POLÍTICA DE PREVENÇÃO DE BRANQUEAMENTO DE CAPITAIS, FINANCIAMENTO DO TERRORISMO E FINANCIAMENTO DA PROLIFERAÇÃO DE ARMAS DE DESTRUIÇÃO EM MASSA

Elaborado por	Maria João Dias – RCN|CCO
Destinatário fina	Toda a estrutura da IFTHENPAY, Lda.
Requisito legal	Artigos 11.º, 14.º e 15.º da Lei n.º 83/2017, de 18 de Agosto Aviso do Banco de Portugal N.º 1/2022
Objectivo	Actualização da Política de Prevenção de Branqueamento de Capitais e Financiamento do Terrorismo
Versão	2026_01

CONTROLO DE VERSÕES

Versão	Data	Elaboração	Aprovação	Entrada em vigor	Observações
01	12/07/2012	Filipe Moura	Gerência	12/07/2012	Versão Inicial
02	07/07/2017	Filipe Moura	Gerência	07/07/2017	Atualização
03	23/11/2019	Filipe Moura e Sandra Guimarães	Gerência	13/12/2019	Atualização
04	25/06/2020	Filipe Moura e Sandra Guimarães	Gerência	25/06/2020	Atualização
05	14/10/2020	Maria João Dias	Gerência	14/10/2020	Atualização
06	21/01/2021	Maria João Dias	Gerência	21/01/2021	Atualização
2022_01	01/02/2022	Maria João Dias	Gerência	01/02/2022	Reestruturação
2023_01	01/02/2023	Maria João Dias	Gerência	01/02/2023	Atualização
2024_01	18/07/2024	Maria João Dias	Gerência	18/07/2024	Atualização
2025_01	10/07/2025	Maria João Dias	Gerência	10/07/2025	Atualização
2026_01	02/12/2025	Maria João Dias	Gerência	23/02/2026	Atualização

ÍNDICE

PREÂMBULO

A IFTHENPAY, Lda. (adiante "IFTHENPAY"), enquanto Instituição de Pagamento autorizada e supervisionada pelo Banco de Portugal, assume o compromisso firme de adoptar elevados padrões de integridade, transparência e responsabilidade no exercício da sua atividade. Este compromisso traduz-se na adoção de uma Política de Prevenção do Branqueamento de Capitais, Financiamento do Terrorismo e Financiamento da Proliferação de Armas de Destruição em Massa (doravante "Política"), que consagra práticas robustas, proporcionais ao risco e plenamente alinhadas com o ordenamento jurídico e regulamentar aplicável.

A crescente complexidade dos serviços financeiros e tecnológicos, bem como a predominância de relações de negócio estabelecidas à distância, tornam as instituições de pagamento especialmente expostas a tentativas de utilização indevida para fins ilícitos. Assim, a Política visa dotar a IFTHENPAY de um quadro normativo claro, coerente e eficaz para prevenir a instrumentalização dos seus serviços em esquemas de branqueamento de capitais, financiamento do terrorismo ou financiamento da proliferação de armas de destruição em massa.

A Política consolida e substitui documentos internos anteriores, integrando num único instrumento as regras, princípios e procedimentos essenciais ao cumprimento dos deveres preventivos do branqueamento de capitais, do financiamento do terrorismo e da proliferação de armas de destruição em massa, em conformidade com:

- A Lei n.º 83/2017, de 18 de agosto, na redação atualmente em vigor;
- A Lei n.º 97/2017, de 23 de Agosto, na redação atualmente em vigor;
- O Aviso do Banco de Portugal n.º 1/2022;
- O Aviso do Banco de Portugal n.º 3/2020, no que respeita a governo interno;
- As Diretivas Europeias Anti-Branqueamento (AMLD);
- As Recomendações do Grupo de Ação Financeira (GAFI/FATF);
- Os Regulamentos da União Europeia aplicáveis;
- As melhores práticas setoriais aplicáveis às instituições de pagamento em matéria de prevenção do BCFT.

