



Política Externa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (PLDFTP)

Nu Pagamentos SA - Instituição de Pagamentos

Nu Financeira S.A. - Sociedade de Crédito, Financiamento e Investimento

Nu Crypto Ltda.

Nu Corretora de Seguros Ltda.

Nu Canais Ltda.

NuPay for Business Instituição de Pagamento Ltda.

Nu Asset Management Ltda.

Nu Investimentos S.A. - Corretora de Títulos e Valores Mobiliários





POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

1. Objetivo	3
2. Público Alvo	3
3. Princípios e Diretrizes	4
4. Programa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (PLDFTP)	4
4.1. Abordagem Baseada em Risco	4
4.2. Avaliação Interna De Risco e Avaliação de Efetividade	5
4.3. Processo de Conheça Seu Cliente (KYC)	5
4.4. Processo de Conheça Seu Fornecedor, Parceiro, Prestador de Serviços Relevantes e Prestador de Serviços Terceirizados (KYS/KYP)	6
4.4.1. Diretrizes de Relacionamento com fornecedores, parceiros, prestadores de serviços relevantes e prestadores de serviços terceirizados	7
4.5. Processo de Conheça Seu Funcionário (KYE)	8
4.6. Processo de Conheça Sua Transação (KYT)	8
4.7. Processo de Avaliação de Novos Produtos, Serviços, Canais, Tecnologias e Funcionalidades (NP&F+)	9
4.8. Programa de Sanções Econômicas e Bloqueio de Ativos	9
4.9. Processos de Monitoramento, Seleção, Análise e Comunicação de Operações Suspeitas (MSAC)	10
4.10. Programa de Treinamento e Aculturação em PLDFTP	10
4.11. Obrigações de Registro e Guarda de Documentos	11
5. Papéis e Responsabilidades	11
5.1. Alta Administração (Diretoria Executiva e Comitê de Auditoria)	11
5.2. Auditoria Interna	12
5.3. Área de Riscos de Crime Financeiro (FinCrime Risks)	12
5.3.1. FinCrime Risks Governance & FinCrime Risks Global Execution	12
5.3.2. Money Laundering Reporting Officer – MLRO	12
5.3.3. FinCrime Risks Analytics	13
5.4. Área de Defesas Operacionais (Ops Defense) & Área de Engenharia Cross Times em Ops Defense (Ops Engineering)	13
5.5. Área de Identidade do Cliente (Customer Identity) & Área de Prevenção à Fraudes (Fraud BU)	13
5.6. Centro de Testes de Controles Brasil (NFR Brazil Control Testing Hub)	14
5.7. Área de Aquisição de Clientes e Produtos (PF e PJ)	14
5.8. Área de Compras (Procurement)	14
5.9. Unidades de Negócio (Business Units)	14
5.10. Funcionários, estagiários e menores-aprendizes	15
6. Legislações Aplicáveis	15
7. Revisão e aprovação	16
8. Canal de Suporte	16
9. Documentos Relacionados	16
10. Controle de Revisão	16



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

1. Objetivo

Consolidar os princípios e diretrizes do Programa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (PLDFTP) do Conglomerado Nubank para promover uma cultura de integridade, ética e de PLDFTP. Espera-se que as Entidades ligadas ao Nubank definam seus direcionamentos a partir dessas orientações, considerando as necessidades específicas e os aspectos legais e regulamentares a que estão sujeitas.

Este documento busca garantir a conformidade com as legislações e regulamentações vigentes, além de se alinhar às melhores práticas nacionais e internacionais. Os critérios, requisitos, normas e procedimentos decorrentes da presente Política estão definidos em normativos internos.

2. Público Alvo

As disposições deste documento são aplicáveis às empresas do Conglomerado Nubank, membros da Alta Administração, funcionários, estagiários, menores aprendizes, parceiros, fornecedores, prestadores de serviços terceirizados, prestadores de serviços relevantes e seus respectivos colaboradores que possuem envolvimento, direto ou indireto, com o Programa de PLDFTP do Nubank.

