MRB INTERMEDIAÇÃO E NEGÓCIOS DIGITAIS	**Política de Know Your Client (KYC)**	Código:	POL-RC-003
		Nº Versão:	1.0

Categoria:	Riscos e Compliance	
Classificação:	Última publicação:	Próxima revisão:
Público	02/04/2024	30/03/2025

SUMARIO

1. TERMOS E DEFINIÇÕES

- **Alta Administração** – Sócios e executivos de alto escalão responsáveis por definir estratégias, tomar decisões cruciais e direcionar o rumo geral da organização.
- **API** – *Interface de Programação de Aplicações* – é um conjunto de regras e protocolos que permite a comunicação entre diferentes softwares, possibilitando que aplicativos e sistemas interajam entre si de forma padronizada e segura.
- **Avaliação Interna de Riscos (AIR)** – Nos termos da Circular BCB nº 3.978/2020.
- **Background check** – Processo de verificação de informações básicas e antecedentes de uma pessoa ou entidade, geralmente focado em histórico criminal, emprego e educação, visando confirmar a veracidade das informações fornecidas. Mais simplificado e superficial que o *due diligence*, mais voltado a verificar veracidade de informações prestadas previamente.
- **BACEN ou BCB** – Banco Central do Brasil.
- **Cliente** – Pessoa jurídica devidamente qualificada para adquirir produtos ou serviços oferecidos pela MRB.
- **Colaboradores** – Indivíduos que trabalham para a organização, incluindo funcionários em tempo integral, meio período, temporários, contratados, terceirizados e freelancers, inclusive estagiários e jovens aprendizes.
- **Comissão de Valores Mobiliários (CVM)** – Órgão regulador do mercado de capitais no Brasil, responsável por regulamentar e fiscalizar empresas e profissionais atuantes nesse mercado, visando proteger investidores e garantir a integridade do mercado.
- **Conselho de Controle de Atividades Financeira (COAF) –** Unidade de inteligência financeira brasileira, criada pela Lei 9.613/98, responsável por combater crimes de lavagem de dinheiro, determinando políticas e diretrizes para prevenir atividades ilícitas no sistema financeiro.
- **Diretoria da Instituição** – Sócia-Administradora ou Diretor designado para representar a Alta Administração.
- **Due diligence** – Investigação abrangente e detalhada de todos os aspectos relevantes de uma pessoa, empresa ou negócio, envolvendo análise financeira, legal, regulatória e operacional, com o objetivo de identificar riscos, oportunidades e questões críticas antes de tomar decisões estratégicas ou financeiras.
- **Fraude** – Quaisquer atos ilegais ou ilegítimos caracterizados por engano malicioso, dissimulação ou violação da verdade, independentemente da aplicação de ameaça, de violência ou de força física. São perpetradas por indivíduos e/ou organizações para obtenção de dinheiro, bens ou serviços; evitar o pagamento ou perda de serviços; assegurar vantagem pessoal ou nos negócios.
- **Instituição de Pagamento** – Pessoa jurídica que viabiliza serviços de compra e venda e de movimentação de recursos, no âmbito de um arranjo de pagamento, sem a possibilidade de conceder empréstimos e financiamentos a seus clientes, e que tenham, como atividade principal ou acessória, alternativa ou cumulativamente, as opções listadas no art. 6º, inciso III, da Lei nº 12.865 de 09 de outubro de 2013. Não compõem o SFN, mas são reguladas e fiscalizadas pelo BC, conforme diretrizes estabelecidas pelo CMN.
- **Know Your Client (KYC)** – "Conheça seu Cliente" – regras e procedimentos institucionais adotados para identificar e mitigar riscos relacionados a clientes, durante seu credenciamento e em momento posterior, visando ao conhecimento de suas atividades e ao monitoramento eficaz de suas operações para prevenir que a estrutura e/ou produtos da MRB sejam utilizados como instrumentos para a prática de ilícitos.
- **LD / FT** – Lavagem de dinheiro / Financiamento ao terrorismo.
- **LGPD** – Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).
- **MRB** – MRB INTERMEDIACAO E NEGOCIOS DIGITAIS LTDA, inscrita no CNPJ sob o nº 38.354.463/0001-24.
- **Office of Foreign Assets Control (OFAC)** – Agência de inteligência financeira do Departamento do Tesouro dos Estados Unidos da América que monitora e atualiza a lista de pessoas e empresas proibidas de realizar negócios com o governo norte-americano e empresas que têm negócios no território americano, com alcance extraterritorial.
- **Oportunidades de melhoria** – Áreas ou processos que podem ser aprimorados para aumentar eficiência, qualidade ou resultados.