A Política assenta nos seguintes princípios estruturantes:

a. *Abordagem baseada no risco* (Risk-Based Approach) – permitindo alocar recursos e controlos proporcionais ao risco identificado em cada relação de negócio, produto, canal ou geografia.
b. *Rastreabilidade* e documentação completa das decisões – garantindo que todas as decisões, verificações e análises ficam devidamente registadas, assegurando transparência e auditabilidade.
c. *Proporcionalidade* entre controlo e risco – compatibilizando exigências legais com a natureza, dimensão e complexidade operacional da IFTHENPAY.
d. *Governação interna* eficaz e responsável – assegurando que as funções de controlo interno atuam de forma independente, coordenada e dotadas de recursos adequados.

e. *Cultura organizacional* orientada para a conformidade – promovendo um ambiente ético, profissional e preventivo, assente na formação contínua e na diligência individual de todos os colaboradores.

f. *Cooperação* com autoridades competentes – garantindo a disponibilização célere, completa e rigorosa de informação sempre que requerida por entidades de supervisão ou investigação.

A presente Política é obrigatória para todos os colaboradores, dirigentes, prestadores de serviços e quaisquer pessoas que atuem em nome ou por conta da IFTHENPAY, independentemente da natureza do vínculo contratual. A sua observação plena é essencial para garantir a confiança no sistema financeiro e assegurar o cumprimento das obrigações legais e regulamentares da IFTHENPAY.

A Política é revista anualmente — ou sempre que alterações legislativas, regulamentares ou operacionais o justifiquem — e entra em vigor após aprovação pela Gerência.

INFORMAÇÃO INSTITUCIONAL

a. Identificação

A IFTHENPAY, Lda. é uma entidade privada, constituída ao abrigo da legislação portuguesa, registada sob o número de pessoa coletiva 510 450 024, com sede na Rua do FeiraPark, n.º 50, Edf. FeiraPark, Ala Esquerda do Rés-do-Chão, 4520-632 São João de Ver, Portugal.

A IFTHENPAY encontra-se autorizada pelo Banco de Portugal a exercer a sua atividade enquanto Instituição de Pagamento, estando inscrita no Registo de Instituições de Pagamento do Banco de Portugal sob o n.º 8707.

A autorização foi concedida nos termos do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo Decreto-Lei n.º 91/2018, de 12 de novembro (doravante "RJSPME"), e respetiva regulamentação complementar.

b. Natureza jurídica e atividade exercida

A IFTHENPAY é uma sociedade por quotas de direito português, cuja atividade principal consiste na prestação de serviços de pagamento, enquadrados no Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica.

No âmbito da autorização concedida pelo Banco de Portugal, a IFTHENPAY encontra-se habilitada a disponibilizar soluções de pagamentos destinadas a comerciantes e outras entidades que exerçam atividades económicas legalmente permitidas, assegurando a execução e o processamento de operações de pagamento de forma segura, transparente e conforme com os requisitos legais e regulamentares aplicáveis.

A atividade da IFTHENPAY é desenvolvida através de processos integralmente digitais, assentando numa arquitetura tecnológica própria e em procedimentos não presenciais para o estabelecimento de relações de negócio e prestação de serviços.

c. Órgãos sociais

A IFTHENPAY dispõe dos órgãos sociais legalmente previstos para sociedades por quotas, responsáveis pela administração, deliberação e fiscalização da sociedade, nos termos do Código das Sociedades Comerciais e demais legislação aplicável.

Gerência

A Gerência é composta por **dois gerentes**, designados nos termos do contrato de sociedade, aos quais compete a administração e representação legal da IFTHENPAY.

A forma de obrigar a sociedade consiste na intervenção conjunta de dois gerentes ou na intervenção de um gerente juntamente com um procurador com poderes bastante especificados.

