

POLÍTICA INSTITUCIONAL DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO E A PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA (PLD-FTP)		
CLASSIFICAÇÃO DA INFORMAÇÃO	ÁREA RESPONSÁVEL	SOCIEDADES APLICÁVEIS
Pública	Compliance	Grupo StoneCo

APROVAÇÃO	
Data da Aprovação	Aprovadores
02/09/2026	Conselho de Administração Diretoria Executiva

HISTÓRICO DE REVISÃO			
No. Revisão	Descrição	Data	Área / Responsável
01	Criação da Política	30/09/2020	Governança PLD-FTP
02	Atualização da Política	02/12/2020	Governança PLD-FTP
03	Atualização da Política	08/10/2021	Governança PLD-FTP
04	Atualização da Política	30/12/2022	Governança PLD-FTP
05	Atualização da Política	30/08/2024	Governança PLD-FTP
06	Atualização da Política	13/11/2025	Governança PLD-FTP
07	Atualização da Política	27/02/2026	Governança PLD-FTP

ÍNDICE

1. TERMOS E DEFINIÇÕES	2
2. OBJETIVO	7
3. ABRANGÊNCIA	7
4. APROVAÇÃO	7
5. VIGÊNCIA	7
6. PRINCÍPIOS	7
7. PROGRAMA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA	8
8. ATRIBUIÇÕES E RESPONSABILIDADES	12
9. REPORTE E CANAIS DE CONTATO	15
10. SIGILO DAS INFORMAÇÕES	15
11. DOCUMENTAÇÃO OU LEGISLAÇÃO RELACIONADA	16
ANEXO I	17

1. TERMOS E DEFINIÇÕES

Área de Auditoria Interna: significa a área responsável pela avaliação independente e periódica da eficácia dos processos de gerenciamento de riscos, controle e governança da Companhia.

Área de Conformidade: significa a área responsável pela conformidade da Companhia com a regulação aplicável, normativos e demais atos emitidos por órgãos reguladores.

Área de Gestão de Riscos: significa a área responsável pelas atividades de gerenciamento de riscos e de capital da Companhia, incluindo a identificação, classificação e resposta a riscos.

Área de Integridade: significa a área responsável por promover e garantir a ética e a transparência dentro da Companhia, atuando na prevenção, detecção e correção de práticas que possam comprometer a reputação da Companhia e que violem o Código de Ética StoneCo.

Área de PLD-FTP: significa a área da Diretoria de Jurídico e *Compliance* responsável pela implementação, manutenção e aprimoramento contínuo do Programa de PLD-FTP. É composta pelas frentes de *Onboarding* (KYC, KYP, KYS e KYE), Monitoramento, Seleção, Análise e Comunicação (MSAC) e Governança de PLD-FTP, assegurando a aderência dos processos às diretrizes internas e à regulamentação aplicável.

Área de Prevenção a Fraudes (Riscos): significa a área responsável por estabelecer as diretrizes e mecanismos para prevenir, identificar e responder a atos fraudulentos internos e externos que possam comprometer a integridade, a segurança e a confiabilidade das operações da Companhia.

Área de Tecnologia de Riscos: significa a área responsável pelo desenvolvimento, manutenção e evolução de sistemas, ferramentas e soluções tecnológicas voltadas ao gerenciamento de riscos, apoiando o atendimento a requisitos regulatórios, controles internos e processos de monitoramento da Companhia.

Auditoria Externa: significa o processo independente e sistemático de exame das demonstrações financeiras, controles internos e práticas de uma organização, realizado por profissionais externos, com o objetivo de verificar sua conformidade com normas legais e contábeis, bem como atestar a fidedignidade e transparência das informações apresentadas.

ABR: significa “Abordagem Baseada em Riscos”, metodologia utilizada para avaliação e gestão de atividades, processos e sistemas visando melhor direcionamento dos esforços e recursos na prática de PLD-FTP com base na probabilidade de ocorrência de eventos adversos e no impacto que esses eventos podem ter.

AIR: significa “Avaliação Interna de Riscos” para fins de PLD-FTP, por meio da qual os riscos e respectivos controles da Companhia são mapeados com o objetivo de definir o nível de apetite de risco da Companhia, consignados na Declaração de Apetite por Riscos (RAS). Portanto, os processos, políticas, procedimentos e controles relacionados à PLD-FTP devem ser baseados na AIR com o intuito de que os riscos de Lavagem de Dinheiro e de Financiamento do Terrorismo (LD-FTP) sejam adequadamente geridos.

Avaliação de Efetividade: significa o processo regulatório destinado a avaliar a efetividade da política, dos processos e dos controles internos de PLD-FTP.

Administradores: significa os membros da alta administração da Companhia, incluindo diretores e membros de órgãos estatutários, responsáveis pela gestão e tomada de decisão no âmbito de suas atribuições.

BCB: significa Banco Central do Brasil.