Para fins da aplicação deste Manual, as empresas do Nubank abrangidas são: Nu Pagamentos S.A. - Instituição de Pagamento ("**Nu Pagamentos**"), a Nu Financeira S.A. - Sociedade de Crédito, Financiamento e Investimento ("**Nu Financeira**"), Nu Crypto Ltda. ("**Nu Crypto**"), Nu Corretora de Seguros Ltda. ("**Nu Corretora**"), Nu Canais Ltda. ("**Nu Canais**"), NuPay for Business Instituição de Pagamento Ltda. ("**NuPay**"), Nu Asset Management Ltda. ("**Nu Asset**") e Nu Investimentos S.A. - Corretora de Títulos e Valores Mobiliários ("**Nu Investimentos**"), aqui denominadas apenas como "Nubank", podendo contemplar também outras entidades do grupo à medida que o Nubank amplie seu escopo de atuação com novas empresas, produtos e serviços.

3. Princípios e Diretrizes

A aplicação coerente desta Política é essencial para uma gestão eficaz e robusta do risco derivado do crime financeiro dentro do Conglomerado Nubank. As Entidades ligadas ao



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

Nubank devem implementar as diretrizes aqui descritas, incluindo, mas não se limitando a, identificar e analisar o risco de LD/FT associado à utilização indevida de seus produtos e serviços.

Este documento poderá ser atualizado a qualquer momento, com o intuito de contemplar outras entidades do grupo, requerimentos legais e/ou regulatórios ou mesmo visando o aprimoramento constante dos controles e boas práticas, à medida que a instituição amplie seus negócios.

4. Programa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (PLDFTP)

O Programa de PLDFTP do Nubank estabelece o conjunto de diretrizes, controles e práticas adotados pela instituição para mitigar o risco de utilização indevida de seus produtos e serviços. Seu objetivo é assegurar conformidade com a legislação e regulamentação aplicáveis, bem como promover uma cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo.

4.1. Abordagem Baseada em Risco

As diretrizes estabelecidas nesta Política estão fundamentadas na Abordagem Baseada em Riscos ("ABR" ou "RBA" – *Risk-Based Approach*), por meio da qual a instituição direciona seus controles e diligências de forma proporcional ao nível de risco identificado. Essa proporcionalidade decorre da classificação de risco dos clientes, terceiros, funcionários, produtos, serviços, canais e demais fatores relevantes, cuja metodologia está ancorada na Avaliação Interna de Riscos ("AIR").

4.2. Avaliação Interna De Risco e Avaliação de Efetividade

O Nubank adota a Avaliação Interna de Risco ("AIR" ou "*Internal Risk Assessment - IRA*") como instrumento central de diagnóstico, integrante da metodologia corporativa de *Enterprise Risk Assessment* (ERA), com o objetivo de identificar, compreender e mensurar a exposição da instituição aos riscos de Lavagem de Dinheiro, Financiamento do Terrorismo e Proliferação de Armas de Destruição em Massa (LDFTP), aplicável a todo o conglomerado.



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

O Nubank realiza, anualmente, a Avaliação da Efetividade do programa de PLDFTP do Conglomerado, assegurando que sejam contemplados os elementos previstos nas regulamentações aplicáveis e a observância aos prazos regulamentares específicos de cada entidade supervisora. O Relatório de Efetividade inclui a metodologia utilizada, os testes aplicados, a qualificação dos avaliadores e as deficiências identificadas. As ações corretivas decorrentes são acompanhadas por meio de um Relatório de Acompanhamento, assegurando a melhoria contínua do programa.

4.3. Processo de Conheça Seu Cliente (KYC)

Trata-se de um conjunto de ações destinadas a assegurar a adequada identificação, qualificação e classificação de clientes, seus administradores, representantes e, quando aplicável, seus beneficiários finais, permitindo avaliar sua capacidade financeira e prevenir o uso indevido dos produtos e serviços. Com base em uma abordagem baseada em risco, clientes com maior exposição são submetidos a análises mais rigorosas.