Compete à Gerência:

- assegurar a direção estratégica e a administração da sociedade;
- aprovar as políticas internas, incluindo a presente Política;

- supervisionar todas as funções de controlo interno (Gestão de Risco, Cumprimento Normativo e Compliance, e Auditoria Interna);
- garantir a afetação adequada de recursos humanos, técnicos e financeiros;
- assegurar a governação e o cumprimento das obrigações legais, regulamentares e contratuais.

A Gerência é a direção de topo para efeitos das obrigações previstas na Lei n.º 83/2017 e no Aviso do Banco de Portugal n.º 3/2020.

Assembleia de Sócios

A Assembleia de Sócios é o órgão deliberativo máximo, competindo-lhe, nos termos da lei e do contrato de sociedade:

- aprovar o relatório e contas e demais documentos de prestação de contas;
- deliberar alterações ao contrato de sociedade;
- designar e destituir os membros da Gerência;
- deliberar aumentos de capital e matérias estruturantes da sociedade.

As quotas da IFTHENPAY são atualmente detidas por três sócios:

- PAYTEN Holding S.A., titular de uma quota no valor de €240.000,00;
- Nuno André Coutinho Freitas Brêda, titular de uma quota no valor de €30.000,00;
- Carlos Filipe Quintas Moura, titular de uma quota no valor de €30.000,00.

O capital social da IFTHENPAY é de €300.000,00, encontrando-se integralmente subscrito e realizado.

Órgão de Fiscalização / Fiscal Único

A IFTHENPAY dispõe de Revisor Oficial de Contas (ROC), atuando como Fiscal Único externo, conforme previsto no Código das Sociedades Comerciais e refletido na estrutura organizacional oficial.

Compete ao Fiscal Único:

- fiscalizar a gestão da sociedade;
- proceder à revisão legal das contas;
- emitir parecer sobre o relatório e contas anual;
- supervisionar a adequação dos sistemas de controlo interno;
- acompanhar relatórios e atividades das funções internas de controlo (RCN, Compliance, Gestão de Risco).

Auditoria Interna

A IFTHENPAY, enquanto instituição de pagamento sujeita ao regime de governo interno e de controlo interno aplicável às entidades supervisionadas pelo Banco de Portugal, está obrigada a dispor de uma função de auditoria interna independente.

Atendendo à sua dimensão e modelo de negócio, a IFTHENPAY optou por externalizar a função de Auditoria Interna, contratando um prestador externo especializado para o exercício destas funções, cuja atividade se iniciará em março de 2026.

A Auditoria Interna atua como terceira linha de defesa, com independência funcional, reportando diretamente à Gerência, competindo-lhe, nomeadamente:

- Avaliar a adequação e eficácia dos sistemas de governo interno e de controlo interno, incluindo o sistema de prevenção do BCFT;
- Realizar revisões temáticas e testes de eficácia, conformidade e qualidade;
- Emitir recomendações e acompanhar a implementação das ações corretivas acordadas com a Gerência;
- Assegurar a existência de um mecanismo formal, documentado e periódico de validação do cumprimento das obrigações legais e regulamentares em matéria de BCFT e demais domínios relevantes.

Até à entrada em funcionamento da Auditoria Interna externa, a IFTHENPAY assegura mecanismos de monitorização proporcionais à sua dimensão e complexidade, incluindo revisões periódicas documentais, acompanhamento pelo Fiscal Único e supervisão direta da Gerência sobre as funções de controlo interno.

d. Supervisão setorial

A IFTHENPAY é supervisionada pelo Banco de Portugal, autoridade competente para acompanhar e fiscalizar a atividade das instituições de pagamento. A IFTHENPAY encontra-se sujeita à supervisão prudencial, comportamental e de prevenção do branqueamento de capitais e do financiamento do terrorismo, abrangendo, designadamente, matérias de governo interno, controlo interno, prestação de serviços de pagamento e cumprimento das obrigações legais e regulamentares aplicáveis.

e. Contactos oficiais

Para efeitos institucionais, regulamentares ou de comunicação com autoridades competentes, a IFTHENPAY disponibiliza os seguintes contactos oficiais:

- Endereço da sede:

Rua do FeiraPark, n.º 50
Edf. FeiraPark, Ala Esquerda do Rés-do-Chão
4520-632 São João de Ver, Portugal

- Correio eletrónico institucional: ifthenpay@ifthenpay.com
- Website oficial: www.ifthenpay.com
- Contacto telefónico geral: (+351) 256 245 560

Contactos específicos das funções de controlo interno — nomeadamente, do Responsável pelo Cumprimento Normativo, da função de Compliance e da Gestão de Risco — poderão ser disponibilizados às autoridades competentes sempre que legalmente exigido ou mediante pedido fundamentado.

f. Estrutura organizacional relevante para BCFT

A estrutura organizacional da IFTHENPAY integra diversas funções com responsabilidades diretas ou indiretas na prevenção do branqueamento de capitais e do financiamento do terrorismo, assegurando a separação e articulação adequadas entre as linhas de defesa, em conformidade com o Aviso do Banco de Portugal n.º 3/2020.

As funções relevantes para efeitos da presente Política incluem:

Gerência
Órgão de direção de topo, responsável pela supervisão global da atividade e pela aprovação das políticas internas, incluindo a Política de Prevenção de BCFT, bem como pela garantia de existência de recursos adequados ao seu cumprimento.

Responsável pelo Cumprimento Normativo (RCN)
Função autónoma de segunda linha, com responsabilidade de supervisão do cumprimento das obrigações legais e regulamentares aplicáveis. O RCN reporta diretamente à Gerência, assegurando independência funcional e acesso direto à direção de topo.

Compliance Officer (CO)
Função operacional de segunda linha responsável pela execução dos controlos de BCFT, pela monitorização diária e pela análise inicial de situações de risco ou suspeição, atuando sob a orientação funcional do RCN e mantendo contacto direto com a Gerência quando necessário.

Gestão de Risco (GR)
Função de segunda linha dedicada à identificação, avaliação e monitorização dos riscos inerentes e residuais, incluindo os riscos de BCFT, reportando os resultados da sua atividade à Gerência de forma regular e sempre que solicitado.

Auditoria Interna
Função assegurada por prestador externo, com início previsto para março de 2026, constituindo a terceira linha de defesa responsável pela avaliação independente da eficácia do sistema de controlo interno e da aplicação da Política, reportando diretamente à Gerência.

Equipas Operacionais
Primeira linha de defesa, responsáveis por aplicar os procedimentos de onboarding, identificação, verificação documental, monitorização transacional e demais atividades previstas na Política, sob supervisão das funções de controlo interno.

A estrutura organizacional assegura a necessária segregação de funções, independência das linhas de defesa e clareza nas responsabilidades e nos fluxos de reporte. A IFTHENPAY adota medidas adequadas para prevenir conflitos de interesses internos e garantir que todas as funções críticas dispõem da autonomia operacional necessária ao cumprimento das suas obrigações.

I. GOVERNANÇA, ORGANIZAÇÃO INTERNA E ESTRUTURA DE CONTROLO INTERNO

1.1 Gerência

A Gerência constitui o órgão de direção de topo da IFTHENPAY, sendo *responsável pela administração efetiva da instituição, pela definição da sua estratégia e pela supervisão global das funções críticas, incluindo o sistema de prevenção do branqueamento de capitais e do financiamento do terrorismo*. Compete-lhe assegurar que a atividade é conduzida de forma prudente, transparente e em conformidade com as obrigações legais e regulamentares aplicáveis, promovendo uma cultura organizacional assente na legalidade, na ética e na prevenção do risco.

No âmbito das suas responsabilidades, a Gerência *aprova a presente Política e demais políticas internas relevantes*, assegurando a existência de um sistema de controlo interno adequado à natureza, dimensão e complexidade da atividade. *Supervisiona a implementação e a eficácia desses controlos*, acompanhando a identificação, avaliação e mitigação dos riscos de BCFT a que a IFTHENPAY esteja exposta, e *intervém sempre que necessário na validação de decisões estratégicas*, incluindo as relacionadas com clientes ou situações classificadas como de risco elevado.