Beneficiário Final: significa a pessoa natural que, em última instância, controla ou influencia significativamente uma entidade, direta ou indiretamente. É também considerado beneficiário final o representante, inclusive o procurador e o preposto, que exerçam o comando de fato sobre as atividades ou transações do Cliente pessoa jurídica.

Cliente(s): significa, para fins desta Política, qualquer pessoa física ou jurídica, atuando em nome próprio ou de terceiros que mantenha cadastro ativo e que contrate produtos ou serviços financeiros comercializados pela Companhia.

COAF: significa o Conselho de Controle de Atividades Financeiras - Unidade de Inteligência Financeira Brasileira, criado pela Lei nº 9.613, de 3 de março de 1998.

Colaborador(es): significa qualquer colaborador(a)/empregado(a) da Companhia, sob o regime CLT, inclusive jovens aprendizes, ou ainda sob o regime de estágio.

CSNU: significa Conselho de Segurança das Nações Unidas.

Companhia: significa a StoneCo e suas controladas, conforme aplicável.

Comissão Deliberativa de PLD-FTP: significa a instância da área de PLD-FTP, composta pela coordenação e gerência da área, responsável por deliberar periodicamente sobre casos suspeitos de LD-FTP. As decisões dessa Comissão podem resultar em comunicação ao COAF, bem como em outras providências consideradas necessárias no contexto do Programa de PLD/FTP da Companhia.

Comitê de Auditoria: significa o órgão de assessoramento à Diretoria Executiva, responsável por monitorar a qualidade das demonstrações financeiras e dos controles internos do Conglomerado Prudencial Stone, acompanhar o desempenho das auditorias interna e externa, dentre outras atribuições correlatas. O Comitê é único para as instituições autorizadas a funcionar pelo BCB integrantes do Conglomerado Prudencial Stone.

Conglomerado Prudencial Stone: significa a Stone Instituição de Pagamento S.A. e suas subsidiárias.

Conselho de Administração: significa o conselho de administração da StoneCo, órgão colegiado

responsável pela definição das diretrizes estratégicas e pela supervisão da gestão da Companhia.

Controles Internos: significa o conjunto de processos, políticas e procedimentos estabelecidos pela Companhia para assegurar a mitigação de riscos e a conformidade regulatória, sendo operacionalizados pelas áreas de segunda linha de defesa, tais como Gestão de Riscos e Conformidade.

Diretoria Executiva: significa os membros da Diretoria da StoneCo, eleitos como *officers* pelo Conselho de Administração, em conjunto com outros diretores que reportam diretamente ao Diretor Presidente. Para fins regulatórios, integram também a Diretoria Executiva os diretores estatutários da Stone Instituição de Pagamento S.A.

Diretoria do Jurídico e Compliance: significa a Diretoria da Companhia responsável pelas atividades das áreas de Jurídico, Compliance e de Governança Corporativa, incluindo mas não se limitando às atividades da Área de PLD-FTP.

Declaração de Apetite a Riscos (RAS): significa o documento por meio do qual a Companhia define os tipos de riscos que está disposta a assumir, bem como os respectivos níveis de tolerância, no cumprimento de seus objetivos estratégicos, incluindo os processos estabelecidos para sua gestão de forma efetiva e prudente.

Financiamento do Terrorismo: significa a captação, provisão, doação, transferência ou disponibilização de recursos, bens, direitos ou valores, de origem lícita ou ilícita, com a finalidade de financiar, direta ou indiretamente, a prática de atos de terrorismo ou o apoio a indivíduos, grupos, entidades ou organizações terroristas.

Financiamento para Proliferação de Armas de Destruição em Massa: significa a captação, provisão, doação, transferência ou disponibilização de recursos, bens, direitos ou valores, de origem lícita ou ilícita, com a finalidade de apoiar, direta ou indiretamente, a produção, desenvolvimento, aquisição, posse, transporte, transferência, armazenamento ou o uso de armas de destruição em massa, bem como de seus materiais, componentes tecnológicos ou meios de entrega.

Fórum de Risco: significa o órgão de assessoramento da Diretoria Executiva ao qual cabe deliberar a respeito de questões relativas à gestão de riscos e de capital que lhe forem delegadas pela Diretoria Executiva.

Fornecedores: significa qualquer pessoa física ou jurídica, seu representante legal e/ou preposto que prestem ou estejam prestando serviços terceirizados para a Companhia.

KYC: significa a sigla em inglês para o termo “*Know Your Customer*”, correspondente a “Conheça o seu Cliente”.

KYE: significa a sigla em inglês para o termo “*Know Your Employee*”, correspondente a “Conheça o seu Funcionário”.

KYP: significa a sigla em inglês para “*Know Your Partner*”, correspondente a “Conheça seu Parceiro”.

KYS: significa a sigla em inglês para “*Know Your Supplier*”, correspondente a “Conheça o seu Fornecedor”.