I. Identificação

Processo destinado a assegurar a correta identificação do cliente. Esta etapa envolve a coleta e verificação de documentos e informações capazes de estabelecer a identidade de forma inequívoca, inclusive mediante cotejo com bancos de dados de caráter público e privado, com foco na prevenção de fraudes.

II. Verificação

Procedimento subsequente à identificação, que visa verificar a consistência, completude e a integridade das informações fornecidas pelo cliente, evitando a manutenção de registros imprecisos ou desatualizados que possam comprometer a eficácia dos controles de PLDFTP.

III. Qualificação

Processo que compreende a validação de informações adicionais sobre o cliente em bancos de dados públicos e privados, com o objetivo de aprofundar o conhecimento sobre seu perfil e características da relação de negócio, conforme exigido pela regulamentação vigente. A qualificação inclui minimamente a validação: (i) da capacidade financeira; (ii) do local de residência ou sede da empresa; (iii) da atividade profissional ou comercial; e (iv) da



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

condição de Pessoa Exposta Politicamente (PEP) ou PEP Relacionada¹. Também abrange a qualificação do beneficiário final² dos clientes pessoa jurídica.

Os procedimentos aplicáveis ao conhecimento de clientes são formalizados em documento específico aprovado pela Diretoria e mantido atualizado.

4.4. Processo de Conheça Seu Fornecedor, Parceiro, Prestador de Serviços Relevantes e Prestador de Serviços Terceirizados (KYS/KYP)

O Nubank mantém procedimentos específicos destinados a conhecer seus fornecedores, parceiros, prestadores de serviços relevantes e prestadores de serviços terceirizados.

O processo de *due diligence* contempla a verificação da condição de Pessoa Exposta Politicamente (PEP) e a checagem em listas restritivas nacionais e internacionais, tais como OFAC e Conselho de Segurança das Nações Unidas (CSNU), além da análise de integridade e de eventuais antecedentes que possam indicar riscos de envolvimento em atividades ilícitas. As diligências incluem a obtenção de informações que permitam compreender a natureza da atividade desempenhada pelo terceiro, sua reputação e licença para operar, quando aplicável.

Para os relacionamentos de maior risco, também são verificadas eventuais investigações ou ações conduzidas por autoridades supervisoras relacionadas à lavagem de dinheiro ou ao financiamento do terrorismo, bem como os controles internos adotados pelo terceiro em matéria de PLDFTP.

A classificação de risco dos terceiros segue as categorias e parâmetros definidos pela AIR, devendo ser revisitada caso ocorram mudanças relevantes em suas atividades, estrutura ou comportamento operacional.

¹ Os procedimentos de qualificação de clientes incluem a verificação da condição do cliente como Pessoas Expostas Politicamente - PEP, nos termos dos normativos legais, bem como a verificação da condição de representante, familiar e estreito colaborador dessas pessoas.

² Os procedimentos de qualificação do cliente pessoa jurídica devem incluir a análise da cadeia de participação societária até a identificação da pessoa natural caracterizada como seu beneficiário final, estabelecendo-se em 15% o valor mínimo de referência de participação societária para a identificação de beneficiário final.



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

Os procedimentos aplicáveis ao conhecimento de terceiros são formalizados em documento específico aprovado pela Diretoria e mantido atualizado.

4.4.1. Diretrizes de Relacionamento com fornecedores, parceiros, prestadores de serviços relevantes e prestadores de serviços terceirizados

Os parceiros, fornecedores, prestadores de serviços relevantes e prestadores de serviços terceirizados (doravante “terceiros”) relacionados ao Nubank devem dispor de um programa de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (PLD/FTP) que atenda a todos os requisitos legais e regulatórios aplicáveis ao negócio e/ou à relação comercial, alinhado, sem se limitar, aos aspectos aqui descritos.