A Gerência é igualmente *responsável por garantir a afetação de recursos humanos, técnicos e financeiros suficientes para o cumprimento das obrigações legais e regulamentares*, assegurando a independência e autonomia operativa das funções de controlo interno, nomeadamente o Responsável pelo Cumprimento Normativo, o Compliance Officer e a Gestão de Risco. Cabe-lhe ainda *promover a existência de mecanismos eficazes de formação e sensibilização*, assegurando que todos os colaboradores compreendem e aplicam as suas responsabilidades no âmbito da prevenção do BCFT.

Em todas as circunstâncias, a Gerência deve atuar de forma diligente e prudente, *garantindo a solidez do sistema de governo interno* e conduzindo a atividade da IFTHENPAY em estrito respeito pelas exigências legais, regulamentares e éticas inerentes à sua qualidade de instituição de pagamento supervisionada. A Gerência assume, em última instância, a *responsabilidade pela integridade, eficácia e permanente adequação do sistema de prevenção do BCFT* implementado na IFTHENPAY.

1.2 Responsável pelo Cumprimento Normativo (RCN)

O Responsável pelo Cumprimento Normativo (RCN) é a função de segunda linha encarregue de *assegurar, de forma autónoma e contínua, a verificação do cumprimento das obrigações legais, regulamentares e internas aplicáveis à atividade da IFTHENPAY*, em especial no que concerne às matérias relativas à prevenção do branqueamento de capitais e do financiamento do terrorismo. O RCN exerce as suas funções com *independência operacional e acesso direto à Gerência, reportando-lhe com a periodicidade necessária para garantir a eficácia do sistema de controlo interno e a pronta identificação de riscos emergentes*.

Compete ao RCN *avaliar, de forma sistemática, a adequação e a eficácia das políticas, procedimentos e controlos implementados*, assegurando que estão alinhados com as exigências legais e regulamentares aplicáveis às instituições de pagamento. No âmbito das

suas responsabilidades, o RCN *promove a atualização da presente Política e das restantes políticas internas relevantes*, garantindo que refletem alterações legislativas, orientações das autoridades de supervisão ou necessidades operacionais identificadas.

O RCN *coordena e supervisiona a execução dos deveres preventivos* previstos na legislação de BCFT, incluindo os deveres de identificação e diligência, exame, comunicação, abstenção, colaboração, formação e conservação. *Monitoriza a deteção de fatores de risco* e assegura que as situações de maior relevância são analisadas e escalonadas de acordo com os procedimentos internos, *promovendo a adoção de medidas corretivas ou mitigadoras* quando necessário.

É igualmente responsabilidade do RCN *assegurar a interlocução com as autoridades competentes*, incluindo o Banco de Portugal, a Unidade de Informação Financeira e demais entidades com competência de supervisão ou investigação, colaborando na prestação de informações, resposta a pedidos formais e apresentação de comunicações obrigatórias sempre que se verifiquem os respetivos pressupostos legais.

O RCN *acompanha e apoia a atuação das restantes funções de controlo interno*, em especial o Compliance Officer e a Gestão de Risco, promovendo a coerência entre as suas análises e contribuindo para a identificação transversal de vulnerabilidades operacionais ou de risco. O RCN pode, quando necessário, solicitar informações a qualquer área da organização, bem como recomendar ajustamentos de processos, metodologias ou controlos quando tal se revele essencial à conformidade e à mitigação do risco.

No exercício das suas funções, o RCN deve atuar com objetividade, rigor, autonomia e confidencialidade, garantindo que a sua atuação contribui para a robustez do sistema de governo interno da IFTHENPAY e para a proteção da instituição contra riscos legais, reputacionais e operacionais associados ao incumprimento das obrigações de BCFT.