- **Pessoa Exposta Politicamente (PEP)** – É todo agente público com exposição pública ou pessoa de seu relacionamento próximo, considerando a verificação dessa condição nos termos do art. 27, bem como da condição de representante, familiar ou estreito colaborador dessas pessoas nos termos do art. 19, ambos da Circular nº 3978/2020 do BCB.
- **PLD/CFT** – Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo.
- **Proponente** – Pessoa jurídica que está demonstrando interesse em se tornar cliente da MRB, seja através de uma proposta de negócio formal, seja por meio de uma comunicação informal de interesse.
- **Riscos e Compliance** – Área responsável por pela governança, implementação e monitoramento do programa de PLD/CFT da MRB, gestão de riscos e conformidade regulatória.
- **Sistema Financeiro Nacional (SFN)** – Rede de instituições públicas e privadas responsável por fiscalizar e fazer a regulação das operações do mercado financeiro no Brasil.
- **Sistema de Pagamentos Brasileiro (SPB)** – Sistema gerido pelo Banco Central do Brasil (BCB) para permitir a realização de operações e a transferência de recursos financeiros em território nacional, tanto em reais quanto em moeda estrangeira. É composto por dois segmentos: Infraestruturas do Mercado Financeiro (IMF) e Arranjos de Pagamento.

2. INTRODUÇÃO

A *Política de Know Your Client (KYC)* (ou "Conheça Seu Cliente") estabelece um conjunto de procedimentos e controles rigorosos adotados pelas instituições de pagamentos para conhecer os respectivos Clientes, com a adoção de diligência prévia e periódica que assegure sua identificação, qualificação e classificação, prevenindo a ocorrência de Lavagem de Dinheiro e Financiamento do Terrorismo. Isso permite entender a natureza de suas atividades e avaliar os riscos associados a elas.

As práticas exigem a manutenção de registros precisos e atualizados, a realização de *due diligence* periódica e a comunicação proativa com as autoridades regulatórias em caso de descoberta de atividades suspeitas.

Deste modo, esta Política não apenas fortalece a segurança financeira, mas também promove a transparência e a confiança entre a instituição e seus clientes.

3. OBJETIVO

Por meio desta Política, a MRB objetiva:

- Adotar procedimentos que permitem identificar e validar a identidade e a idoneidade do cliente, incluindo a obtenção, a verificação e a validação da autenticidade de informações de sua identificação, mediante confrontação dessas informações com as listas disponíveis em bancos de dados de caráter público e/ou privado, quando necessário, e de acordo com a categoria de risco do cliente.
- Estabelecer disposições e regramentos específicos destinados à adoção de diligência prévia e periódica que assegure sua identificação, qualificação e classificação para conhecimento dos clientes, prevenindo a ocorrência de LD/FT.

4. ABRANGÊNCIA

Esta Política aplica-se a todos da MRB, incluindo gestores, investidores, colaboradores, estagiários, prestadores de serviço, consultores e demais pessoas físicas ou jurídicas que utilizam ou suportam os negócios da Instituição de Pagamento.