Lavagem de Dinheiro: significa a prática criminosa que consiste na ocultação ou dissimulação da natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de crime ou contravenção penal antecedente. Essas práticas ocorrem por meio de transações que objetivam eliminar ou dificultar o rastreamento da origem ilegal dos recursos e posterior reintegração dos recursos no sistema financeiro, de forma a ocultar sua origem ilícita.

LD-FTP: significa a sigla para Lavagem de Dinheiro, Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

Lista OFAC - Specially Designated Nationals and Blocked Person List (SDN List): Listas de sanções administradas pela OFAC.

MSAC: significa a sigla para monitoramento, seleção, análise e comunicação de movimentações suspeitas.

OFAC ou Office of Foreign Assets Control: significa uma autoridade de supervisão do Departamento do Tesouro dos Estados Unidos, responsável por administrar e aplicar sanções econômicas e comerciais contra países, empresas, organizações e indivíduos que representem ameaça à segurança nacional ou à política externa dos EUA.

Orelhão: significa o Canal disponibilizado a todos os Colaboradores, Terceiros e ao público em geral para comunicação confidencial e, se desejada, anônima, de fato, alegação e/ou ato suspeito, previsível ou consumado, que envolve uma violação e/ou irregularidades ao Código de Ética, políticas, normas e procedimentos internos da Companhia, bem como às leis vigentes e demais regulamentos.

Parceiro(s): significa entidades que podem desempenhar um papel crítico no fornecimento de produtos, serviços ou suporte essencial para as operações da Companhia. A parceria envolve a troca de informações, recursos e ações conjuntas com o objetivo de atingir metas e objetivos compartilhados.

PEP Relacionado: significa o representante, familiar ou estreito colaborador de uma Pessoa Exposta Politicamente (PEP Titular). Nos termos do art. 19 da Circular BCB nº 3.978/2020, consideram-se familiares os parentes, em linha reta ou colateral, até o segundo grau, bem como o cônjuge, companheiro(a) e/ou enteado(a); e colaborador estreito aquele que mantém relação próxima com o PEP, como participação conjunta em empresas ou arranjos sem personalidade jurídica, atuação como mandatário ou controle de estruturas criadas em benefício do PEP.

PEP Titular: significa “Pessoa Exposta Politicamente” e corresponde a todo agente público que desempenha ou tenha desempenhado, nos últimos 5 (cinco) anos, no Brasil ou em país, território ou dependência estrangeira, cargo, emprego ou função pública relevante, nos termos do art. 27 da Circular

BCB nº 3.978, de 23 de janeiro de 2020.

PLD-FTP: significa Prevenção à Lavagem de Dinheiro, Combate ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

Prestadores de Serviços Terceirizados ou **Terceiros:** significa qualquer pessoa física ou jurídica, seu representante legal e/ou preposto que prestem ou estejam prestando serviços terceirizados para a Companhia.

Programa de PLD-FTP: significa o conjunto de políticas, manuais, processos, procedimentos, controles e estrutura de governança adotados pela Companhia com o objetivo de identificar, prevenir e reportar operações ou práticas de Lavagem de Dinheiro, Financiamento ao Terrorismo, ou quaisquer atividades criminosas envolvendo simulação ou ocultação de recursos financeiros.

Política: significa a presente Política Institucional de Prevenção à Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo e a Proliferação de Armas de Destruição em Massa (PLD-FTP).

StoneCo: significa a StoneCo Ltd., sociedade constituída e validamente existente sob as leis das Ilhas Cayman, sediada na Harneys Fiduciary (Cayman) Limited, 4th Floor, Harbour Place, 103 Church St., PO Box 10240 KY1-1002, Georgetown, Ilhas Cayman, inscrita no CNPJ/MF sob o n.º 31.752.270/0001-82.

Stone IP: significa a Stone Instituição de Pagamento S.A., sociedade anônima, inscrita no CNPJ/ME sob nº 16.501.555/0001-57.

2. OBJETIVO

Esta Política tem por objetivo consolidar os princípios e fundamentos da Companhia quanto à prevenção à Lavagem de Dinheiro e ao combate ao Financiamento do Terrorismo e ao Financiamento para Proliferação de Armas de Destruição em Massa, em conformidade com a legislação e regulamentação vigentes, bem como com as melhores práticas nacionais e internacionais. Adicionalmente, esta Política visa padronizar o tratamento de PLD-FTP no âmbito da Companhia e implementar uma estrutura efetiva para prevenir a sua utilização em práticas de Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa.

3. ABRANGÊNCIA

Esta Política se aplica à Companhia e, portanto, a todos os seus Clientes, Colaboradores, Administradores, Parceiros, Fornecedores e Prestadores de Serviços Terceirizados, os quais estão a ela vinculados e que têm o dever de cumprimento de todas as suas disposições.

