Política de PLD/FTP

Esta política define as regras internas e os protocolos necessários para mitigar a ocorrência de atividades criminosas como Lavagem de Dinheiro (LD), Financiamento do Terrorismo e a Proliferação de Armas de Destruição em Massa (FTP), de acordo com a legislação vigente no Brasil.

A Alta Administração da BRP PAY se compromete com a efetividade e a melhoria contínua da política de PLD/FTP, aprovando-a e assegurando seu cumprimento pela firma na Política de Governança e Comprometimento da Alta Administração com a PLD/FTP (PGCA), que faz parte do nosso Programa de Compliance.

1. ESTRUTURA DE PLD/FTP E AUDITORIAS

Nossa área de PLD/FTP supervisiona, monitora e relata atividades suspeitas identificadas, como também, contratamos especialistas para realizar auditorias independentes dos processos de Prevenção à Lavagem de Dinheiro, Combate ao Financiamento do Terrorismo e a Proliferação de Armas de Destruição em Massa, assegurando conformidade regulatória e a melhoria constante das práticas implementadas.

1.1. GOVERNANÇA DA AVALIAÇÃO INTERNA DE RISCO

O processo de avaliação interna de riscos é fundamental, deve ser aprovada e registrada oficialmente pelo Diretor responsável pela Política PLD/FTP, em seguida encaminhada à ciência do Comitê de Gerenciamento de Riscos e do Conselho Administrativo (Alta Administração), bem como revisada a cada dois anos ou sempre que ocorrerem mudanças substanciais nos perfis de risco identificados.

2. CONCEITOS E LEGISLAÇÃO

Centralizamos as referências legais e normativas no nosso Programa de Compliance que norteia os principais Conceitos, Definições, Disposições, Normas disciplinadoras, Portarias, Instruções e Normativos de qualquer órgão regulador e disciplinador da legislação brasileira do mercado financeiro

e de meios eletrônicos de pagamentos brasileiro, que deve ser consultada para a continuidade da leitura deste documento. Algumas delas, especialmente no contexto desta Política de PLD/FTP, são:

- Banco Central do Brasil – BCB:
  - Circular nº 3.978/2020 e nº 4.005/2020.
  - Resoluções: nº 119/2021; nº 282/2022 e nº 344/2023.
  - Carta Circular: 4.001/2020.
- As Leis nº 9.613/98; nº 12.850/13; nº 12.864/13, nº 13.260/2016 e nº 13.810/2019.
- Conselho de Controle de Atividades Financeiras (COAF).
- Resoluções CMN.
- Recomendações do Grupo de Ação Financeira Internacional (GAFI/FATF), FCPA e UK Bribery Act.
- Estratégia nacional de combate à corrupção e a lavagem de dinheiro (ENCCLA).

3. APLICABILIDADE E ESCOPO

Esta política se aplica a:

- Todos os ECs (clientes finais);
- A própria BRP PAY e sua governança;
- Todas as operações, transações, produtos e serviços oferecidos;
- Funcionários, parceiros e prestadores de serviços terceirizados.

4. ATRIBUIÇÕES E RESPONSABILIDADES

4.1. GESTOR DE PLD/FTP

Conforme exigido pelo BACEN, indicamos formalmente um gestor responsável por PLD/FTP, cujas atribuições incluem:

I. Supervisionar a avaliação interna de riscos de lavagem de dinheiro;
II. Assegurar a implementação de controles internos eficazes para detecção de atividades suspeitas;
III. Aprovar relatórios de efetividade da política e auditorias internas.
IV. Supervisionar a comunicação de operações suspeitas ao COAF;

V. Assegurar que todas as transações sejam devidamente analisadas e reportadas, quando necessário.
VI. Assegurar que todos os funcionários recebam treinamento periódico sobre PLD/FTP;
VII. Promover cultura de prevenção e conformidade.
VIII. Monitorar listas restritivas de sanções nacionais e internacionais;
IX. Supervisionar as ferramentas utilizadas para triagem de clientes, fornecedores e parceiros comerciais.
X. Definir, aprovar e revisar periodicamente a Política de PLD/FTP;
XI. Representar a Empresa junto ao Banco Central e demais órgãos reguladores;
XII. Assegurar que os procedimentos de prevenção à lavagem de dinheiro estejam em conformidade com normativas do BACEN, COAF e padrões internacionais (GAFI).