Quando aplicável, os parceiros, fornecedores e prestadores de serviços terceirizados e relevantes do Nubank devem conhecer seus clientes desde o início do relacionamento de negócios, observando os requisitos mínimos de cadastro definidos na legislação e regulamentação vigentes; tais diligências devem contemplar a coleta, verificação, validação, atualização e manutenção dos registros das respectivas informações cadastrais, armazenadas pelos prazos exigidos na legislação aplicável, inclusive após o término do relacionamento com o cliente.

Os terceiros devem seguir os mesmos padrões de controle adotados pelo Conglomerado Nubank e dispor de procedimentos formais de *screening* para evitar o início ou a manutenção de relacionamento com indivíduos ou entidades constantes de listas restritivas de sanções.

Assim como o Nubank, seus parceiros, fornecedores e prestadores de serviços terceirizados e relevantes devem possuir políticas e procedimentos para o monitoramento, seleção, análise e comunicação de operações e situações suspeitas às autoridades competentes e, quando aplicável e/ou necessário, ao time responsável por PLD/FTP do Nubank.

Os terceiros devem também dispor de políticas e/ou procedimentos destinados a conhecer seus colaboradores, fornecedores, prestadores de serviços e parceiros comerciais para fins de PLD/FTP, bem como promover ações de treinamento e comunicação contínuas para a capacitação de seus colaboradores em temas de PLD/FTP, em conformidade e alinhamento com o Programa de PLD/FTP do Nubank.

Os procedimentos aplicáveis devem ser formalizados em documento(s) específicos, aprovados pela alta administração do terceiro e mantidos atualizados; os registros das diligências e das decisões tomadas devem ser arquivados pelo prazo legalmente exigido.



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

A celebração e manutenção de contratos entre o Nubank e terceiros deve prever cláusulas que assegurem o cumprimento das presentes diretrizes, cabendo ao Nubank o direito de avaliar e monitorar a aderência dos terceiros às exigências previstas no Programa de PLD/FTP.

4.5. Processo de Conheça Seu Funcionário (KYE)

O processo de Conheça Seu Funcionário (KYE) do Conglomerado Nubank, para fins de PLDFTP, estabelece diligências obrigatórias destinadas a conhecer os funcionários da instituição.

O Programa contempla tanto o momento de contratação quanto a manutenção do vínculo empregatício e compreende procedimentos formais de identificação e qualificação dos funcionários, compatíveis com a Política de PLDFTP e com a Avaliação Interna de Risco (AIR).

As diligências incluem a realização de *screening* durante o processo de contratação e manutenção do relacionamento, com a finalidade de identificar potenciais riscos relacionados a mídias negativas, sanções e condição de Pessoa Exposta Politicamente (PEP).

Os procedimentos aplicáveis ao conhecimento de funcionários são formalizados em documento específico aprovado pela Diretoria e mantido atualizado.

4.6. Processo de Conheça Sua Transação (KYT)

O Nubank adota controles específicos para o monitoramento, avaliação e mitigação dos riscos associados a transações envolvendo criptoativos e outros ativos virtuais. Esses controles seguem padrões internacionais de governança, as recomendações do GAFI e Resolução 520/2025 do Banco Central do Brasil, bem como demais regulamentações aplicáveis, assegurando a rastreabilidade, integridade e transparência das operações.

Os parâmetros de monitoramento e critérios de risco aplicáveis ao processo são formalizados em documento específico aprovado pela Diretoria e mantido atualizado.



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

4.7. Processo de Avaliação de Novos Produtos, Serviços, Canais, Tecnologias e Funcionalidades (NP&F+)

O conglomerado Nubank adota processo estruturado para avaliar, sob a ótica de PLDFTP, todo novo produto, serviço, canal, tecnologia, funcionalidade ou alteração relevante antes de sua implementação. Essa avaliação, integrada ao processo corporativo de *New Products & Features* (Novos Produtos e Funcionalidades ou "NP&F+"), assegura que potenciais riscos, lacunas de controle ou impactos regulatórios sejam identificados e mitigados tempestivamente, em alinhamento com a ABR da instituição.