O documento é adotado de forma unificada para todo o Conglomerado Prudencial Stone, em conformidade com o art. 4º da Circular BCB nº 3.978/2020.

4. APROVAÇÃO

Esta Política e suas atualizações devem ser aprovadas pelo Conselho de Administração e pela Diretoria Executiva.

5. VIGÊNCIA

Esta Política entra em vigor na data de sua aprovação, permanecendo vigente por tempo indeterminado e sendo atualizada sempre que necessário em função de alterações na AIR, nos processos aqui descritos ou em decorrência de exigências legais ou regulatórias aplicáveis.

6. PRINCÍPIOS

6.1 Avaliação Interna de Risco

A AIR da Companhia deverá ser elaborada com o objetivo de identificar, mensurar e mitigar o risco de utilização de seus produtos e serviços na prática de Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa, considerando minimamente os seguintes perfis de risco:

- dos Clientes;
- da instituição, incluindo o modelo de negócio e a área geográfica de atuação;
- das operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias; e

- das atividades exercidas pelos Colaboradores, Parceiros e Prestadores de Serviços Terceirizados.

Com base nessa avaliação, é aplicada a metodologia de Abordagem Baseada em Risco (ABR), que estabelece processos, controles e procedimentos que garantem, em relação ao risco de Lavagem de Dinheiro e Financiamento do Terrorismo e da Proliferação: (i) a identificação e avaliação; (ii) a definição de critérios na priorização das ações de gerenciamento direcionadas para os riscos mais críticos ou significativos; (iii) a elaboração de respostas por meio da adoção de medidas proporcionais de prevenção e mitigação; e (iv) o monitoramento contínuo das condições e contextos que permitam atualizar a avaliação de risco sempre que necessário.

A AIR deverá ser revisada a cada 2 (dois) anos, bem como sempre que ocorrerem alterações significativas nos perfis de risco mencionados acima.

6.2 Abordagem Baseada em Risco

A Companhia adota a ABR, estruturada a partir da avaliação de categorias e variáveis de risco. Essa metodologia assegura que as medidas adotadas para prevenir e mitigar os riscos de LD-FTP sejam proporcionais aos riscos identificados no processo de aceitação, monitoramento e manutenção do relacionamento.

A ABR permite a aplicação de medidas e controles compatíveis com o nível de risco identificado, possibilitando a alocação eficiente de recursos e esforços. Nesse contexto, a Companhia adota procedimentos de devida diligência simplificada, padrão e reforçada para Clientes, Colaboradores, Parceiros e Prestadores de Serviços Terceirizados, em conformidade com a Circular BCB nº 3.978/2020.

6.3 Avaliação de Efetividade

A efetividade das políticas, normas, procedimentos e controles internos de PLD-FTP deve ser avaliada anualmente e submetida à apreciação dos órgãos competentes da Companhia.

Após a emissão, revisão e validação dos pontos de aprimoramento eventualmente identificados na Avaliação de Efetividade, a Diretoria de Jurídico e *Compliance* deverá elaborar planos de ação para acompanhar, junto às áreas envolvidas, a implementação das medidas necessárias para correção das deficiências apontadas. Os planos de ação deverão ser submetidos à Diretoria Executiva e ao Comitê de Auditoria para avaliação e acompanhamento.

7. PROGRAMA DE PREVENÇÃO À LAVAGEM DE DINHEIRO E COMBATE AO FINANCIAMENTO DO TERRORISMO E DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Esta Política estabelece o Programa de PLD-FTP da Companhia, com o objetivo de assegurar a conformidade com a legislação e a regulamentação aplicáveis por meio de um conjunto de diretrizes, processos e controles fundamentados na ABR. O Programa de PLD-FTP busca garantir que as medidas de prevenção e mitigação adotadas sejam compatíveis com o perfil de risco dos Clientes, da Companhia, das

suas operações, produtos e serviços, bem como de seus Colaboradores, Parceiros e Prestadores de Serviços Terceirizados.

Os processos e controles que compõem o Programa de PLD-FTP têm como finalidade viabilizar o cumprimento das diretrizes estabelecidas nesta Política e nos normativos internos aplicáveis, prevenindo a utilização dos produtos e serviços da Companhia para a prática de ilícitos relacionados à Lavagem de Dinheiro, ao Financiamento do Terrorismo e ao Financiamento da Proliferação de Armas de Destruição em Massa.

Para a efetiva implementação do Programa de PLD-FTP, deverão ser observados, de forma integrada e contínua, os seguintes pilares:

7.1 Políticas, normas e procedimentos

A Companhia mantém políticas, normas e procedimentos destinados a disciplinar a implementação e a execução dos controles de PLD-TP, em conformidade com a legislação e a regulamentação vigente. Esses documentos estabelecem as diretrizes e medidas aplicáveis aos diferentes perfis de risco identificados pela Companhia e são revisados, atualizados e aprovados periodicamente, de acordo com as alçadas e prazos definidos em sua estrutura de governança.

