

Política de Prevenção à Lavagem de Dinheiro, Combate ao Financiamento do Terrorismo e a Proliferação de Armas de Destruição em Massa (PLD-CFTP)

Banco HSBC S.A. – HBBZ

Janeiro 2026

Conteúdo

1.	POLÍTICA	3
2.	APLICAÇÃO	3
3.	GOVERNANÇA DO PROGRAMA DE PLD-CFTP	3
3.1	Pilares	3
3.2	Aprovações	3
3.3	Registro e Retenção de Documentos	4
3.3.1	Registros	4
3.3.2	Retenção de Registros	4
4.	MODELOS E METODOLOGIAS DE RISCO DE PLD-CFTP	4
4.1	Avaliação Interna de Risco de PLD-CFTP Integrada (<i>EWRA – Enterprise-Wide AML Risk Assessment</i>)	4
4.2	Modelo de Avaliação de Risco de Clientes (<i>FCC-RAM – Financial Crime Customer Risk Assessment Model</i>)	4
4.3	Modelo de Avaliação de Risco de Países (<i>FCCRM – Financial Crime Country Risk Model</i>)	4
4.4	Risco da atividade/negócio	5
4.5	Risco do tipo de entidade	5
4.6	Modelo de Avaliação de Risco de Produtos e Serviços (<i>PRAM – AML Product Risk Assessment Model</i>)	5
5.	PROCEDIMENTOS PARA CONHECER OS CLIENTES (<i>CDD – Customer Due Diligence</i>)	5
5.1	Conheça Seu Cliente (<i>KYC – Know Your Customer</i>)	5
5.2	Diligência Adicional (<i>EDD– Enhanced Due Diligence</i>)	6
5.3	Estabelecendo relacionamento antes do completo CDD	6
5.4	Revisão Periódica do CDD	6
5.5	Suitability	6
5.6	Procedimento de encerramento de relacionamento (<i>CSEM – Customer Selection and Exit Management</i>)	6
5.7	Relacionamentos comerciais proibidos	6
6	MONITORAMENTO, SELEÇÃO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS	7
6.1	Contexto	7
6.2	Comunicação de Operação Atípica ou Suspeita (<i>FC-UAR</i>)	7
6.3	Monitoramento de Transações (<i>TM – Transaction Monitoring</i>)	7
6.4	Verificações contra Listas de Sanções e Financiamento ao Terrorismo (<i>TS – Transaction Screening</i>)	7
6.5	Sanções impostas por resoluções do Conselho de Segurança das Nações Unidas (<i>CSNU</i>)	7
6.6	Sanctions Name Screening	8
6.7	Comunicação de Atividade Suspeitas (<i>SAR – Suspicious Activity Report</i>)	8
6.8	Proibição de divulgação de SARs	8
7	PROCEDIMENTOS PARA CONHECER FUNCIONÁRIOS, PARCEIROS E PRESTADORES DE SERVIÇOS TERCEIRIZADOS	8
7.1	Contexto	8
7.2	Conheça Seu Funcionário (<i>KYE – Know Your Employee</i>)	8
7.3	Conheça Seu Parceiro e Prestador de Serviço (<i>KYS – Know Your Supplier</i>)	9
8	TREINAMENTO E CULTURA DE PLD-CFTP	9
8.1	Treinamento Mandatário	9
9	PRODUTOS E SERVIÇOS	9
9.1	Requerimentos Gerais	9
9.2	Produtos e Serviços Proibidos	10
10	AVALIAÇÃO DE EFETIVIDADE	10
11	MECANISMOS DE ACOMPANHAMENTO E CONTROLE	10
11.1	<i>Compliance Assurance</i>	10
11.2	Auditoria Interna	10
12.	LINKS	11

1. POLÍTICA

A Política de Prevenção à Lavagem de Dinheiro, Combate ao Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa ("Política de PLD-CFTP" ou a "Política") do Banco HSBC S.A. ("HBBZ") estabelece os principais princípios e requisitos para permitir que a Instituição cumpra com os requisitos legais e regulamentares aplicáveis 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, de 3 de março de 1998, e de financiamento do terrorismo, previsto nas Leis nº 13.260, de 16 de março de 2016 e 13.810, de 08 de março de 2019, bem como evasão fiscal ou qualquer outra atividade criminosa, aqui coletivamente denominados de "crimes financeiros".