4.8. Programa de Sanções Econômicas e Bloqueio de Ativos

O Nubank mantém o compromisso de vetar o início ou a continuidade de qualquer relacionamento com indivíduos ou entidades incluídos em listas internacionais de sancionados, alinhado aos requerimentos vigentes, sejam clientes, funcionários, parceiros, prestadores de serviços ou fornecedores. Isso abrange a verificação na lista do *Office of Foreign Assets Control* (OFAC) dos Estados Unidos da América e a lista do Conselho de Segurança das Nações Unidas (CSNU), bem como outras listas consideradas relevantes.

Além disso, o Nubank não estabelece relações de negócios com países ou regiões sujeitos a sanções e embargos constantes das listas internacionais emitidas pela OFAC, assim como aquelas jurisdições classificadas como *High-Risk Jurisdictions subject to a Call for Action* pelo Grupo de Ação Financeira Internacional (GAFI).

Nos casos em que forem identificadas propostas de relacionamentos por pessoas físicas ou entidades listadas pelo CSNU, além de negar o relacionamento, deverão ser realizados os reportes obrigatórios ao Coaf, ao Ministério da Justiça e Segurança Pública (MJSP) e aos órgãos reguladores (BCB, CVM, Susep). Da mesma forma, quando detectado que um cliente ativo passou a constar em lista do CSNU, além do reporte às autoridades competentes, todos os ativos financeiros, virtuais (criptoativos) ou não financeiros relacionados ao cliente deverão ser imediatamente bloqueados e segregados. Caso o cliente não possua ativos, o relacionamento deverá ser encerrado conforme os procedimentos internos aplicáveis.

4.9. Processos de Monitoramento, Seleção, Análise e Comunicação de Operações Suspeitas (MSAC)



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

O Nubank implementa procedimentos de monitoramento, seleção e análise de operações e situações com o objetivo de identificar, avaliar e dispensar especial atenção àquelas que possam configurar suspeitas de lavagem de dinheiro ou financiamento do terrorismo, em conformidade com os requisitos previstos na regulamentação aplicável. Tais procedimentos abrangem não apenas operações efetivamente realizadas, mas também propostas de operações.

O período máximo para execução dos procedimentos de monitoramento e seleção não deve exceder 45 dias a partir da data da operação ou situação que apresente indícios de atipicidade e os sistemas utilizados deverão manter informações detalhadas das operações, das partes envolvidas e dos parâmetros aplicados, devendo ser passíveis de verificação quanto à adequação e efetividade.

As instituições do conglomerado conduzem a análise das operações e situações selecionadas, com o objetivo de caracterizá-las ou não como suspeitas de LDFTP, observando:

- prazo máximo de 45 dias contados da seleção da operação ou situação;
- formalização da análise em dossiê, independentemente de posterior comunicação ao Coaf.

Após a conclusão da análise de operações, situações ou propostas de operações que apresentem indícios de lavagem de dinheiro ou financiamento do terrorismo, o Nubank deve proceder com a comunicação ao Coaf, quando aplicável.

Os procedimentos e fluxos aplicáveis encontram-se descritos em documento devidamente aprovado pela Diretoria

4.10. Programa de Treinamento e Aculturação em PLDFTP

O Nubank mantém um Programa de Treinamento e Aculturação em PLDFTP com o objetivo de assegurar que todos os públicos relevantes compreendam suas responsabilidades na prevenção, detecção e mitigação de riscos relacionados à lavagem de dinheiro, financiamento do terrorismo e proliferação de armas de destruição em massa.

O cumprimento dos treinamentos mandatórios, bem como a observância das políticas, procedimentos e diretrizes de PLDFTP, é obrigatório para todos os públicos abrangidos por esta Política.