7.2 Identificação, qualificação e classificação

A Companhia adota procedimentos para a identificação, qualificação e classificação de Clientes, Fornecedores, Parceiros e Colaboradores, em conformidade com a legislação aplicável e com as diretrizes estabelecidas na Norma de KYs. Esses processos contemplam a coleta, verificação, validação, atualização e armazenamento de informações cadastrais em sistemas informatizados, bem como sua utilização nos procedimentos de monitoramento, seleção e análise de operações e situações suspeitas.

A Companhia estabelece mecanismos de identificação, qualificação e classificação por níveis de risco de seus Clientes (KYC), Fornecedores (KYS), Parceiros (KYP) e Colaboradores (KYE). Tais mecanismos visam mitigar riscos relacionados à LD-FTP, abrangendo desde a coleta e validação de informações no início do relacionamento até o monitoramento contínuo ao longo de todo o seu ciclo de vida, em estrita consonância com a AIR e a ABR.

As informações cadastrais são atualizadas periodicamente, conforme os critérios de risco definidos na AIR, observando-se obrigatoriamente o intervalo máximo de 5 (cinco) anos para Clientes ativos, sem prejuízo de revisões antecipadas sempre que identificadas alterações relevantes no perfil de risco ou na relação de negócio.

A Companhia adota medidas reforçadas de gestão e monitoramento para relacionamentos classificados como de alto ou altíssimo risco para fins de LD-FTP.

Também são adotadas medidas de caráter restritivo para o início ou a manutenção de relacionamentos com Clientes, Fornecedores, Parceiros e Colaboradores quando identificadas situações que possam indicar envolvimento em práticas de LD-FTP.

Adicionalmente, a Companhia implementa procedimentos e controles internos compatíveis com relacionamentos envolvendo Pessoas Expostas Politicamente (PEPs), incluindo PEP Titular e PEP Relacionado, considerando essa condição para fins de classificação de risco e avaliação do interesse no início ou na manutenção do relacionamento.

Além disso, são adotados procedimentos específicos para os casos em que não seja possível identificar ou verificar o Beneficiário Final.

7.3 Monitoramento, seleção, análise e comunicação de operações ou situações suspeitas

Todas as transações e operações realizadas pelos Clientes são monitoradas por meio de sistemas informatizados, com alertas parametrizados destinados à identificação de situações que possam configurar indícios de LD-FTP, em conformidade com os requisitos e prazos estabelecidos na regulamentação vigente.

Os parâmetros, variáveis, regras e cenários de monitoramento são definidos com base na AIR, considerando as tipologias e exemplos previstos na Carta Circular BCB nº 4.001/2020, bem como boas práticas de mercado, de forma compatível com o modelo de negócio da Companhia. Os parâmetros adotados são passíveis de verificação quanto à sua adequação e efetividade.

No âmbito do monitoramento e seleção de operações, a Companhia adota procedimentos específicos para a identificação e análise das contrapartes envolvidas em transações realizadas em ambientes de registro.

Nos termos da ABR, Clientes com maior exposição a riscos de LD-FTP estão sujeitos a critérios mais rigorosos e a procedimentos de monitoramento reforçados, de forma proporcional ao seu perfil de risco.

A análise dos alertas gerados é realizada de forma centralizada pela área de PLD-FTP da Companhia, sendo formalizada por meio de dossiê. Essas atividades não são objeto de terceirização, exceto no que se refere à contratação de serviços e ferramentas tecnológicas auxiliares, na forma admitida pela regulamentação vigente.

A decisão sobre a comunicação de operações ou situações suspeitas aos órgãos reguladores competentes é de responsabilidade da Comissão Deliberativa de PLD-FTP, com base nas informações constantes dos dossiês elaborados pela Área de PLD-FTP. A Comissão se reúne periodicamente e pode ser convocada de forma extraordinária sempre que necessário. Nos casos considerados de maior risco de exposição (risco crítico) ou com potencial de risco reputacional relevante, bem como quando houver divergência de entendimento entre os membros da Comissão Deliberativa de PLD-FTP, a matéria deverá ser escalada para deliberação do diretor responsável, indicado formalmente perante os órgãos reguladores, por

coordenar e garantir o cumprimento do Programa de PLD-FTP, observada a matriz de alçadas da Companhia.

Os procedimentos de comunicação são realizados em estrita observância à regulamentação aplicável e às diretrizes estabelecidas na Norma de MSAC, sendo que as comunicações realizadas de boa-fé não ensejam responsabilidade civil ou administrativa, nos termos da legislação vigente.

7.4 Registro e manutenção de dados e operações

Todas as informações relacionadas a cadastros, operações, produtos e serviços da Companhia devem ser mantidas em sua forma original ou em formato eletrônico, em sistemas que assegurem sua integridade, disponibilidade, rastreabilidade, recuperação e proteção contra acessos não autorizados, observados os prazos de retenção, responsabilidades e demais requisitos estabelecidos na legislação e regulamentação aplicáveis.