Este documento é uma versão resumida da Política de PLD/FTP e foi elaborada em **complemento** à Política Global do Grupo HSBC de Crimes Financeiros (*Global Financial Crime Policy* – doravante denominada "*Global FC Policy*"), para abordar regulamentações específicas do Brasil sobre o tema:

- **Banco Central do Brasil (BACEN)**
 - Circular nº 3.978 de 23 de janeiro de 2020 ("Circular 3978")
 - Carta-Circular nº 4.001 de 29 de janeiro de 2020 ("Carta Circular 4001")
 - Resolução Conjunta nº 6 de 23 de maio de 2023 ("Resolução Conjunta 6") / Resolução nº 343 de 04 de outubro de 2023

- **Comissão de Valores Mobiliários (CVM)**
 - Resolução CVM nº 50, de 31 de agosto de 2021 ("Resolução CVM 50").

A regulamentação Brasileira deve ser seguida na sua integralidade e não há opção de dispensas ou exceções aos seus requerimentos. Sempre e quando os requisitos locais regulatórios impossibilitarem o cumprimento dos requisitos das políticas globais do HSBC, uma dispensa permanente ou temporária deve ser solicitada.

2. APLICAÇÃO

O Grupo HSBC tem tolerância zero para a facilitação de qualquer crime financeiro. Cabe a todos os funcionários e estagiários, aqui coletivamente denominados colaboradores, bem como os parceiros e prestadores de serviços terceirizados do HBBZ, atuarem de forma responsável e estarem atentos aos requisitos internos e não permitir que o HBBZ seja utilizado como intermediário para a prática de quaisquer crimes financeiros. Essa política entra em vigor a partir do momento da sua aprovação e divulgação.

3. GOVERNANÇA DO PROGRAMA DE PLD-CFTP

3.1 Pilares

O Programa de PLD-CFTP do HBBZ está alinhado a *Global FC Policy* e é compatível ao modelo de negócios e perfil de risco (i) dos seus clientes; (ii) das suas operações, transações, produtos e serviços; e (iii) dos seus colaboradores, parceiros e prestadores de serviços terceirizados. Os cinco pilares do Programa de PLD-CFTP incluem:

- I. Papeis e Responsabilidades;
- II. Sistema de Controles Internos;
- III. Treinamento & Capacitação;
- IV. Promoção de cultura organizacional; e
- V. Testes Independentes.

3.2 Aprovações

A Política de PLD-CFTP deve ser documentada, revisada anualmente e aprovada, quando houver alguma alteração material, pela Diretoria Executiva do HBBZ (OpCo – *Operating Committee*), estando sempre alinhada à *Global FC*

Policy. Por determinação desta Política, alterações não materiais podem ser aprovadas pelo Responsável pela Área de *Compliance* do HBBZ.

3.3 Registro e Retenção de Documentos

3.3.1 Registros

O HBBZ deve manter o registros de todas as operações realizadas por meio dos produtos e serviços contratados nos termos das regulamentações aplicáveis.

3.3.2 Retenção de Registros

As linhas de negócios e funções do HBBZ devem manter à disposição dos Reguladores e conservar os registros pelo período estabelecido na regulamentação vigente.

4. MODELOS E METODOLOGIAS DE RISCO DE PLD-CFTP

O HBBZ adotou uma abordagem baseada em risco na definição e implantação procedimental de sua Política. Sendo assim, faz-se essencial que os modelos e metodologias de Risco de PLD-CFTP sejam abrangentes. Detalhes estão disponíveis internamente no documento “Modelos e Metodologias de Risco de PLD-CFTP”.

4.1 Avaliação Interna de Risco de PLD-CFTP Integrada (*EWRA – Enterprise-Wide AML Risk Assessment*)

O processo de *EWRA* permite que o HBBZ identifique, avalie e mensure sua exposição ao risco de utilização de seus produtos e serviços na prática de crimes financeiros (lavagem de dinheiro, financiamento ao terrorismo, proliferação de armas de destruição em massa, sanções, suborno e corrupção). Ele fornece uma medida do risco inerente aos crimes financeiros, fatores atenuantes e riscos residuais, possibilitando que o HBBZ adote controles de gerenciamento e de mitigação reforçados para situações de maior risco e a adoção de controles simplificados nas situações de menor risco.