4.2. DIRETORIA

I. Revisar e aprovar as diretrizes aplicáveis às questões de PLD e CFT, bem como todas as Políticas de KYC, KYE, KYP, KYS, dentre outras, bem como avalia as solicitações de autorização excepcionais ou de mais elevado privilégio decisório;
II. Zelar e supervisionar o cumprimento e aderências das práticas com o auxílio do Compliance e das demais áreas abrangidas neste documento;
III. Disponibilizar e viabilizar recursos para que toda a organização possa alcançar seus objetivos;

4.3. RECURSOS HUMANOS (RH)

I. Viabilizar programas de treinamento periódicos garantindo que todos os Colaboradores estejam treinados, constantemente, quanto às suas responsabilidades de acordo com as diretrizes deste documento, alertando-os em relação às sanções aplicáveis em caso de violação dessas políticas, juntamente com o Compliance;
II. Selecionar e recrutar os Colaboradores em consonância com as definições do *KYE*;

4.4. GESTORES

Devem acompanhar o desempenho e conduta dos colaboradores, participar dos treinamentos e assegurar que todos se empenhem para cumprir as diretrizes aqui definidas.

4.5. COMPLIANCE

I. Ajuda na criação, revisão, aprovação das diretrizes aplicáveis de todas as Políticas relativas ao tema, validando as atualizações da legislação vigente aplicável, assegurando a conformidade;
II. Divulga e conscientiza aos Colaboradores e Parceiros sobre as disposições deste documento e suas atualizações;
III. Informa a UIF - Unidade de Inteligência Financeira os casos considerados suspeitos, após ter passado pelo Comitê de Compliance.
IV. Participa da verificação das pessoas físicas envolvidas com as atividades da BRP PAY, constam nas listas restritivas, PEP, *Blacklist interna*, Mídia Negativa, COAF, dentre outras, mediante solicitação, bem como revisa periodicamente, podendo reprová-la, bem como deliberar sobre o desligamento de suas atividades relacionadas.
V. Garante o funcionamento do Canal de Denúncias de forma confidencial e segura para o denunciante, para relatar possíveis violações desta Política.

4.6. AUDITORIA INTERNA

Realiza auditorias regulares, sempre que necessário, gerando relatórios de conformidade com sugestões de melhorias e ações práticas.

4.7. COMITÊ DE PLD/FTP, COMPLIANCE E CONTROLES INTERNOS

É de responsabilidade do Comitê de PLD/FTP, Compliance e Controles Internos:

I. Deliberar em face da proposta de comunicação ao Conselho de Controles de Atividades Financeiras (COAF), relativo às operações realizadas ou serviços prestados que possam configurar a existência de indícios de lavagem de dinheiro e financiamento ao terrorismo.

II. Promover a adequação das atividades operacionais com as exigências legais e regulamentares, assim como aplicar as melhores práticas na análise das transações e nos procedimentos de comunicação aos órgãos competentes.

III. Validar as manutenções das normas pertinentes a essa política e assegurar o envolvimento de todas as áreas para conformidade dos termos aqui definidos e sua aplicabilidade.

O Comitê de PLD/FTP, Compliance e Controles Internos será composto de no mínimo 3 (três) e sem número máximo de membros, sendo obrigatória a presença do Gerente de PLD/FTP, Compliance e Controles Internos, bem como do Diretor Executivo responsável pelo cumprimento das obrigações previstas na Circular 3.978/20 do Banco Central do Brasil.

4.8. OPERAÇÕES

I. Analisar os Clientes, Fornecedores, Parceiros e Colaboradores, mitigando o risco aplicando as Políticas de *KYC*, *KYP*, *KYS e KYE*, solicitando ao Compliance a aplicação das suas responsabilidades quanto aos procedimentos de validação, recebendo resposta positiva ou negativa quanto a sua avaliação.

II. Manter o sistema atualizado com todas as informações e documentos da operação;

III. Monitorar e controlar o risco analisando as transações dos clientes e reportando ao Compliance caso seja identificada alguma atipicidade, validando a quantidade, frequência e perfil comportamental do(s) *chargeback* por Cliente;

4.9. TECNOLOGIA DA INFORMAÇÃO

A área de TI deve:

I. Garantir a segurança dos sistemas e da informação, protegendo os dados de toda a operação, monitorando e respondendo a qualquer incidente de segurança;

II. Implementar controles de acesso aos dados dos sistemas e atualizações de segurança;

III. Participar de treinamentos para se atualizar constantemente sobre novas tecnologias e as melhores práticas de segurança da informação;

IV. Garantir a conformidade com as normas de segurança da informação, em especial quanto ao PCI DSS.

4.10. TODOS OS FUNCIONÁRIOS

Todos os funcionários devem cumprir esta política e reportar atividades suspeitas ao setor de Compliance.