7.5 Avaliação de novos produtos e serviços

Novos produtos, serviços, canais de distribuição e tecnologias devem ser previamente avaliados, conforme as diretrizes estabelecidas em normativos internos, com objetivo de identificar, avaliar e mitigar eventuais riscos de utilização para a prática de crimes de LD-FTP.

7.6 Sanções

A Companhia não admite o início ou a manutenção de relacionamento com pessoas naturais, pessoas jurídicas ou entidades sujeitas a sanções nacionais ou internacionais, incluindo, mas não se limitando, às listas emanadas pelo Conselho de Segurança das Nações Unidas (CSNU) e pelo Escritório de Controle de Ativos Estrangeiros (Office of Foreign Assets Control - OFAC) - Lista OFAC, e às designações nacionais previstas na Lei nº 13.810/2019.

Além das listas de sanções nacionais e internacionais, de observância obrigatória, a Companhia poderá em caráter complementar de suporte à análise de riscos, consultar listas privadas, bases públicas e outras fontes idôneas de inteligência e de due diligence que identifiquem pessoas físicas ou jurídicas com supostos vínculos com o crime organizado, inclusive integrantes ou associados ao Primeiro Comando da Capital - PCC e ao Comando Vermelho - CV, observados os requisitos legais, a confiabilidade da fonte e a proporcionalidade na utilização.

Nesse contexto, a Companhia adota procedimentos destinados à identificação de pessoas, entidades, ativos e operações sujeitas a sanções, bem como controles para prevenir a realização de transações envolvendo partes ou contrapartes sancionadas, em observância à Lei nº 13.810/2019, à Resolução BCB nº 44/2020, à Instrução Normativa BCB nº 262/2022 e demais normas aplicáveis.

A Companhia implementa, ainda, procedimentos para identificação, indisponibilização e comunicação imediata de ativos e valores de titularidade, direta ou indireta, de pessoas naturais, pessoas jurídicas ou

entidades sancionadas, nos termos da legislação vigente, sem prejuízo do cumprimento de determinações judiciais e demais obrigações legais aplicáveis.

7.7 Treinamento e Promoção de Cultura Organizacional

Com o objetivo de aprimorar o conhecimento e fomentar o engajamento contínuo em relação aos temas de PLD-FTP, a Companhia desenvolve programas periódicos de capacitação e comunicação direcionados aos Colaboradores, Parceiros e Prestadores de Serviços Terceirizados elegíveis. Essas iniciativas reforçam a importância do tema no contexto das responsabilidades corporativas, legais e regulatórias, bem como das diretrizes institucionais estabelecidas nesta Política e nos normativos internos aplicáveis.

As ações de treinamento e comunicação de PLD-FTP são realizadas de forma periódica e abrangem todas as áreas da Companhia, podendo incluir cursos presenciais ou a distância (*e-learning*), palestras, campanhas, comunicados, publicações e outros mecanismos de disseminação do conhecimento.

O programa também contempla iniciativas específicas voltadas ao engajamento dos diferentes níveis da Companhia, incluindo a Diretoria Executiva, com o objetivo de fortalecer a cultura organizacional e promover práticas alinhadas aos princípios e controles de PLD-FTP.

7.8 Intercâmbio de Informações

A Companhia dispõe de mecanismos formais de intercâmbio de informações entre as suas áreas que desempenham funções de Controles Internos (Gestão de Riscos, Conformidade e Auditoria Interna), com o objetivo de assegurar o adequado cumprimento das obrigações relacionadas à PLD-FTP.

O intercâmbio ocorre de forma tempestiva e proporcional à relevância do risco identificado em cada caso, conforme a AIR, e pode compreender, entre outros elementos, o compartilhamento de dados cadastrais de Clientes, informações sobre perfil de risco e classificação atribuída, histórico de alertas e análises realizadas, e demais informações necessárias à adequada gestão integrada de riscos de LD-FTP. Esta integração garante que a Companhia avalie continuamente as interações entre o risco de LD-FTP e os demais riscos mapeados pela instituição, mitigando efeitos adversos compostos.

O compartilhamento observa os limites legais e regulatórios aplicáveis, inclusive quanto ao dever de sigilo e proteção de dados pessoais.

8. ATRIBUIÇÕES E RESPONSABILIDADES

Conselho de Administração

- Aprovar a presente Política.

Comitê de Auditoria

- Tomar ciência da AIR, da Avaliação de Efetividade e dos respectivos planos de ação destinados a endereçar eventuais deficiências identificadas.