5. REFERÊNCIAS NORMATIVAS

- **Lei nº 9.613, de 3 de março de 1998** – Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei.
- **Lei nº 13.260, de 16 de março de 2016** – Regulamenta o inciso XLIII do art. 5º da CF, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista.
- **Lei n° 13.709 de 14 de agosto de 2018** (e alterações) – Lei Geral de Proteção de Dados Pessoais (LGPD).
- **Circular n° 3.978 de 23/1/2020** – Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613/1998, e de financiamento do terrorismo, previsto na Lei nº 13.260/ 2016.
- **Resolução Coaf nº 40, de 22 de novembro de 2021** – Dispõe sobre procedimentos a serem observados, em relação a pessoas expostas politicamente, por aqueles que se sujeitam à supervisão do Conselho de Controle de Atividades Financeiras (COAF).
- **Resolução Conjunta n° 6 de 23/5/2023** – Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Bacen.
- **Resolução BCB n° 343 de 4/10/2023** – Dispõe sobre as medidas necessárias à execução do compartilhamento de dados e informações sobre indícios de fraudes de que trata a Resolução Conjunta nº 6, de 23 de maio de 2023.
- **Lei 14.790/23 de 29 de dezembro de 2023** – Permite que empresas privadas operem apostas esportivas online e em estabelecimentos físicos, como casas de apostas e cassinos.
- **Política de Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (PLD/CFT)** da MRB.
- **Política de Gestão de Riscos** da MRB.

As leis e normas são citadas de forma exemplificativa, e não esgotam toda a legislação aplicável às atividades da MRB.

5.1. Aplicabilidade

Caso venha a solicitar autorização de funcionamento ao Banco Central para a modalidade de "Instituição de Pagamento", nos termos da Lei nº 12.865 de 09 de outubro de 2013 e da Resolução BCB nº 80/2021, a MRB providenciará o necessário para o cumprimento da Resolução Conjunta n° 6 de 23/5/2023 e da Resolução BCB n° 343 de 4/10/2023, relacionadas ao compartilhamento de dados e informações sobre indícios de fraudes.

6. DISPOSIÇÕES GERAIS

- Os procedimentos de KYC devem ser formalizados em manuais específicos e ser compatíveis com:
  a) O perfil de risco do cliente, contemplando medidas reforçadas para clientes classificados em categorias de maior risco;
  b) A Política de PLD/CFT[1];

[1] Especial atenção para os itens *"Due diligence"* e *"Procedimento de Comunicação ao COAF"*, quando aplicáveis, bem como as diretrizes previstas em *"Know Your Client (KYC)"* e seus subitens.

c) Avaliação Interna de Risco (AIR)[2]

- Os procedimentos de KYC devem observar a LGPD, adotando medidas robustas de segurança para proteger informações sensíveis coletadas de proponentes/clientes contra acessos não autorizados ou violações de privacidade.
- As informações obtidas e utilizadas nos procedimentos de KYC devem ser armazenadas em sistemas informatizados e utilizadas nos procedimentos de monitoramento, seleção e análise de operações e situações suspeitas. Para tanto, devem ser atendidos os parâmetros e melhores práticas de Segurança da Informação, estabelecidos pela área responsável.
- Esta política deve ser compreendida em conjunto com outras políticas institucionais pertinentes, e seu conteúdo não substitui nem prevalece sobre qualquer instrumento legal.

7. PAPEIS E RESPONSABILIDADES

Os procedimentos de KYC exigem uma verificação rigorosa da identidade e histórico dos clientes, e é essencial que cada função dentro da instituição financeira compreenda claramente suas responsabilidades neste processo.

Sem uma definição clara de papéis e responsabilidades, a MRB corre o risco de falhar nos processos, o que pode resultar em violações regulatórias, multas significativas e danos à reputação da empresa. Portanto, é fundamental que cada área e membro compreendam sua função específica no cumprimento desta Política.

7.1. Alta Administração

- Assegurar a adesão institucional às boas práticas de cadastramento, KYC e PLD/CFT, ao cumprimento das leis e das normas vigentes relacionadas.
- Aprovar a elaboração, revisão e alterações da presente Política, para posterior publicação.

