadas em qualquer situação de anormalidade ou mudança no comportamento operacional do cliente.

O respectivo formulário é disponibilizado aos clientes no ato do cadastramento dos dados para a abertura de conta, ou seja, antes do início de suas operações. O preenchimento do formulário poderá ser solicitado pelo Compliance quando este entender necessário o preenchimento e/ou atualização dos respectivos dados.
O formulário “Conheça seu Cliente” será arquivado eletronicamente, quando assim preenchido, ou fisicamente junto ao dossiê cadastral do cliente.

## 5.Conheça Seu Funcionário (Know Your Employee)

A RIBUS TECNOLOGIA adota postura rígida e transparente na contratação de seus colaboradores. Antes do ingresso na Empresa, todos os candidatos devem ser entrevistados pelo departamento de Recrutamento e pela Diretoria (quando aplicável). Requisitos ligados à reputação no mercado e perfil serão avaliados, bem como os antecedentes profissionais do candidato.

Além destes procedimentos, a Empresa promove treinamentos periódicos sobre os conceitos de seu Código de Conduta e da presente Política, possibilitando o conhecimento de seus colaboradores acerca de atividades vedadas e dos princípios da instituição.

Cabe destacar que a RIBUS TECNOLOGIA supervisiona constantemente as condutas profissionais e pessoais de seus colaboradores e quaisquer descumprimentos aos princípios éticos da Instituição são severamente repreendidos.

## 6.Indícios de Lavagem de Dinheiro

Em conformidade com o estipulado na regulamentação anteriormente citada, é de sumaimportância que todos os estagiários, funcionários, prestadores de serviços, agentesautônomos e sócios tenham conhecimento das operações que configuram indícios delavagem de dinheiro. São considerados indícios de lavagem de dinheiro, as operações:

- cujos valores se afigurem objetivamente incompatíveis com a ocupação profissional e a situação financeira patrimonial declarada;
- realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas no que se refere a algum dos envolvidos;
- evidenciem oscilação significativa em relação ao volume e/ou freqüência de negócios de qualquer das partes envolvidas;
- cujas características e/ou desdobramentos evidenciem atuação, de forma contumaz, em nome de terceiros;
- que evidenciem mudança repentina e objetivamente injustificada relativamente às modalidades operacionais usualmente utilizadas pelo(s) envolvido(s);
- realizadas com finalidade de gerar perda ou ganho para as quais falte, objetivamente, fundamento econômico; e
- cujo grau de complexidade e risco se afigurem incompatíveis com a qualificação técnica do cliente ou de seu representante.

Podem ser também configuradas como indícios de lavagem de dinheiro, as seguintes práticas:

- criar resistência em facilitar as informações necessárias para a de conta;
- declarar diversas contas bancárias e/ou modificá-las com habitualidade; e
- abrir conta e autorizar procurador que não apresente vínculo aparente.

Todos os estagiários, funcionários, prestadores de serviços, agentes autônomos e sócios devem, obrigatoriamente, reportar os casos de suspeita de lavagem de dinheiro ao

Compliance que será responsável por respeitar o sigilo do reporte e proporcionar a devida averiguação dos fatos.

## 7.Identificação e Tratamento de Indícios de Lavagem de Dinheiro

O departamento de Fraudes é o responsável pelas rotinas de monitoramento das operações para identificação de indícios de lavagem de dinheiro. As rotinas visam a identificar operações com reincidência de contraparte, transferências injustificadas ou atípicas, operações com incompatibilidade patrimonial, não limitadamente.

O sistema de prevenção à lavagem de dinheiro gerará ocorrências relacionadas às operações dos clientes. Um cliente cujas operações sejam atípicas será sinalizado pelo sistema que informará também outras informações deste cliente tais como:

- se é pessoa politicamente exposta;
- se fez mudança atípica de endereço ou titularidade de conta bancária ou procurador;
- se reside/possui conta/procurador em locais de fronteira.

Uma vez gerada a ocorrência, caberá ao Compliance analisar mais profundamente o cliente para confirmar ou não a suspeita de indícios de lavagem de dinheiro. A análise consistirá na verificação de documentos, movimentações e dados confrontados pelo respectivo sistema.

Diversas são as providências possíveis, dentre elas: a exigência de atualização cadastral, um pedido de esclarecimentos ao assessor, comercial do cliente ou ao próprio cliente, análise do departamento de Risco face inconsistências de movimentação ou o próprio arquivamento da ocorrência. Cada uma será utilizada de acordo com o caso em questão.

Se após as demais análises a suspeita se confirmar, o Compliance deverá registrar tais análises em sistema no histórico do cliente e preparar a comunicação formal ao COAF.O Comitê de PLD será envolvido para deliberar pela comunicação ao não ao COAF.Isso ocorre sempre que o procedimento específico da respectiva rotina do Compliance exigir.

## 8.Comitê de Prevenção e Combate à Lavagem de Dinheiro

O Comitê de Prevenção e Combate à Lavagem de Dinheiro e Financiamento doTerrorismo será composto pelos Diretores responsáveis pelas áreas de Compliance, Fraudes e Operações e deliberará sobre a política, treinamentos e ações diversas relacionadas à lavagem de dinheiro. Tais deliberações poderão ocorrer em reuniões presenciais ou eletrônicas (e-mail ou outros dispositivos aplicáveis).

## 9.Treinamentos

O Compliance deve proporcionar a todos os estagiários, funcionários, prestadores de serviços, agentes autônomos e sócios treinamentos que visem revisar os conceitos contidos nesta Política e incentivar a adoção das medidas cabíveis frente aos casos de suspeita de lavagem de dinheiro.

A Empresa exige que, no momento da contratação, todo colaborador realize um treinamento interno. Este treinamento tem por objetivo reforçar a importância ao combate do crime de lavagem de dinheiro e desenvolver atividades que auxiliem na detecção de operações que caracterizem indícios deste crime.

O respectivo treinamento é composto por uma parte conceitual e por outra dedicada à avaliação dos conhecimentos adquiridos. Para aprovação, os colaboradores devem obter no mínimo, 70% (setenta por cento) de acertos, caso contrário será exigido uma nova realização do treinamento.

Anualmente, o Compliance revisa os materiais e promove programas de reciclagem.