5. PESSOAS POLITICAMENTE EXPOSTAS (PEP)

Para os fins deste documento, conforme exposto na Circular nº 3.978/20, consideramos Pessoas Expostas Politicamente (PEPs) como:

"I - familiar, os parentes, na linha reta ou colateral, até o segundo grau, o cônjuge, o companheiro, a companheira, o enteado e a enteada; e

II - estreito colaborador:

a) pessoa natural conhecida por ter qualquer tipo de estreita relação com pessoa exposta politicamente, inclusive por:

1. ter participação conjunta em pessoa jurídica de direito privado;

2. figurar como mandatária, ainda que por instrumento particular da pessoa mencionada no item 1; ou

3. ter participação conjunta em arranjos sem personalidade jurídica; e

b) pessoa natural que tem o controle de pessoas jurídicas ou de arranjos sem personalidade jurídica, conhecidos por terem sido criados para o benefício de pessoa exposta politicamente."

Bem como o disposto no Art. 27 "Da Qualificação como Pessoa Exposta Politicamente" da mesma circular.

A BRP PAY deve adotar controles reforçados para clientes classificados como Pessoas Expostas Politicamente (PEPs), incluindo: (i) Verificação em listas de sanções internacionais; (ii) Monitoramento de suas transações; (iii) Solicitar a aprovação da Diretoria e do Compliance para se estabelecer negócios com PEPs e reavaliação periódica desta relação comercial; e (iv) Identificar a origem dos recursos envolvidos nas transações dos clientes, avaliando a compatibilidade das operações com o patrimônio, caso seja conhecido.

6. AMAZENAMENTO DE REGISTROS

Todos os registros de identificação, verificação e transações dos clientes, bem como dos fornecedores, parceiros e prestadores de serviços (e os contratos com eles), dentre outras informações transacionais, devem ser armazenados por no mínimo 5 anos, podendo ser estendidos para 10 anos conforme a relevância e o risco associado às transações. Essa exigência segue o disposto na Circular 3.978/2020 e outras regulamentações aplicáveis.

7. ANÁLISE PRÉVIA DE NOVOS PRODUTOS, SERVIÇOS E TECNOLOGIAS

Ocorrerá uma análise de novos produtos e tecnologias antes de introduzi-los no mercado, com a finalidade de reduzir os riscos relacionados ao tema desta política. Essas avaliações levam em conta:

a) Prévia:
   I. Como o novo produto/serviço pode influenciar o risco de LD e FT;
   II. O perfil dos clientes que visados e o risco potencial associado a eles;
   III. Aprovação do setor de Compliance sobre o risco da BRP PAY sobre o novo produto / serviço;
b) Posterior a implementação: Avaliação contínua para verificar se está funcionando adequadamente.

O cumprimento das normas regulamentares e das melhores práticas do mercado.

8. PERFIS DE LIMITES DE RISCO

A definição dos limites de risco para os EC é uma segmentação dinâmica, não sendo um valor único para todos, mas baseada na análise de risco, na avaliação do perfil comportamental padrão do segmento de atuação, no tempo e modelo de operação, dentre outros fatores.

Todas as transações atípicas geram alertas ao time de risco, que dependendo da operação, age imediatamente ou em D+1 a transação, sempre antes da liquidação dos recursos ao EC.

O sistema de monitoramento transacional possui um motor de regras para classificar automaticamente as transações atípicas, sempre que processadas as transações realizadas, baseado em alguns fatores e características, e estão definidas no Manual de MSAC.

9. PROCESSOS E PROCEDIMENTOS

9.1. MSAC – MONITORAMENTO, SELEÇÃO, ANÁLISE E COMUNICAÇÃO

Os procedimentos internos de MSAC de transações e situações suspeitas objetivando a prevenção de LD e o FT, conforme a regulação do BCB, estão definidos no "Manual de MSAC", que é parte integrante de toda a nossa política antifraude e anticorrupção.