7.2. Riscos e Compliance

- Verificar da adequação dos dados cadastrais dos clientes da instituição, orientando a gestão responsável pelo Cadastro sobre necessidades de correções e oportunidades de melhoria nos processos de cadastramento, a fim de prevenir a utilização da estrutura da instituição para crimes de LD/FT.
- Realizar a verificação da adequação dos dados cadastrais dos clientes da instituição.
- Reportar à área responsável pelo Cadastro, necessidade de correções e implementação de melhores práticas de cadastramento.
- Dar suporte à área de Cadastro para melhores práticas no manejo de informações e documentações de proponentes e clientes.
- Gerir ferramentas e estabelecimento de processos relacionados a *background check* e *due diligence*.
- Assegurar a conformidade das áreas de negócio e de todos os procedimentos internos da MRB.
- Criar e coordenar a comunicação e treinamento dos Administradores e Colaboradores.
- Assegurar o cumprimento dos mecanismos de atuação do Canal de Denúncia.
- Monitorar as ocorrências sobre Transações atípicas ou suspeitas identificadas pelas ferramentas tecnológicas da MRB ou que sejam comunicadas pelos Colaboradores.
- Enquadramento e monitoramento de PEP, quando houver necessidade.
- Comunicação com o COAF e com o Bacen, além de atendimento de auditorias e demais órgãos de fiscalização e autoridades competentes.
- Promover comunicação efetiva da Política, nos canais institucionais e por meio de treinamentos.

[2] Item 13 da *Política de Gestão de Riscos* e item 9 da *Política de PLD/CFT*.

- Verificar eventual atualização, revogação e a edição de novas normas.
- Realizar a revisão periódica da Política.
- Analisar casos omissos ou exceções ao estabelecido nesta Política (via Diretoria, conforme item 13).

7.3. Comercial / Marketing

- Dar suporte à área de Cadastro e à área de *Riscos e Compliance*, com informações e documentos adequados e necessários a respeito de pretensos clientes e suas operações.
- Cumprir os procedimentos estabelecidos pela MRB para KYC.
- Procurar a área de *Riscos e Compliance* em caso de dúvidas de procedimento, inseguranças em relação a clientes e documentos, bem como suspeitas e casos de denúncia de que tiver conhecimento.

7.4. Cadastro

- Coletar, registrar, analisar e validar informações e documentos de identificação de clientes com os quais a MRB mantém relacionamento.
- Reportar dificuldades, vulnerabilidades e oportunidades de melhoria para a TI/SI, relacionadas aos sistemas de cadastramento da MRB.
- Estabelecer revisão periódica dos clientes cadastrados.
- Gerir o cadastro de clientes ativos, inativos, suspensos e demais status de classificação padronizados pela MRB.

7.5. Financeiro / Operações

- Implementar controles de PLD/CFT relacionados ao comportamento do cliente para reportar internamente operações suspeitas.
- Implementar processos necessários em caso de bloqueio, restrições, bem como demais situações necessárias conforme disposições legais e orientações da área de *Riscos e Compliance*.

7.6. Tecnologia da Informação / Segurança da Informação

- Assegurar que sistemas informatizados e utilizados nos procedimentos de monitoramento, seleção e análise de operações e situações suspeitas, estejam disponíveis e garantam informações confiáveis e integrais.
- Promover melhorias na infraestrutura que suporta os cadastramentos de clientes.
- Estabelecer parâmetros e melhores práticas de Segurança da Informação para produtos, serviços e operações da MRB.
- Garantir que sejam obedecidas integralmente as determinações de restrições de acesso a sistemas, aprovações de processos eletrônicos, alterações de parametrizações de regras em sistemas e outras, que estejam formalizada, implementando Gestão de Acessos baseada em funções, Política de Segurança da Informação e demais normativos e procedimentos internos necessários.
- Testar os controles relacionados à segurança cibernética para prevenção a fraudes;
- Atuar com diligência na proteção e sigilo dos dados e para manutenção das ferramentas tecnológicas e infraestrutura da MRB.
- Acompanhar e gerir a segurança de todas as aplicações, sistemas, comunicação com fornecedores e estruturas de tecnologia da MRB a fim de mitigar qualquer risco de manipulação, cyber ataque ou exploração de vulnerabilidades sistêmicas;
- Garantir que sejam implementados múltiplos fatores de autenticação e demais práticas que sirvam para assegurar o controle de acessos os ativos e informações da empresa.
- Gestão de fornecedores de Tecnologia da Informação e Segurança.