Adicionalmente, mais detalhes sobre o *EWRA* estão disponíveis internamente no documento “Modelos e Metodologias de Risco de PLD-CFTP”.

4.2 Modelo de Avaliação de Risco de Clientes (*FCC-RAM – Financial Crime Customer Risk Assessment Model*)

O *FCC-RAM* é a metodologia do Grupo HSBC que identifica os critérios de risco necessários para medir o risco potencial de crime financeiro inerente aos clientes e suas transações, no início e ao longo do relacionamento com o HSBC. A metodologia calcula o nível de risco, definindo e atribuindo a classificação de risco de todos os clientes do HBBZ em baixo, médio ou alto.

Adicionalmente, todos os detalhes sobre o modelo *FCC-RAM* utilizado pelo HBBZ para classificação de risco de clientes estão disponíveis internamente no documento “Modelos e Metodologias de Risco de PLD-CFTP”.

4.3 Modelo de Avaliação de Risco de Países (*FCCRM – Financial Crime Country Risk Model*)

A metodologia *FCCRM* do Grupo HSBC mensura o risco inerente de crime financeiro de um país atribuindo pontuações e uma classificação de risco super alto, alto, médio ou baixo para cada país, utilizando ponderações em relação ao risco de Lavagem de Dinheiro, Financiamento ao Terrorismo, Suborno e Corrupção, Sigilo Financeiro, Transparência Fiscal e Estabilidade Política.

A metodologia do *FCCRM* utiliza elementos específicos definidos pelo Grupo HSBC, os quais combinam uma série de fatores e indicadores que dão subsídio às pontuações para as classificações de cada país.

Mais detalhes estão disponíveis internamente no documento “Modelos e Metodologias de Risco de PLD-CFTP”.

4.4 Risco da atividade/negócio

Certas atividades/tipos de negócios são mais suscetíveis ao risco de crime financeiro.

A avaliação do fator de risco é baseado na identificação do tipo de atividade/negócio de cada cliente. O Grupo HSBC considera as variáveis do ponto de vista do crime financeiro que uma atividade/negócio possua, atribuindo ao cliente uma classificação de baixo, médio ou alto risco.

4.5 Risco do tipo de entidade

Fator projetado para levar em consideração os diferentes níveis em que as estruturas das empresas podem ser utilizadas para ocultação de bens ou fundos.

4.6 Modelo de Avaliação de Risco de Produtos e Serviços (*PRAM – AML Product Risk Assessment Model*)

A metodologia *PRAM* do Grupo HSBC mensura o risco inerente de crime financeiro dos produtos e serviços oferecidos pelo HSBC, incluindo o respectivo canal de distribuição e ambiente de negociação e registro.

Mais detalhes estão disponíveis internamente no documento “Modelos e Metodologias de Risco de PLD-CFTP”.

5. PROCEDIMENTOS PARA CONHECER OS CLIENTES (*CDD – Customer Due Diligence*)

Um processo robusto destinado a conhecer os clientes é essencial como suporte para uma gestão eficaz do risco de crime financeiro. O nível e a natureza do CDD realizado são determinados pelos riscos inerentes aos crimes financeiros do relacionamento com o cliente e pelo tipo de cliente. O CDD é mais do que um processo de documentação e é projetado para ajudar na identificação de clientes e no gerenciamento de qualquer risco de crime financeiro associado. O CDD é composto por:

- Identificação e Verificação do Cliente (*ID&V - Identification & Validation*);
- Conheça Seu Cliente (*KYC – Know Your Customer*);
- Diligências adicionais para clientes de maior risco (*EDD – Enhanced Due Diligence*);
- Revisão contínua (periódica e eventual motivada por evento específico e significativo); e
- Procedimento de encerramento de relacionamento.

O HBBZ deve manter um Perfil CDD para cada cliente, continuamente difundindo perante os clientes a importância da manutenção de seus dados cadastrais atualizados e disponibilizando canais para que esses possam comunicar quaisquer atualizações.