9.2. INDISPONIBILIZAÇÃO DE BENS E ATIVOS

Em conformidade legislação brasileira, caso haja identificação de vínculo de clientes, colaboradores, parceiros ou qualquer terceiro, com o terrorismo, procederemos com a indisponibilidade de bens e ativos, que pudermos executar.

9.3. CLASSIFICAÇÃO DOS RISCOS

Os riscos identificados são examinados considerando tanto as chances de acontecer quanto o tamanho de suas consequências nos âmbitos financeiro, jurídico, de reputação e socioambiental. As categorias de risco são:

- Risco Alto: Necessita de medidas de segurança adicionais e vigilância minuciosa;
- Risco Moderado: Acompanhamento regular e avaliações adicionais conforme necessário;
- Risco Reduzido: Implementação de controles simplificados em conformidade com as normas regulamentares.

Poderemos usar como apoio para essa análise os relatórios e pesquisas de entidades públicas do Brasil, sempre que estiverem disponíveis, tais como Banco Central do Brasil e COAF e organismos internacionais.

9.4. QUALIFICAÇÃO E AVALIAÇÃO BASEADA EM RISCO – ABR

Periodicamente realizamos uma avaliação de riscos interna, a fim de identificar e qualificar as ameaças relacionadas aos crimes de lavagem de dinheiro e ao financiamento do terrorismo. Esse processo considera os seguintes perfis:

Clientes (ECs)	A BRP PAY	Operações, transações, produtos e serviços	Funcionários, parceiros e terceiros
incluindo segmento de atuação, perfil das transações e histórico financeiro e comportamental (possível envolvimento em atividades suspeitas ou presença em listas de sanções);	considerando seu modelo de negócio e área geográfica de atuação;	abrangendo modelos de negócios, segmentos operacionais, natureza, volume e frequência das transações, portifólio, canais de distribuição e a utilização de novas tecnologias	levando em conta seu envolvimento em processos críticos para a segurança financeira

As principais fases, suas as análises e ações são:

I. IDENTIFICAÇÃO: Riscos inerentes, Tecnológicos e de Fraude;
II. ANÁLISE: Grau de relevância, Probabilidade e Impacto;
III. RESPOSTA: Aceitar, Compartilhar e Evitar;
IV. CONTINGÊNCIA: Plano de Contingência.

9.5. DILIGÊNCIA CONTÍNUA E COOPERATIVA

O monitoramento constante dos Clientes Finais (ECs), e suas transações, fazem parte de um processo contínuo de avaliação de riscos, onde identifica-se mudanças de perfil, sejam no cadastro (endereço, sócios, beneficiários finais etc.) e no comportamento de uso e consumo dos nossos produtos e serviços (transacional), onde constantemente analisamos o perfil de risco, visando a prevenção a fraudes, especialmente os indícios sobre a possível atividade de lavagem de dinheiro ou financiamento ao terrorismo.

Nesse processo, descrito por esta política e suas partes integrantes, todas as transações analisadas e identificadas como suspeitas, as identificadas como ilícitos de alto impacto, identificadas como indícios de fraude, lavagem de dinheiro ou financiamento ao terrorismo, as diligenciadas para comunicação ao COAF, e outras que sejam elencadas ao bloqueio preventivo de valores, visando indisponibilizar os ativos, serão comunicadas ao Credenciador / Adquirente para deliberação conjunta das ações a serem tomadas, que podem até ensejar o encerramento do relacionamento comercial com o EC (conta, contrato etc.).

9.6. CHARGEBACK

As diretrizes estabelecidas na **Política de Gestão de Chargebacks (PGC), da Política de Gestão de Riscos (PGROL),** que incluem os riscos financeiros e operacionais, em conjunto com as definições aqui especificadas, visam orientar o gerenciamento das ocorrências e prevenção de possíveis riscos financeiros, garantindo o cumprimento regulatório vigente.