8. CLASSIFICAÇÃO DE CLIENTES

São os tipos de clientes da MRB:

8.1. Clientes Próprios

- Pessoas jurídicas brasileiras, devidamente constituídas e registradas sob CNPJ ativo e válido na Receita Federal do Brasil, com objeto social lícito e atividades lícitas, havendo relacionamento com a MRB, em caráter permanente, destinado à prestação de serviços de pagamento conforme termos, políticas e dispositivos legais.

8.2. Usuários (transitórios)

- Indivíduos que não são clientes da MRB, mas das empresas que a contrataram para processar pagamentos. O cadastro desse usuário é feito com informações mínimas e de forma automatizada, com relacionamento meramente operacional e de controle.
- O *due diligence* do usuário é realizado pela empresa cliente em seu ambiente.
- O usuário fica sujeito aos controles internos de PLD/CFT da MRB e aos limites operacionais estabelecidos.
- A MRB estabelecerá mecanismo de comunicação com as empresas clientes para reportar atividades suspeitas ou anômalas desses usuários, ou ainda, informar bloqueios e suspensões, quando aplicados.

9. PROCEDIMENTOS DE KYC

A MRB possui abordagens de KYC prioritariamente eletrônicas, por meio de uso de sistemas, a fim de conferir impessoalidade e registro das averiguações. São os procedimentos:

i. Cadastro;
ii. *Due diligence*;
iii. Definição e monitoramento de limites operacionais.

9.1. Cadastro

- Na ***Política de Cadastro*** da MRB, podem ser consultados:
  - Diretrizes e o detalhamento das regras de cadastramento de clientes;
  - Status dos clientes (qualificação).
- De acordo com o objetivo da abertura da conta, a área Comercial e de Cadastro deverão providenciar as informações do cliente para preenchimento da *Ficha Cadastral* no sistema. Para tanto, serão captadas, minimamente, as seguintes informações do cliente:
  a) Cartão CNPJ;
  b) Contrato Social;
  c) Documentos pessoais dos Sócios (RG, CPF, comprovante de endereço atualizado);
  d) Identificação do Sócio-Administrador;
  e) Faturamento (informações financeiras como Balanço Patrimonial, Demonstração de Resultado do Exercício, Projeção de Faturamento);
  f) E-mail para cadastramento;
  g) Número de celular para cadastramento;
  h) Pontos focais (pessoas-chave para contato nas operações).
- Caso o Cliente desenvolva atividade empresária ou profissional em estabelecimento físico, a MRB ou um Parceiro Comercial (caso aplicável) poderá, de forma física ou remota (inclusive utilizando de tecnologias de geolocalização), verificar a efetiva existência do estabelecimento no local indicado.

9.2. Consultas de dados e *due diligence*

9.2.1. Coletas de dados e informações

Para fins de *due diligence* e cruzamento de informações, os clientes (e seus representantes legais) terão seus dados e informações consultados em bancos de dados públicos e privados e listas de sanções e restrições, verificando-se, por exemplo:

- Regra de validação de Pessoa Politicamente Exposta (Verifica se uma pessoa é considerada PEP);
- Indivíduos na lista de SDN[3] da OFAC;
- Nome na Receita Federal (regularidade do CPF);
- Registro de óbito na Receita Federal (não deve constar registro de óbito na Receita Federal);
- Data de Nascimento na Receita Federal (data de Nascimento deve ser igual ao cadastrado na Receita Federal);
- Situação Cadastral Regular (Situação cadastral do CPF deve ser REGULAR);
- Antecedentes Criminais (não devem constar antecedentes criminais);
- Mandados de Prisão com Homônimos (verifica a existência de mandados de prisão para o nome buscado, utilizando nome da mãe e data de nascimento para ajudar na desambiguação de homônimos);
- Consulta do cadastro da empresa na Receita Federal (razão social, objeto social, quadro societário, status da pessoa jurídica (ativa, inativa, baixada, suspensa, etc.), endereço comercial, atualização cadastral, dados de contato);
- Análise do Contrato Social ou Estatuto;
- São verificados processos junto aos tribunais e mídias desabonadoras.

9.2.2. Ferramentas de verificação auxiliar

Poderão ser utilizados como auxílio no processo de *due diligence* da MRB:

- Sistemas de validação de identidade;
- Softwares de consulta de dados;
- Foto capturada com a foto do documento enviado.

9.2.3. Atualização de informações, prazos e retenções de dados

Tendo em vista que os procedimentos de KYC retratam um histórico e situação/condição econômico/financeira no momento, torna-se necessário manter uma atualização e complementação das informações inicialmente apresentadas pelos Clientes.

- As informações dos Clientes serão atualizadas periodicamente, por período não superior a 12 (doze) meses ou sempre que alguma das áreas envolvidas no processo (Comercial, Cadastro, Compliance, Diretoria) entenderem necessário.
- O resultado das verificações de KYC e due diligence pode alterar a qualificação do cliente, inclusive podendo inviabilizá-lo temporária ou permanentemente.
- Vide item 11 da *Política de PLD/CFT* para demais prazos e retenções de dados.

9.3. Limites Operacionais

- A MRB estabelece critérios de mitigação de riscos no credenciamento de Clientes, considerando o perfil de risco, mediante a fixação de limite máximo para a realização das transações em períodos determinados.

[3] *Specially Designated Nationals and Blocked Persons List* ("SDN List") é a lista de cidadãos especialmente designados e pessoas bloqueadas, que normalmente é conhecida como a lista da OFAC.

- Os limites operacionais e o mecanismo de monitoramento do comportamento dos clientes estão descritos na ***Política de Monitoramento e Análise de Operações e Situações Suspeitas***, em conformidade com a *Política de Prevenção de Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo (PLD/CFT)* da MRB.
    - A definição do limite operacional é estabelecida com base no exame da capacidade financeira do cliente (faturamento, considerando o perfil atual de clientes serem pessoas jurídicas), observadas a compatibilidade e a proporcionalidade do nível de risco.
    - A documentação exigida dos clientes, para fins da comprovação da capacidade financeira, terá seu tipo e forma definidos de acordo com o respectivo propósito da relação de negócio, produtos ou serviços consumidos, bem como a natureza de suas operações.
    - A alteração de limites, quando possível, considerará, entre outros fatores, a capacidade financeira da empresa cliente, demandando a apresentação de documentos complementares.

10. BLOQUEIO E RECUSA DE CLIENTES

Em relação à avaliação do cliente, a MRB não se relaciona com clientes próprios, usuários (transitórios) ou proponentes (relacionamento comercial inicial) que se enquadrem nas seguintes circunstâncias, devendo ser recusados sumariamente:

10.1. Clientes Próprios

- Circunstâncias suspeitas e/ou evidências relacionadas a práticas de corrupção, lavagem de dinheiro, financiamento de terrorismo, fraude, ocultação de informações, crimes de responsabilidade socioambiental, prática de trabalho escravo, assim como demais atividades ilícitas ou de violações de direitos;
- Se nas averiguações das listas de sanções e restrições forem constatadas ocorrências.
- Se o cliente for contra os valores da MRB ou violar suas políticas institucionais.

10.2. Usuários (transitórios)

- Circunstâncias, suspeitas e/ou evidências de irregularidades sobre clientes transitórios, sendo feito bloqueio diretamente na API.
- Poderão ser usados ferramentas e processos de *due diligence* da MRB para suporte à tomada de decisão.