5.1 Conheça Seu Cliente (*KYC – Know Your Customer*)

Como parte do processo de KYC, no início e de forma permanente, as linhas de negócios devem ser capazes de qualificar seus clientes:

- Obter a cadeia de participação societária do cliente e todas as partes relacionadas como, por exemplo, controladores, administradores, diretores, representantes legais e, se houver, Beneficiários Finais (*UBOs – Ultimate Beneficial Owners*). Verificação (*Screening*) dos clientes e partes relacionadas;
- Natureza de negócios do cliente;
- Origem do Patrimônio (*SOW – Source of Wealth*): entender como o cliente gerou e mantém seu patrimônio;
- Origem dos Recursos (*SOF – Source of Funds*): entender de onde os recursos depositados no HBBZ se originaram, ou seja, a forma que foram gerados; e

- Entender o propósito de relacionamento do cliente com HBBZ.

5.2 Diligência Adicional (EDD– Enhanced Due Diligence)

Diligência adicional (*EDD*) é um processo que permite ao HBBZ gerenciar relacionamentos com certos tipos de clientes que apresentam maior risco de crimes financeiros. A extensão e profundidade do *EDD* deve corresponder ao potencial de risco imposto pelo cliente, conforme identificado no processo CDD. Portanto, a ênfase no *EDD* está na gestão de riscos e não simplesmente na documentação.

Se as medidas de EDD não puderem fornecer conforto suficiente sobre os riscos de lavagem de dinheiro apresentados pelo cliente, o Negócio não deve prosseguir com o Relacionamento Comercial.

Mais detalhes estão disponíveis internamente na seção de *EDD* do *Global Financial Crime Policy Standards*.

5.3 Estabelecendo relacionamento antes do completo CDD

O relacionamento com um cliente somente deve ser ativado quando o perfil CDD estiver completo. É vedado por requiremento regulatório local o início de relacionamento de negócios sem que os procedimentos de CDD do cliente estejam concluídos.

Admite-se, por um período máximo de 30 (trinta) dias, o início da relação de negócios em caso de insuficiência de informações relativas ao KYC do cliente, desde que não haja qualquer prejuízo aos procedimento de monitoramento e seleção de operações e situações suspeitas. Nestes casos, as linhas de negócios devem ter controles internos que permitam realizar um screening mínimo e monitorar as transações do cliente, permitindo a suspensão ou encerramento do relacionamento de uma maneira comercialmente razoável, se necessário.

5.4 Revisão Periódica do CDD

Com o tempo, o nível de risco associado aos clientes existentes pode aumentar. Para manter as informações de CDD de um cliente atualizadas, as linhas de negócios devem realizar uma revisão das informações de CDD periodicamente e/ou com base em eventos específicos (*trigger events*), aplicando uma abordagem baseada em risco para a revisão periódica obrigatória do CDD do cliente.

Os eventos específicos “*trigger events*” desencadeiam a necessidade de atualização do CDD pois são mudanças em circunstâncias que podem afetar materialmente o risco representado por um relacionamento existente com o cliente e que podem alterar a classificação de risco. Estes eventos podem ser específicos do cliente ou orientados por políticas.

5.5 Suitability

A adequação dos produtos, serviços e operações ao perfil dos clientes do HBBZ e os principais aspectos decorrentes da Resolução CVM nº 30, de 11 de Maio de 2021 devem ser observados na comercialização de valores mobiliários por meio da verificação de adequação do produto, serviço ou operação às necessidades do cliente, da situação financeira do cliente e a compatibilidade com o produto, serviço ou operação e do conhecimento necessário do cliente para compreender os riscos relacionados ao produto, serviço ou operação.

5.6 Procedimento de encerramento de relacionamento (CSEM – Customer Selection and Exit Management)

O Grupo HSBC oferece produtos e serviços financeiros a clientes dentro de seu apetite pelo risco de crimes financeiros. Durante o relacionamento com o cliente, vários fatores podem mudar, o que resultará na exclusão do cliente do apetite de risco de crime financeiro e / ou risco de reputação do HSBC.

As linhas de negócios devem ter procedimentos (incluindo critérios de governança) e controles internos para identificar e encaminhar um cliente potencial ou existente que ela acredita estar fora do apetite de risco do Grupo HSBC.

5.7 Relacionamentos comerciais proibidos

A linha de negócio não deve iniciar ou manter um relacionamento comercial com clientes com naturezas listadas no *Global Financial Crime Policy - Policy Standards*.