1.3 Compliance Officer (CO)

O Compliance Officer (CO) é a função de segunda linha *responsável pela execução operacional dos controlos* relacionados com a prevenção do branqueamento de capitais e do financiamento do terrorismo, assegurando a *monitorização diária* da atividade e a *deteção tempestiva* de situações que possam indiciar risco ou incumprimento. O CO atua sob orientação funcional do RCN, mantendo, contudo, autonomia técnica na análise das operações, alertas e exceções identificadas nos sistemas e procedimentos internos.

Compete ao CO *assegurar a implementação prática dos deveres preventivos* previstos na legislação aplicável e na presente Política, executando verificações regulares sobre clientes, operações, documentos e padrões comportamentais. O CO é responsável por *analisar os alertas* gerados pelos sistemas de monitorização, avaliar a sua relevância, proceder à respetiva documentação e, quando necessário, escalonar os casos que exijam exame aprofundado, intervenção do RCN ou decisão da Gerência.

No âmbito das suas atividades, o CO *recolhe, organiza e mantém registos completos e atualizados das diligências realizadas*, garantindo a rastreabilidade e auditabilidade das decisões e verificações efetuadas. O CO assegura igualmente a aplicação dos procedimentos

de verificação da identidade, avaliação de risco, monitorização contínua e atualização de informação, colaborando estreitamente com as equipas operacionais e contribuindo para a uniformidade e consistência dos processos internos.

O CO desempenha ainda funções de *apoio técnico ao RCN*, colaborando na atualização de políticas, procedimentos e metodologias de controlo, bem como na preparação de reportes internos e externos quando aplicável. Sempre que necessário, o *CO substitui o RCN* nas suas funções, garantindo a continuidade operacional e a salvaguarda do cumprimento das obrigações legais e regulamentares em matéria de BCFT.

O exercício das funções de CO exige rigor, independência, discrição e capacidade de julgamento técnico, devendo o titular da função atuar de forma objetiva e diligente, contribuindo para a robustez do sistema de controlo interno e para a mitigação dos riscos legais, operacionais e reputacionais associados ao BCFT.

1.4 Auditoria Interna (AI)

A Auditoria Interna constitui a terceira linha de defesa da IFTHENPAY, assegurando uma *avaliação independente da eficácia dos sistemas de governo interno, controlo interno e prevenção do branqueamento de capitais e do financiamento do terrorismo*. Embora a legislação aplicável permita a externalização da função, a sua existência é obrigatória para as instituições de pagamento, pelo que a IFTHENPAY recorre a um prestador especializado para o exercício das responsabilidades inerentes à Auditoria Interna, cuja atividade terá início em março de 2026.

A Auditoria Interna atua com total independência funcional, reportando diretamente à Gerência e mantendo autonomia no planeamento e execução dos seus trabalhos. Compete-lhe *avaliar, de forma sistemática, a adequação e eficácia dos controlos implementados*, *testar processos e procedimentos* associados ao cumprimento das obrigações legais e regulamentares, e *identificar potenciais fragilidades ou oportunidades de melhoria* nos sistemas de prevenção do BCFT.

No exercício das suas funções, a Auditoria Interna *realiza revisões temáticas, análises pontuais e testes de conformidade*, emitindo recomendações e acompanhando a sua implementação, de modo a assegurar que as ações corretivas são concluídas de forma eficaz e atempada. A função avalia igualmente a qualidade dos processos de monitorização, a robustez dos sistemas de reporte interno e externo e a fiabilidade da documentação e dos registos associados à atividade da IFTHENPAY.

A Auditoria Interna mantém uma relação de cooperação firme, mas independente, com o Responsável pelo Cumprimento Normativo, o Compliance Officer e a Gestão de Risco, colhendo informação necessária ao exercício das suas atividades e contribuindo para a melhoria contínua dos sistemas de controlo interno. A Gerência assegura que a Auditoria Interna dispõe dos recursos e acesso a informação necessários para o adequado desempenho das suas funções.