9.7. FLUXO DE VERIFICAÇÃO DAS LISTAS RESTRITIVAS

Utilizamos a plataforma ZABIT PLD para o *Screening* e a consulta nas listas de sanções e o *Background Check* é feito com base no Nome, Razão Social, CPF e/ou CNPJ. As principais listas consultadas são:

i. OFAC;
ii. EU;
iii. GOVUK;
iv. FBI;
v. INTERPOL;
vi. UNSC (CSNU);
vii. Canada *Sanctions*;
viii. *Directorate of Defense Trade Controls* (DDTC);
ix. CVM - Alerta Suspensão;
x. CVM - Penalidade Temporária;
xi. CVM - Termo Compromisso;
xii. CEAF;
xiii. CNEP;
xiv. MTE (Trabalho Escravo);
xv. CEPIM;
xvi. CEIS;
xvii. Listas do Banco Central do Brasil
xviii. Embargos do Ibama;
xix. Inidôneos TCU (Tribunal de Contas da União);
xx. Acordos de Leniência (Controladoria-Geral da União);
xxi. Processo Administrativo Disciplinar (BSM Supervisão);

xxii. Impedidos de Licitar e Contratar Banco;
xxiii. Tribunal de Contas do Estado de São Paulo;
xxiv. SEAPE-DF;
xxv. Conselho Nacional de Justiça;
xxvi. COAF,

Durante o monitoramento diário, semanal ou mensal, conforme as regras configuradas, monitoramos as seguintes listas:

Listas Padrões:

I. CSNU - Sanções impostas pelo Conselho de Segurança das Nações Unidas (Internacional);
II. OFAC - Sanções impostas pelo governo dos Estados Unidos (Internacional);
III. Regiões Fronteiriças: CEPs de regiões de fronteira do Brasil (IBGE);
IV. PEP - Pessoa politicamente exposta - arquivo enviado pelo cliente;

Listas Extras:

I. HM Treasury - Sanções impostas pelo governo do Reino Unido (Internacional);
II. EU - Sanções impostas pela União Europeia (Internacional);
III. CEIS - Cadastro nacional de Empresas Inidôneas e Suspensas;
IV. CEPIM - Cadastro de Entidades Privadas sem fins lucrativos Impedidas;
V. CNEP: Cadastro Nacional de Empresas Punidas;
VI. CEAF - Cadastro de Expulsões da Administração Federal;
VII. Trabalho escravo;

O processo ocorre em 3 fases:

1. Extração: onde diariamente são atualizadas as listas das fontes.
2. Match: comparamos o arquivo cadastral e de movimentação do EC com as bases das listas, seja por CNPJ ou CPF do EC, e da contraparte, caso tivermos os dados. A análise das regiões fronteiriças é feita pelo CEP. O código da profissão é usado para identificar as atividades de risco. Passamos nas listas internacionais e faz-se o batimento por *Match* do Nome e do *AKA* por aproximação de similaridade. Os nomes utilizados são os enviados no Arquivo Cadastral (Titular) ou Arquivos de Movimentações (Contraparte).
3. Alerta / Apontamento: para evitar duplicidade de informações, aplica-se a seguinte lógica na geração de apontamentos:

- Titulares: Quando um titular é identificado em uma determinada lista e um apontamento é gerado, novos apontamentos não são emitidos caso ele volte a aparecer na mesma lista. No entanto, se o mesmo titular for identificado em uma lista diferente, um novo apontamento é devidamente gerado.
- Contrapartes: As contrapartes seguem a mesma lógica descrita para os titulares, sendo que cada contraparte é associada a um titular específico. Caso uma mesma contraparte seja consultada em relação a outro titular, um novo apontamento será emitido.

Para facilitar a visualização, os apontamentos gerados são agrupados por titular e listados na plataforma ZABIT.

9.8. SISTEMAS E FERRAMENTAS

Para assegurar o cumprimento das obrigações de PLD/FTP, utilizamos a Plataforma Zabit para gestão 360° do nosso programa de PLDFTP. O detalhamento dos módulos e funcionalidades da plataforma, pode ser encontrado na apresentação técnica da ferramenta, onde demonstramos o monitoramento de transações e análise de risco, integração com terceiros para *screening* de ECs e Beneficiários Finais, verificação de listas restritivas e acesso aos Bureaus de informação para avaliação de riscos e qualificação de clientes.

9.9. CONHEÇA O SEU CLIENTE (MANUAL DE *KYC – KNOW YOUR CUSTOMER*)

A BRP PAY implementou processos para identificar os ECs (clientes), sejam pessoas físicas ou jurídicas, que realizam operações ou mantêm relacionamento comercial ativo, que por meio da uma análise cuidadosa, coleta, análise, classificação, qualificação, identificação e monitoramento, desde o cadastro inicial até o encerramento da relação, assegurando a constante atualização das informações. O detalhamento dos procedimentos e demais diretrizes no processo de KYC estão descritos no Manual de KYC.