Se um cliente proibido for identificado, o início ou a continuidade do relacionamento devem ser suspensos e o cliente encaminhado ao Diretor da Linha de Negócios no país e para *Compliance*.

6 MONITORAMENTO, SELEÇÃO E ANÁLISE DE OPERAÇÕES E SITUAÇÕES SUSPEITAS

6.1 Contexto

O HBBZ entende que uma das maneiras mais importantes que podem ajudar a combater crimes financeiros é o dever de todos os colaboradores, parceiros e prestadores de serviços terceirizados estarem vigilantes na identificação e escalonamento de atividades atípicas ou suspeitas.

Atividades ou comportamentos atípicos ou suspeitos podem ser identificados por uma série de métodos durante o relacionamento.

6.2 Comunicação de Operação Atípica ou Suspeita (FC-UAR)

Todos os colaboradores e prestadores de serviços terceirizados do HBBZ devem submeter um *FC-UAR* e todos os parceiros devem realizar uma denúncia por meio do *HSBC Confidencial*, quando tenham, ou acreditem ter, conhecimento de quaisquer operações ou propostas, cujas características, no que se refere às partes envolvidas, valores, formas de realização e instrumentos utilizados, ou que, pela falta de fundamento econômico ou legal, indiquem risco de ocorrência dos crimes de lavagem de dinheiro ou de financiamento ao terrorismo previstos nas regulamentações brasileira vigentes, ou com eles relacionados, ainda que não realizadas pela instituição, fornecendo indicação de envolvidos, contas ou transações etc.

6.3 Monitoramento de Transações (TM – Transaction Monitoring)

O Monitoramento de Transações (TM) é definido como a verificação retrospectiva e contínua das transações ou atividades dos clientes para identificar operações e situações que, por sua habitualidade, valor ou forma possam gerar alertas que indiquem conhecimento ou suspeita razoável de crime de lavagem de dinheiro e financiamento ao terrorismo.

O período para a execução dos procedimentos de TM não pode exceder o prazo de 45 (quarenta e cinco) dias, contados a partir da data de ocorrência da operação ou da situação, devendo o monitoramento contemplar transações que aparentem estar relacionadas com outras operações e situações conexas ou que integrem o mesmo grupo de operações.

6.4 Verificações contra Listas de Sanções e Financiamento ao Terrorismo (TS – Transaction Screening)

As verificações contra lista de sanções, financiamento ao terrorismo e a proliferação de armas de destruição em massa (TS) têm como objetivo mitigar os possíveis riscos regulatórios e de reputação associados a violações de leis e regulamentações (globais ou locais) de sanções e financiamento ao terrorismo envolvendo produtos e serviços oferecidos por meio do HBBZ, sejam elas transações domésticas em moeda local ou transações relacionadas a atividades / comércio internacional (*cross-border*).

As checagens são realizadas em tempo real para o cliente e a contraparte e demais elementos que envolvam a operação (ex. país etc) sempre antes da transação ser executada.

6.5 Sanções impostas por resoluções do Conselho de Segurança das Nações Unidas (CSNU)

As determinações de indisponibilidade de ativos decorrentes de resoluções do Conselho de Segurança das Nações Unidas (CSNU) ou de designações de seus comitês de sanções são monitoradas. Na ocorrência de um caso positivo, as comunicações são imediatamente reportadas aos órgãos competentes a indisponibilidade de ativos e as tentativas de transferências relacionadas às pessoas naturais, às pessoas jurídicas ou às entidades sancionadas.

6.6 Sanctions Name Screening

As verificações de correspondência entre nomes de indivíduos ou empresas contra lista de sanções, financiamento ao terrorismo e a proliferação de armas de destruição em massa têm como objetivo mitigar os possíveis riscos regulatórios e de reputação associados a violações de leis e regulamentações (globais ou locais) de sanções e financiamento ao terrorismo envolvendo clientes, prestadores de serviços e funcionários do HBBZ.

As checagens são realizadas diariamente contra a base de clientes, partes relacionadas e representantes legais, além dos prestadores de serviço e funcionários do HBBZ.