Bloqueios e recusas de clientes poderão ocorrer conforme situações estabelecidas na *Política de Monitoramento e Análise de Operações e Situações Suspeitas*.

11. COMUNICAÇÃO E TREINAMENTO

- Esta Política é aplicada e amplamente divulgada pela Alta Administração, por meio da área de *Riscos e Compliance,* aos colaboradores da MRB envolvidos com: captação de clientes, comercial, cadastramento, atendimento ao cliente e ouvidoria, compliance; bem como áreas operacionais, financeiro e de atividades de controles internos.
- Poderão ser usados canais de comunicação diversos, incluindo: *site da MRB*, e-*mail de comunicação corporativa* e *link para acesso à Política.*
- Poderão ser conduzidos treinamentos corporativos periódicos (podendo aplicar processo de avaliação interna dos participantes, quando necessário).
- Deverão ser revisados, periodicamente, os normativos internos e procedimentos relacionados à KYC.
- Dúvidas sobre esta Política poderão ser dirimidas por e-mail: *compliance@mrbdigitais.com.br*

12. VIOLAÇÃO E SANÇÕES

- Eventuais descumprimentos ou suspeitas de violações às disposições desta Política deverão ser imediatamente comunicadas ao Canal de Denúncias da MRB, que irá realizar o tratamento adequado das ocorrências pelo e-mail *ouvidoria@mrbdigitais.com.br*, por meio de recebimento, análise preliminar, classificação, tratamento, monitoramento, investigação, tomada de decisão, reporte das denúncias e encerramento das ocorrências.
    - A MRB receberá e atuará nas denúncias de Administradores, Colaboradores, Fornecedores, Clientes, Parceiros de Negócio ou quaisquer terceiros, sobre atividades atípicas ou suspeitas que possam se caracterizar como indícios de crimes relacionados com a Lavagem de Dinheiro e Financiamento ao Terrorismo.
    - As denúncias serão recebidas por um profissional capacitado e com autonomia necessária, sendo garantido o anonimato e sigilo das comunicações, bem como a preservação da integridade do denunciante.
- O descumprimento da legislação aplicável, além de poder causar graves prejuízos à MRB, poderá sujeitar o(a) infrator(a) a penalidades criminais, cíveis e administrativas pelas autoridades.
    - Ademais, sujeitará o(a) colaborador(a) infrator a medidas disciplinares, com base na legislação aplicável, incluindo advertência (verbal ou formal), suspensão e sanção pecuniária, podendo, ainda, culminar na demissão por justa causa do(a) infrator (a), sem prejuízo da adoção das medidas legais cabíveis.
    - Poderão ser adotadas outras penalidades que estiverem pactuadas em contrato juridicamente válido.

13. DISPOSIÇÕES FINAIS

- Os casos omissos ou exceções ao estabelecido nesta Política ou que dependam de aprovação específica, deverão ser submetidos e formalmente avaliados pelo Diretoria responsável pela gestão de *Riscos e Compliance* da MRB.
- Decorrente do KYC será derivada a *Política de Cadastro* e a *Política de Monitoramento e Análise de Operações e Situações Suspeitas*.

14. VIGÊNCIA, REVISÃO E ALTERAÇÕES

- Esta Política entra em vigor na data da sua publicação, revogando outros dispositivos em contrário, e vigorará por tempo indeterminado.
- Será revisada e atualizada **anualmente** (ou em menor tempo, se necessário para fins de efetividade, adequação aos riscos e melhores práticas, ou conformidade legal/regulatória), pela área de *Riscos e Compliance,* e submetidas à aprovação da Alta Administração, de acordo com suas atribuições internas, com posterior publicação.

Data	Versão	Descrição	Autores
25/03/2024	1.0	Elaboração	Consultoria Externa
02/04/2024	1.0	Aprovação	Raquel Birck – Sócia-Administradora