PROCEDIMENTOS DE ESPECIAL ATENÇÃO “RED FLAG”

Alguns procedimentos mais rigorosos de análise e monitoramento de Clientes ou Parceiros os quais devem conter a aprovação do Comitê de PLD, Compliance e Controles Internos para início da relação de negócio ou manutenção do relacionamento com Cliente ou Parceiro já existente, são considerados como de Especial Atenção (*Red Flags*).

9.10. CONHEÇA O SEU FUNCIONÁRIO (MANUAL DE *KYE – Know Your Employee*)

Os processos de verificação e monitoramento que garantem que os funcionários e terceiros sigam as diretrizes de Prevenção à Lavagem de Dinheiro (PLD), Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa (FTP) estão definidos no Manual de KYE. Ela garante que estejam em conformidade com os padrões éticos profissionais legais para evitar fraudes e cumprir a legislação atual aplicável.

9.11. CONHEÇA O SEU PARCEIRO (MANUAL DE *KYP – Know Your Partner*)

O Manual de KYP visa orientar sobre a devida diligência que precisa ser feita no parceiro e acompanhar a sua jornada comercial, garantindo que esteja seguindo as normas regulatórias estabelecidas pela legislação, em relação à qualidade dos serviços prestados, bem como os nossos valores éticos, e no cumprimento das leis regulatórias vigentes.

9.12. CONHEÇA O SEU FORNECEDOR (MANUAL DE *KYS – Know Your Supllier*)

Para assegurar que se realize uma avaliação detalhada ao escolher e contratar seus fornecedores, garantindo que eles estejam em conformidade com as leis, praticando condutas éticas adequadas, e sem representarem ameaças aos negócios e sua continuidade, devido a prática de possíveis atividades ilegais ou violações de direitos humanos, entre outros desvios comuns de comportamento empresarial inadequado, criou-se o Manual de KYS, onde é aplicável a todos os fornecedores de produtos ou serviços, independentemente do porte ou localização.

9.13. IDENTIFICAÇÃO E CORREÇÃO DE DEFICIÊNCIAS NOS CONTROLES INTERNOS

A área de Compliance será responsável por coordenar a identificação e correção de deficiências nos controles internos, e pode envolver outras áreas para:

- Realização de auditorias regulares para verificar se os controles internos estão sendo seguidos corretamente;
- Acompanhamento constante de possíveis falhas e irregularidades;
- Implementar medidas corretivas com cronogramas estabelecidos para sua execução;
- Informar regularmente a Direção sobre como os controles estão funcionando e quais ajustes podem ser necessários, se for o caso.

10. PROIBIÇÕES

Nos manuais de KYC, KYS, KYP e KYE estão definidos os segmentos restritos, as proibições, vedações e sanções para cada caso e segmento comercial, que devem ser seguidos rigorosamente.

É terminantemente proibido o fornecimento a terceiros e aos respectivos envolvidos, informações sobre eventuais comunicações efetuadas em decorrência de indícios de lavagem de dinheiro ou financiamento ao terrorismo.

Na impossibilidade de cumprir com a devida diligência em face aos procedimentos de coleta, verificação, validação, atualização de informações cadastrais, a relação de negócio com o Cliente, Fornecedor, Parceiro ou candidato a colaborador não poderá ser estabelecida, devendo todo e qualquer tipo de operação, que tenha sido iniciada, seja descontinuada e finalizada.

11. SANÇÕES

Em decorrência de qualquer identificação de indício, ou descumprimento tácito, de lavagem de dinheiro, financiamento ao terrorismo, corrupção, suborno ou qualquer ato ilícito, será aplicado as sanções previstas no referido diploma legal, cabíveis as pessoas infratoras, dentre elas: (i) desligamento do contrato de trabalho do Colaborador; (ii) encerramento de parceria comercial com o Parceiro; (iii) descontinuidade da relação de negócios com um Fornecedor; (iv) rescisão do contrato de quaisquer terceiros contratados ou prestadores de serviço e, (v) clientes, como Estabelecimentos Comerciais, que terão suas contas bloqueadas (e bens/ativos indisponibilizados) enquanto durar o processo de apuração da fraude e o contrato de prestação de serviços rescindido, além de penalidades administrativas, criminais e até mesmo a comunicação dessas infrações aos órgãos competentes, quando aplicável.

A negligência e a falha voluntária são consideradas descumprimento das previsões desse documento e dos documentos aqui referenciados, sendo passível de aplicação de medidas disciplinares aqui previstas e nos normativos internos, código de ética, integridade e conduta, bem como outros que sejam aplicáveis.