6.7 Comunicação de Atividade Suspeitas (SAR – Suspicious Activity Report)

O HBBZ tem a obrigação legal e regulatória de investigar o risco potencial de crime financeiro e documentar em um Relatório de Atividade Suspeita (SAR – *Suspicious Activity Report*), podendo ou não comunicar ao COAF. Apenas a área de Investigações de PLD-CFTP em *Compliance* tem acesso e alçada para comunicar um SAR. Todo SAR tem que ser aprovado pelo Diretor de PLD-CFTP antes de sua comunicação.

Os SARs são comunicados ao COAF para relatar tentativas ou transações concluídas pelo, por meio ou no HBBZ, com motivos razoáveis para suspeitar que a transação ou outra atividade envolve lavagem de dinheiro, financiamento do terrorismo ou qualquer outra atividade criminosa. Os SARs devem ser arquivados de acordo com os requisitos mínimos legais e regulatórios locais e deve ser realizado no prazo de 24 horas a contar da conclusão da análise que caracterizou a atipicidade.

6.8 Proibição de divulgação de SARs

As investigações de crimes financeiros são de natureza restrita, portanto devem ser tratadas exclusivamente com as pessoas sujeitas à necessidade de conhecimento.

7 PROCEDIMENTOS PARA CONHECER FUNCIONÁRIOS, PARCEIROS E PRESTADORES DE SERVIÇOS TERCEIRIZADOS

7.1 Contexto

O HBBZ entende que uma das maneiras mais importantes que podem ajudar a combater crimes financeiros é que todos os colaboradores, parceiros e prestadores de serviços terceirizados têm o dever de estar vigilantes na identificação e escalonamento de atividades atípicas ou suspeitas.

7.2 Conheça Seu Funcionário (KYE – Know Your Employee)

Desde a contratação dos funcionários, o HBBZ adota procedimentos para garantir aderência aos padrões de ética e conduta, e identificar eventual envolvimento em atividades ilícitas ou de lavagem de dinheiro e de financiamento do terrorismo.

Conhecer seus funcionários vai além da prevenção de fraudes contra a instituição. As fraudes, além de trazerem um prejuízo imediato em função dos recursos desviados, podem trazer sérios danos à reputação da instituição.

O processo de Conheça Seu Funcionário (KYE) tem base em procedimentos aplicados antes da contratação e de monitoramento contínuo através da observação e identificação de sinais de alerta. Além disso, em qualquer caso de

sinal de alerta identificado por qualquer funcionário do HBBZ, este deve utilizar os seguintes canais internos do HSBC para comunicar o ocorrido:

- Sinais de Alerta de má conduta ou não observância de Leis, Regulamentações, políticas internas ou procedimentos devem ser comunicados por meio do canal *HSBC Confidencial*.
- Sinais de alerta envolvendo transações e clientes com características atípicas que podem configurar fraudes, lavagem de dinheiro ou financiamento do terrorismo devem ser comunicados por meio de um FC-UAR.

7.3 Conheça Seu Parceiro e Prestador de Serviço (KYS – Know Your Supplier)

A gestão inadequada de parceiros e prestadores de serviços pode levar ao não cumprimento dos requisitos operacionais, comerciais ou ainda regulatórios que, por sua vez, podem impactar os clientes, envolver violações regulatórias, penalidades civis ou monetárias ou danos à reputação.

O HBBZ deve assegurar que todos os novos parceiros e prestadores de serviços sejam avaliados previamente à prestação de serviços e de forma continuada, em conformidade aos controles estabelecidos na política do Grupo HSBC de *Third Party Risk*.

Todos os contratos devem ter um TPEM (*Third-Party Engagement Manager*), que é a pessoa responsável pelo gerenciamento do relacionamento com o parceiro ou prestador de serviços terceirados.

A área de compras do HBBZ (*Procurement*) é a responsável por assegurar que todos os parceiros e prestadores de serviços novos e existentes tenham sido submetidos às verificações antes da assinatura do contrato

Além disso, todos os prestadores de serviço do HBBZ são submetidos a verificação diária contra listas internas e externas de nexos de sanções e de indivíduos passíveis de serem associadas a atos terroristas ou ao financiamento de terrorismo e verificação de notícias materiais adversas, para identificar eventuais mídias desabonadoras relacionadas a LD/FTP, crimes financeiros ou irregularidades semelhantes.