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

4.11. Obrigações de Registro e Guarda de Documentos

O Nubank mantém, em conformidade com as regulamentações aplicáveis, sistemas e repositórios dedicados ao registro e à guarda das informações coletadas nos procedimentos de identificação, qualificação e atualização cadastral. Esses dados são armazenados pelo período mínimo de 10 (dez) anos, contado inclusive a partir do primeiro dia do ano subsequente ao encerramento do relacionamento, permanecendo disponíveis para consulta mediante registros internos.

No mesmo período, são igualmente conservadas as informações obtidas nos processos de verificação e diligência aplicáveis a funcionários, parceiros, fornecedores, prestadores de serviços terceirizados e demais terceiros relevantes, conforme requerido pelos normativos vigentes.

O Nubank assegura, ainda, que todas as transações, informações e registros associados às atividades de PLDFTP e Sanções sejam devidamente documentados e mantidos pelos prazos regulamentares. Isso inclui, entre outros, os alertas gerados, os históricos de análise, as evidências consideradas e os pareceres que fundamentam as conclusões adotadas.

5. Papéis e Responsabilidades

5.1. Alta Administração (Diretoria Executiva e Comitê de Auditoria)

- Aprovar e tomar ciência das Políticas e dos relatórios de PLDFTP (incluindo AIR/RAIR e Relatórios de Efetividade) e acompanhar planos de ação;
- Garantir a integridade das demonstrações financeiras, o cumprimento das obrigações legais e regulatórias, a independência e qualidade das auditorias e eficácia dos controles internos e do gerenciamento de riscos;
- Definir, monitorar e revisar indicadores e iniciativas de PLDFTP (clientes, operações, produtos/serviços, KYC e metodologias aplicáveis);
- Assegurar que a política esteja alinhada ao modelo de negócio e aos requisitos regulatórios;

5.2. Auditoria Interna



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

- Realizar avaliações independentes periódicas das atividades de PLDFTP, reportar resultados às instâncias de governança e acompanhar a implementação das recomendações.
- Monitorar a implementação de planos de ação provenientes de Auditorias Internas, inspeções regulatórias, Avaliação de Efetividade e Ofícios Regulatórios.

5.3. Área de Riscos de Crime Financeiro (FinCrime Risks)

5.3.1. FinCrime Risks Governance & FinCrime Risks Global Execution

- Manter políticas, procedimentos e padrões (incluindo AIR/ABR) de PLDFTP atualizados e alinhados à regulamentação e às melhores práticas do mercado;
- Definir processos e controles para prevenir, detectar e reportar transações/situações suspeitas;
- Avaliar novos produtos, serviços e funcionalidades sob a ótica de PLDFTP, mantendo evidências;
- Mapear e tratar pontos de melhoria com planos de ação e prazos;
- Garantir a execução do Programa de Avaliação de Efetividade compatível com a Política e com a AIR.
- Desenvolver programas de capacitação e monitorar suas métricas.
- Formalizar, disseminar e atualizar a Política Global de PLD/CFT e Sanções;
- Avaliar a adesão dos países, identificar lacunas e recomendar melhorias locais;
- Reportar periodicamente o andamento do Programa à liderança e aos fóruns de governança.

5.3.2. Money Laundering Reporting Officer – MLRO

- Supervisionar análise e reporte de alertas e deliberar sobre comunicações de operações suspeitas quando delegado;
- Garantir comunicações ao órgão regulador dentro dos prazos e comunicações de não ocorrência quando exigido;
- Assegurar registros das análises e decisões (reporte ou arquivamento);
- Produzir relatórios gerenciais para o Diretor responsável.

5.3.3. FinCrime Risks Analytics



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

- Desenvolver, parametrizar, ajustar e implementar regras de monitoramento/seleção conforme novas tipologias.
- Definir e aplicar políticas para modelos de machine learning; manter e monitorar modelos de classificação de risco.
- Garantir a integridade dos dados utilizados para monitoramento e seleção.
- Monitorar modelo de classificação de risco e manter modelos de *machine learning*.