12. DENÚNCIAS E INVESTIGAÇÃO

Nós recomendamos e incentivamos que a ocorrência de ações, comportamentos inadequados, sinais de alerta de infringências e outras situações contrárias as definições, orientações e diretrizes aqui deste documento (e suas referências), bem como procedimentos internos e legislação brasileira de conhecimento geral, que seja de conhecimento de qualquer parte envolvida, sejam imediatamente comunicadas para averiguação através do Canal de Denúncia disponível em https://brp-pay.com.br/canal-de-denuncias, onde todas serão investigadas com transparência, ética e imparcialidade, garantindo o sigilo no processo como um todo e apuração adequada, resultado em possíveis sansões e punições das partes envolvidas, conforme definidos no Programa de Compliance.

13. TREINAMENTOS

Será promovido a contínua capacitação periódica por meio de conteúdo digital, na forma de *lives*, *webinars*, estudos de caso, cursos online especializados e/ou campanhas de divulgação, onde o Compliance será responsável por eles, que podem ser periódicos com frequência mínima anual ou esporádicos. Todo o conteúdo programático previsto está disponível no Programa de Capacitação por Área, onde tem a seção específica de PLD/FTP . Os treinamentos ficam ser registrados, incluindo a lista de participantes, data e conteúdo programático, bem como quando aplicadas avaliações de aprendizado.

14. GOVERNANÇA, ATUALIZAÇÕES E VERIFICAÇÕES

O presente documento e suas respectivas atualizações estão em vigor a partir de sua apresentação, sendo certo que todos deverão tomar ciência, anuindo eletronicamente.

Realizaremos verificações periódicas em face do cumprimento das disposições deste documento, revalidando os cadastros e promovendo questionários de integridade, bem como forneceremos treinamentos sobre as práticas contidas nesta Política, e seus documentos integrantes, para garantir a efetividade. A contínua fomentação da “cultura de controle” relativo ao monitoramento, controle e denúncia de qualquer suspeita de violação das regras e normas desta Política.

Avaliações de verificação da efetividade em face do disposto nesta Política, serão realizadas no mínimo anualmente ou pontualmente sempre que houver alterações na regulação, bem como a identificação e a correção das deficiências verificadas, podendo utilizar "Multiplicadores Interno de Conhecimento".

15. CONSIDERAÇÕES DIVERSAS

É de responsabilidade de todos os envolvidos, o conhecimento amplo de suas responsabilidades, a compreensão dos termos deste documento e a busca constante para prevenir e detectar fraudes. Em casos de dúvidas ou esclarecimentos sobre o conteúdo desta Política ou em relação a algum assunto específico, a parte interessada deverá entrar em contato com o Compliance ou Ouvidora, que sempre estará com os canais de comunicação disponíveis.

Em decorrência de qualquer identificação de indícios de Lavagem de Dinheiro, Corrupção, Financiamento ao Terrorismo ou Atos Ilícitos, por parte dos Clientes, Parceiros ou Colaboradores, deverá seguir-se com o envolvimento da área de Compliance e Operacional para o bloqueio do cadastro suspeito até que o processo seja avaliado e, caso seja comprovado iniciar o processo de término do relacionamento com o investigado.

16. VERSIONAMENTO, APROVAÇÃO E VIGÊNCIA

Responsável: Diretoria de Risco, Gestor de PLD/FTP, Controles Internos, RH, TI, Jurídico e Compliance.

Versão	Criação / Alteração	Aprovação	Vigência	Descrição
1.0	maio/2025	junho/2025	junho/2026	Inicial
1.1 (atual)	setembro/2025	setembro/2025	setembro/2026	Atualização do Item "8.6."

Esta política entrou em vigor na data de sua aprovação pela Diretoria Executiva, definida acima e conforme cada versão. Será amplamente divulgada a todos os colaboradores e partes interessadas e, conforme o Art. 7º da Circular 3978/2020, diz que política referida em seu art. 2º, deve ser: *"I - documentada; "II - aprovada pelo conselho de administração ou, se inexistente, pela diretoria da instituição; e "III - mantida atualizada."*

RICARDO PINHEIRO BRAGA:89637488120

Assinado de forma digital por RICARDO PINHEIRO BRAGA:89637488120
Dados: 2025.09.25 14:42:21 -03'00'

ÍNDICE