8 TREINAMENTO E CULTURA DE PLD-CFTP

8.1 Treinamento Mandatário

O treinamento é um elemento-chave para o gerenciamento de risco de crime financeiro e contribui para a promoção de uma forte cultura organizacional de *Compliance*. Todos os funcionários do HBBZ devem receber treinamento de conscientização de PLD-CFTP liderado pelo Grupo HSBC.

Todos os funcionários estão sujeitos a treinamento anual de PLD-CFTP e todos os novos contratados do HBBZ devem concluir o treinamento obrigatório dentro de 45 dias corridos a partir da contratação.

Todo o conteúdo dos materiais de treinamento novos e existentes deve ser revisado anualmente. A revisão deve ser conduzida por especialistas no assunto para avaliar a eficácia do treinamento de PLD-CFTP, validar se está adequado ao propósito e está de acordo com as políticas, regulamentos ou procedimentos locais mais recentes.

9 PRODUTOS E SERVIÇOS

9.1 Requerimentos Gerais

Tendo em vista o risco de crime financeiro em produtos e/ou serviços, bem como a utilização de novas tecnologias relacionadas, as linhas de negócios devem realizar análise prévia para efeitos de mitigação dos riscos associados a cada um dos produtos e/ou serviços oferecidos, os classificando, no mínimo, em baixo, médio ou alto risco. Além disso, é fundamental analisar como a forma de oferta ou a natureza do produto ou serviço podem gerar vulnerabilidades potenciais a práticas de LD/FTP e crimes financeiros semelhantes. É obrigatória a obtenção de aprovação formal de

Compliance antes do lançamento de qualquer produto e/ou serviço novo ou existente, que tenham alterações materiais significativas

A Área de PLD-CFTP dentro da estrutura de *Compliance* analisará o *design* proposto do produto e/ou serviço para determinar se os controles associados são adequados para mitigar riscos de crimes financeiros e atender aos requisitos regulatórios de PLD-CFTP.

9.2 Produtos e Serviços Proibidos

As linhas de negócios não devem oferecer produtos ou serviços que são proibidos pela Política Global de FC (detalhes estão disponíveis internamente na seção *Prohibited and Restricted Relationships and Activities* do *Global Financial Crime Policy Standards*) devido ao elevado risco de crimes financeiros.

10 AVALIAÇÃO DE EFETIVIDADE

Um dos pilares centrais desta Política é o monitoramento periódico regular para mensurar a efetividade desta Política, dos procedimentos e dos controles internos de PLD-CFTP.

O Relatório de Efetividade deve ser elaborado anualmente referente ao ano calendário anterior devendo ser encaminhado formalmente ao Comitê de Auditoria e ao *Operating Committee* (OpCo) do HBBZ, respeitando-se os prazos estabelecidos pelo regulador.

No HBBZ essa avaliação é realizada pela área de Controles Internos que é segregada da área de *Compliance* e distinta da Auditoria Interna.

11 MECANISMOS DE ACOMPANHAMENTO E CONTROLE

11.1 Compliance Assurance

A fim de demonstrar que o HBBZ possui controles apropriados para gerenciar seu risco de crime financeiro, os elementos desta Política estão sujeitos a testes realizados pela área regional de *Compliance Assurance*.

A área regional de *Compliance Assurance* se reporta ao Diretor de *Compliance* da América Latina e conduz atividades de testes com foco no gerenciamento de risco de crime financeiro nas áreas, testando controles-chave e conduzindo análises temáticas, direcionadas e customizadas para identificar lacunas ou fraquezas na estrutura de gerenciamento do risco de crime financeiro.

Eventuais deficiências ou problemas identificados são informados ao *Compliance* e aos responsáveis da área sujeita aos testes. O gerenciamento e acompanhamento das medidas de correção devem ser capturados e submetidos aos membros da Alta Administração.

11.2 Auditoria Interna

Um dos pilares centrais desta Política é o teste independente do Programa de PLD-CFTP realizado pela Auditoria Interna. A Auditoria Interna do HBBZ é uma unidade independente das demais áreas do banco e está sob a gestão do Chefe de Auditoria, que se reporta administrativamente ao Diretor-Presidente do HBBZ e funcionalmente ao Chefe Regional de Auditoria Interna da América Latina.

12. LINKS

- Global Financial Crime Policy
[Financial Crime Policy | HSBC Holdings plc](#)