Diretoria Executiva

- Aprovar a presente Política e recomendar sua aprovação ao Conselho de Administração;
- Tomar ciência da AIR e da Avaliação de Efetividade, bem como avaliar os planos de ação destinados a endereçar eventuais deficiências identificadas; e
- Assegurar o compromisso com a efetividade e a melhoria contínua das políticas, normas, procedimentos e controles internos relacionados à PLD-FTP, bem como a existência de estrutura de governança adequada ao seu cumprimento.

Fórum de Risco

- Assessorar a Diretoria Executiva nas deliberações sobre gestão de riscos que lhe forem delegadas;
- Auxiliar o membro da Diretoria Executiva responsável pela gestão de riscos em suas atribuições;
- Apoiar a Diretoria do Jurídico e *Compliance* nas decisões que forem requeridas por esta, para a boa governança do Programa de PLD-FTP; e
- Apoiar a Comissão Deliberativa de PLD-FTP sempre que requerido.

Comissão Deliberativa de PLD-FTP

- Deliberar e aprovar os casos que demandam comunicação aos órgãos competentes e/ou o descredenciamento de clientes, com base na avaliação detalhada das evidências disponíveis.

Diretoria do Jurídico e *Compliance* (Área de PLD - Diretor responsável pelo cumprimento das obrigações previstas nas normas de PLD-FTP)

- Assegurar a implementação, manutenção e aprimoramento contínuo do Programa de PLD-FTP;
- Elaborar e aprovar a AIR;
- Elaborar a Avaliação de Efetividade e os relatórios de acompanhamento dos respectivos planos de ação;
- Definir as diretrizes e os critérios mínimos para classificação dos riscos de LD-FTP de Clientes, Colaboradores, Parceiros, Fornecedores e Prestadores de Serviços Terceirizados;
- Assegurar o cumprimento das exigências legais e regulatórias relacionadas à PLD-FTP;
- Desenvolver, atualizar e manter esta Política e os demais normativos internos relacionados ao tema, em conformidade com a legislação, a regulamentação aplicável e as melhores práticas de mercado;
- Definir as diretrizes e validar os programas de treinamento e capacitação contínua em PLD-FTP destinados aos Colaboradores;
- Realizar o monitoramento, a seleção e a análise de operações e situações com indícios de LD-FTP, por meio de sistemas automatizados e procedimentos internos, observados os requisitos e prazos estabelecidos na regulamentação aplicável;
- Formalizar as análises realizadas por meio de dossiês técnicos e manter os registros correspondentes;
- Implantar e aprimorar processos e controles destinados a assegurar a conformidade das atividades da Companhia com as normas de PLD-FTP;
- Dar ciência da AIR, da Avaliação de Efetividade e dos respectivos planos de ação à Auditoria Interna;

- Conduzir a Comissão Deliberativa de PLD-FTP para deliberação dos casos que demandam comunicação aos órgãos competentes e/ou o descredenciamento de Clientes;
- Assegurar a comunicação de operações suspeitas aos órgãos reguladores competentes, nos prazos e termos da regulamentação vigente; e
- Realizar a comunicação de não ocorrência, quando aplicável, nos termos da Circular BCB nº 3.978/2020.

Área de Prevenção a Fraudes (Riscos)

- Assegurar os procedimentos que lhe forem atribuídos para a adequada validação da identidade dos Clientes no início do relacionamento;
- Reportar à área de PLD-FTP qualquer situação atípica característica de LD-FTP que for identificada.

Área de Produto Regulatório - Cadastro

- Garantir que as políticas e processos para manutenção dos dados cadastrais sejam executados conforme definidos, com o objetivo de manter a base de dados cadastrais atualizada e confiável.

Área de Tecnologia de Risk & Identity

- Garantir a manutenção dos dados cadastrais do cliente ao longo do ciclo de vida na base, com o objetivo de manter a base de dados cadastrais atualizada e confiável;
- Gestão, manutenção e melhoria do(s) sistema(s) informatizado(s) utilizados nos Processos de PLD-FTP geridos pela Área de Tecnologia de Risk & Identity;
- Analisar os requerimentos legais e regulatórios de PLD-FTP que lhe forem informados pela Diretoria do Jurídico e *Compliance* e avaliar os respectivos impactos nos sistemas geridos pela Área de Tecnologia de Risk & Identity; e
- Reportar à Diretoria do Jurídico e *Compliance* as atualizações de políticas internas que necessitem de atenção ou ensejem desenvolvimento sistêmico de novas diretrizes.

Área de Auditoria Interna

- Aplicar testes e procedimentos de auditoria em matéria de PLD-FTP conforme priorização de escopo definido no plano anual de auditoria aprovado pelo COAUD;
- Acompanhar as ações de regularização dos apontamentos oriundos de cada trabalho de Auditoria Interna.

Área de Gestão de Riscos

- Apoiar as áreas de negócio, a primeira linha de defesa, na avaliação dos processos e riscos operacionais, e na validação do desenho dos controles e dos planos de ação;
- Garantir a adequação às regulamentações externas e internas aplicáveis, principalmente no que diz respeito a supervisão do sistema de Controles Internos; e
- Monitorar e reportar a qualidade dos controles das operações através de testes e indicadores.