5.4. Área de Defesas Operacionais (Ops Defense) & Área de Engenharia Cross Times em Ops Defense (Ops Engineering)

- Identificar e reportar situações suspeitas (cadastro, documentação, comportamento transacional) conforme critérios internos;
- Realizar verificações em listas restritivas e validação de PEPs (titulares e relacionados), além de conduzir pesquisas de mídia negativa;
- Garantir atuação contínua nas filas operacionais regulatórias sob responsabilidade da área;
- Desenvolver, manter e aprimorar fluxos operacionais sistêmicos de Ops Defense conforme diretrizes de FinCrime Risks e AML Analytics;
- Documentar análises, decisões e classificações de risco, mantendo evidências em conformidade com requisitos regulatórios e internos;
- Escalar casos de alto risco ou com indícios de PLDFTP às áreas de risco competentes e executar encerramentos de relacionamento quando orientado;
- Criar, revisar e implementar procedimentos de primeira linha para assegurar aderência regulatória e consistência dos controles;
- Implementar melhorias solicitadas e prestar suporte técnico/transversal entre times.
- Participar e promover treinamentos periódicos para manter e atualizar competências.

5.5. Área de Identidade do Cliente (Customer Identity) & Área de Prevenção à Fraudes (Fraud BU)

- Sanitizar e validar dados cadastrais após aquisição, assegurando completude, acurácia e atualização.
- Viabilizar e controlar fluxos de atualização cadastral pelos clientes; aplicar restrição de navegação no app para clientes que não completam o fluxo.
- Implementar e manter controles robustos de validação de identidade para prevenção a fraudes.



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

- Desenvolver e acompanhar indicadores para monitorar sanitização, verificação, atualização cadastral e eficácia das medidas antifraude.
- Reportar tempestivamente ao Diretor responsável por PLDFTP e ao Financial Crime Risks Fórum sobre fragilidades ou incidentes relevantes; reportar potenciais casos de LDFTP ao time de Ops Defense.
- Garantir armazenamento e guarda das evidências de verificação, validação e atualização cadastral por, no mínimo, 10 anos a contar do primeiro dia do ano seguinte ao término do relacionamento com o cliente.

5.6. Centro de Testes de Controles Brasil (NFR Brazil Control Testing Hub)

- Aplicar testes periódicos e a Avaliação de Efetividade anual para verificar aderência e eficácia dos controles;
- Registrar e acompanhar planos de ação e validar evidências junto aos times afetados.

5.7. Área de Aquisição de Clientes e Produtos (PF e PJ)

- Conduzir onboarding seguro e compliance de KYC/KYB (identificação, qualificação e classificação), garantir fluxo diligente de cadastro e avaliar/mitigar riscos de novos produtos, serviços e canais em coordenação com FinCrime Risks.

5.8. Área de Compras (Procurement)

- Cadastrar e manter informações de fornecedores/terceiros (incluindo beneficiários finais), categorizar para *due diligence*, realizar *screening* (PEP, mídias negativas, sanções), reportar hits a FinCrime Risks Governance, cumprir diligências das circulares do BCB e arquivar evidências por no mínimo 5 anos.

5.9. Unidades de Negócio (Business Units)

- Cadastrar e atualizar parceiros e prestadores relevantes (incluindo beneficiários finais), categorizar para *due diligence*, executar *screening* (PEP, mídias negativas, sanções), reportar hits a FinCrime Risks Governance, cumprir diligências aplicáveis e manter evidências por pelo menos 5 anos.



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

5.10. Funcionários, estagiários e menores-aprendizes

- Atuar conforme o Programa PLDFTP e regulamentação;
- Cumprir treinamentos obrigatórios;
- Reportar suspeitas ao time de Ops Defense;
- Manter sigilo e não alertar clientes sobre investigações.