A função de Auditoria Interna é um elemento estruturante do sistema de governação da IFTHENPAY, contribuindo para a transparência, integridade e robustez da atividade e para a mitigação dos riscos legais, operacionais e reputacionais a que a instituição está exposta.

1.5 Gestão de Risco (GR)

A função de Gestão de Risco (GR) integra a segunda linha de defesa da IFTHENPAY e é responsável pela *identificação, avaliação, monitorização e reporte dos riscos* a que a instituição está ou possa vir a estar exposta, incluindo os riscos inerentes e residuais associados ao branqueamento de capitais e ao financiamento do terrorismo. A função atua de forma autónoma relativamente às linhas operacionais e em estreita coordenação com a Gerência, o RCN e o CO, assegurando uma visão integrada e transversal do perfil de risco da instituição.

A GR *implementa um modelo estruturado de identificação e avaliação dos riscos*, suportado por metodologias adequadas à natureza da atividade da IFTHENPAY e proporcional à sua dimensão. Este modelo incorpora uma matriz de risco BCFT, que permite avaliar a exposição da instituição a fatores de risco inerentes ao cliente, produto, canal, geografia e operação, bem como o efeito mitigador dos controlos existentes. A aplicação sistemática desta metodologia assegura uma avaliação consistente, documentada e atualizada do nível de risco assumido e das medidas necessárias à sua mitigação.

Compete igualmente à GR elaborar e manter atualizado o Risk Appetite Statement, que estabelece os limites e tolerâncias de risco considerados aceitáveis pela IFTHENPAY, incluindo no domínio específico do BCFT. Este documento orienta a tomada de decisão estratégica e operacional, garantindo que a atividade permanece dentro dos níveis de risco definidos pela Gerência.

No exercício das suas funções, a GR procede à *monitorização contínua dos riscos operacionais, reputacionais e de BCFT*, avaliando tendências, variações significativas e potenciais vulnerabilidades decorrentes da evolução da atividade, das características dos clientes ou de alterações no enquadramento tecnológico, legal ou regulamentar. Esta monitorização permite a deteção precoce de riscos emergentes e a recomendação de medidas de mitigação adequadas.

A GR assegura ainda o *reporte periódico e circunstancial* à Gerência, contribuindo para a supervisão efetiva do perfil de risco e das medidas implementadas. Mantém *uma interação regular* com o RCN e o CO, partilhando análises, dados relevantes e avaliações específicas que reforcem a fiabilidade e a coerência das decisões de controlo interno. Sempre que se revele necessário, a função *desenvolve ou acompanha testes de resiliência* e cenários internos que permitam aferir a capacidade da instituição para responder a situações de stress operacional ou comportamental no âmbito do BCFT.

Todas as atividades da GR são devidamente *documentadas*, garantindo rastreabilidade, transparência e suporte às atividades de auditoria interna e externa. A função contribui, assim, para a robustez do sistema de governo interno da IFTHENPAY, reforçando a prevenção do risco legal, operacional e reputacional associado ao BCFT e assegurando que a instituição atua dentro dos parâmetros definidos pela Gerência.

1.6 Código de Conduta (CdC)

O Código de Conduta da IFTHENPAY estabelece os *princípios éticos e comportamentais que orientam a atuação* de todos os colaboradores, dirigentes e prestadores de serviços, assegurando que a atividade da instituição é conduzida com integridade, rigor e respeito pelas normas legais e regulamentares aplicáveis. A observância destes princípios é essencial para a manutenção da confiança dos clientes, parceiros e autoridades de supervisão, bem como para a prevenção de riscos legais, operacionais e reputacionais associados à atividade.

A IFTHENPAY espera que todos os seus colaboradores ajam de forma diligente, honesta e profissional, pautando a sua atuação pelos valores da transparência, imparcialidade, responsabilidade e respeito pelas regras internas e externas que regem a atividade da instituição. Os colaboradores devem *abster-se* de qualquer comportamento que possa comprometer a integridade dos processos operacionais, influenciar de forma indevida decisões internas ou externas, ou criar perceções de favorecimento ou de conflito de interesses.