Área de Conformidade

- Garantir a independência, autonomia e autoridade necessárias para a adequada execução das atividades da Área de Conformidade, assegurado reporte direto à Diretoria Executiva para comunicação de eventos, falhas e eventuais irregularidades que possam impactar o gerenciamento do risco de conformidade, bem como dos respectivos planos de ação para sua remediação; e
- Garantir a aplicação de medidas corretivas para as falhas de conformidade identificadas.

Área de Integridade

- Executar controles de aderência e participação dos Colaboradores nos treinamentos de PLD-FTP;
- Recepcionar e reportar às áreas competentes (incluindo a área de PLD-FTP) denúncias de natureza de Lavagem de Dinheiro e/ou Financiamento do Terrorismo captadas via Orelhão.

Colaboradores

- Conhecer, entender e cumprir as diretrizes desta Política;
- Participar dos treinamentos que lhes forem disponibilizados ou demandados, em virtude da necessidade de aprofundamento e capacitação em suas funções;
- Comunicar toda situação, operação ou proposta suspeita de envolvimento com qualquer tipo de ilicitude à Área de Integridade ou por meio do Orelhão; e
- Manter sigilo dos processos e informações confidenciais e restritas.

9. REPORTE E CANAIS DE CONTATO

A Área de PLD-FTP será responsável pelo tratamento de dúvidas relativas aos temas tratados nesta Política ou a possíveis assuntos não contemplados, por meio do e-mail: governanapld@stone.com.br. Quaisquer violações a esta Política deverão ser reportados à Companhia por meio do Orelhão, em:

- Site: <https://www.contatoseguro.com.br/orelhaostone>
- Telefone: 0800 881 3629
- Aplicativo: Aplicativo “Contato Seguro” no dispositivo móvel
- Whatsapp: +55 51 3376-9353

A Companhia garante a confidencialidade e anonimato das informações reportadas, bem como a não retaliação a denunciante que estiverem agindo de boa-fé.

10. SIGILO DAS INFORMAÇÕES

Todas as informações relacionadas a dados de indícios e ou suspeitas de Lavagem de Dinheiro e combate ao Financiamento do Terrorismo são de caráter confidencial, não devendo, em hipótese alguma, ser disponibilizadas às partes envolvidas. As comunicações de operações e situações suspeitas, com base na Circular BCB nº 3.978/2020 e na Carta Circular BCB nº 4.001/2020 são de uso exclusivo dos órgãos reguladores para análise e investigação, sendo vedado dar ciência de sua existência ou conteúdo às partes envolvidas ou a quaisquer terceiros, ressalvados os casos previstos em lei.

11. DOCUMENTAÇÃO OU LEGISLAÇÃO RELACIONADA

- Código de Ética StoneCo;
- Norma de Governança de PLD-FTP;
- Norma de KYs de PLD-FTP;
- Norma de MSAC de PLD-FTP;
- Norma de Alçadas de PLD-FTP;
- Lei Federal nº 9.613/1998;
- Lei Federal nº 13.260/2016;
- Lei Federal nº 13.810/2019;
- Decreto-Lei nº 2.848/2040;
- Circular BCB nº 3.978/2020;
- Carta Circular BCB nº 4.001/2020;
- Instrução Normativa BCB nº 262/2022;
- Resolução BCB nº 44/2020;
- Resolução CVM nº 50/2021;
- Resolução COAF nº 29/2017;
- Resolução COAF nº 31/2019.

ANEXO I

Termo de Aceite aos Termos da Política Institucional de Prevenção à Lavagem de Dinheiro, Combate ao Financiamento do Terrorismo e a Proliferação de Armas de Destruição em Massa

Declaro que recebi, li e compreendi os termos da “*POLÍTICA INSTITUCIONAL DE PREVENÇÃO À LAVAGEM DE DINHEIRO, COMBATE AO FINANCIAMENTO DO TERRORISMO E A PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA – (PLD-FTP)*”, comprometendo-me a cumpri-la integralmente, bem como a relatar ao **ORELHÃO***, caso tome conhecimento sobre qualquer descumprimento da Política, sob pena de sujeitar-me às medidas administrativas e legais cabíveis, durante todo o período de meu vínculo empregatício (e posteriormente, naquilo que for aplicável).

Aceite de Colaboradores Stone**Nome Completo:****CPF:****Assinatura:****Local e Data:**

Data: ____/____/____

*Significa o Canal disponibilizado a todos os Colaboradores, Terceiros e ao público em geral para comunicação confidencial e, se desejada, anônima, de fato, alegação e/ou ato suspeito, previsível ou consumado, que envolve uma violação e/ou irregularidades ao Código de Ética, políticas, normas e procedimentos internos da Companhia, bem como às leis vigentes e demais regulamentos.