6. Legislações Aplicáveis

Esta Política e as atividades aqui previstas devem seguir as disposições de:

- Lei 9.613/1998 (alterada pela 12.683/2012)
- Resolução 96/2021 do Banco Central do Brasil
- Circular 3.978/2020 do Banco Central do Brasil
- Carta Circular 4.001 do Banco Central do Brasil
- Lei 13.260/2016
- Lei 13.810/2019
- Decreto no 9.825/2019
- Lei Federal Complementar nº 105/2001
- Instrução Normativa nº 5/2020, na forma dos arts. 10, IV, e 14, § 1o, da Lei nº 9.613/1998.
- Resolução 44/2020 do Banco Central do Brasil
- Resolução Conjunta nº 6 do Banco Central do Brasil
- Instrução Normativa BCB nº 262
- Resolução 131/2021, do Banco Central do Brasil
- Resolução 35/2021 da Comissão de Valores Mobiliários (CVM)
- Resolução 50/2021 da Comissão de Valores Mobiliários (CVM)
- Resolução 520/2025 do Banco Central do Brasil
- Instrução Normativa 2.291/2025 da Receita Federal do Brasil
- Ofício Circular 04/2020, da Comissão de Valores Mobiliários
- Ofício Circular 03/2019, da Comissão de Valores Mobiliários
- Circular 612/2020 da Susep
- Guia ANBIMA de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa
- Resolução BCB 265/22 do Banco Central do Brasil
- Recomendações do *Financial Action Task Force* - Grupo de Ação Financeira (GAFI)
- Decreto 3.976/2001
- Decreto 5.640/2005



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

7. Revisão e aprovação

Esta Política deve ser aprovada pelos Diretores Estatutários da Empresa e mantida atualizada em decorrência de alterações em regulamentos e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos do Nubank.

8. Canal de Suporte

O Nubank disponibiliza o endereço amlgovernance@nubank.com.br para o recebimento de denúncias relacionadas a comportamentos atípicos, além de esclarecimento de dúvidas ou solicitação de suporte referente às diretrizes desta Política.

9. Documentos Relacionados

- Política Global de PLDFTP;
- Política Interna de PLDFTP;
- Avaliação Interna de Riscos do Nubank;
- Abordagem Baseada em Risco da Nu Investimentos;
- Manual de KYC do Nubank;
- Manual de Procedimentos de KYC do Nubank;
- Manual de KYE do Nubank;
- Manual de KYP/KYS do Nubank;
- Manual de KYT do Nubank;
- Manual de Monitoramento e Seleção do Conglomerado;
- Manual de Análise e Comunicação do Conglomerado.

10. Controle de Revisão

Revisão	Data	Descrição da alteração
01	12/2021	Versão inicial
02	01/2023	Adaptação ao novo layout de Políticas Corporativas e revisão do escopo de abrangência.
03	04/2024	Revisão geral do texto, ajuste do Glossário e dos Papéis e Responsabilidades.



POLÍTICA CORPORATIVA NÍVEL 2

POLÍTICA EXTERNA DE PREVENÇÃO À LAVAGEM DE DINHEIRO, AO FINANCIAMENTO DO TERRORISMO E À PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Vigência: Dezembro de 2021

Última revisão: Março de 2026

04	03/2026	• Atualização do objetivo do documento, ampliando seu escopo para alinhar-se às diretrizes externas do Programa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (PLDFTP), em substituição ao enfoque anterior restrito à política de PLD voltada exclusivamente a terceiros. • Inclusão do item 4 — Programa de Prevenção à Lavagem de Dinheiro, ao Financiamento do Terrorismo e à Proliferação de Armas de Destruição em Massa (PLDFTP) — e de seus respectivos subitens. • Incorporação das diretrizes de relacionamento com fornecedores, parceiros, prestadores de serviços relevantes e prestadores de serviços terceirizados, estabelecendo requisitos e procedimentos aplicáveis. • Revisão e atualização dos papéis e responsabilidades, com detalhamento das atribuições e responsabilidades das áreas envolvidas.
----	---------	--

Criado por: FinCrime Risks Governance	Revisado por: FinCrime Risks Governance	Aprovado por: Diretoria de PLD
Data: Dezembro de 2021	Data: Março de 2026	Data: Março de 2026

Nível de Confidencialidade: Público