São *expressamente proibidas* condutas que violem a legislação aplicável, que facilitem ou possam facilitar práticas de branqueamento de capitais ou de financiamento do terrorismo, ou que ponham em causa a independência e eficácia das funções de controlo interno. Os colaboradores devem *evitar* situações que possam originar *conflitos de interesses*, reais ou aparentes, e comunicar prontamente à Gerência ou ao RCN quaisquer circunstâncias que possam afetar a objetividade ou a imparcialidade no exercício das suas funções.

O CdC reforça ainda a importância da *confidencialidade* e *da proteção de dados pessoais e profissionais*, impondo o dever de guardar sigilo sobre a informação a que tenham acesso no âmbito da sua atividade e de a utilizar exclusivamente para fins profissionais legítimos.

O cumprimento rigoroso do CdC é parte integrante das responsabilidades individuais de cada colaborador e constitui elemento essencial para a eficácia do sistema de controlo interno e para a aplicação da presente Política. A IFTHENPAY promove, sempre que necessário, ações de formação e sensibilização destinadas a reforçar a compreensão e a aplicação dos princípios consagrados no CdC, contribuindo para uma cultura organizacional sólida e alinhada com os mais elevados padrões éticos e profissionais.

1.7 Canais de Comunicação de Irregularidades (Whistleblowing)

A IFTHENPAY dispõe de *canais internos de comunicação de irregularidades* que *permitem* a todos os colaboradores, dirigentes e prestadores de serviços *reportar*, *de forma segura e confidencial*, qualquer situação que possa constituir *violação de normas legais, regulamentares ou internas*, incluindo as relativas à prevenção do branqueamento de capitais e do financiamento do terrorismo. Estes canais, concebidos em conformidade com a legislação aplicável e com as melhores práticas de governo interno, asseguram a possibilidade de apresentação de comunicações relativas a comportamentos indevidos, fragilidades operacionais, incumprimentos ou suspeitas que possam afetar a integridade da atividade da instituição.

Os canais de comunicação garantem a *confidencialidade da identidade do denunciante*, bem como a *proteção da informação* transmitida, podendo, quando legalmente permitido, *assegurar o anonimato* da comunicação. A IFTHENPAY adota medidas para *prevenir qualquer forma de retaliação* contra colaboradores que, de boa-fé, utilizem estes canais, assegurando que a denúncia não resulta em prejuízo injustificado para o denunciante.

As comunicações recebidas são analisadas com rigor e imparcialidade, sendo tratadas pela função competente, com salvaguarda da independência das linhas de defesa e da autonomia das funções de controlo interno. Sempre que a natureza da comunicação assim o exija, o RCN é envolvido no processo de análise, garantindo a articulação com as obrigações de reporte às autoridades competentes, quando aplicável.

A IFTHENPAY assegura o *registo, documentação e conservação das comunicações recebidas*, bem como a implementação de medidas corretivas ou mitigadoras que resultem da sua análise. A existência e utilização dos canais de comunicação contribuem para o reforço do sistema de governo interno, promovendo uma cultura de transparência, responsabilidade e tolerância zero relativamente a comportamentos que possam comprometer a integridade da instituição ou facilitar práticas de BCFT.

1.8 Recursos, independência e segregação funcional

A IFTHENPAY *assegura* que a sua organização interna *dispõe de recursos humanos, técnicos e financeiros adequados à natureza, dimensão, complexidade e risco* da atividade desenvolvida, garantindo que as funções críticas, nomeadamente as funções de controlo interno, dispõem dos meios necessários ao exercício eficaz das suas responsabilidades. A *afetação de recursos é periodicamente avaliada* pela Gerência, tendo em consideração a evolução da atividade, a introdução de novos produtos, serviços ou tecnologias e a identificação de necessidades adicionais decorrentes de alterações regulamentares ou operacionais.

A *independência funcional das funções de controlo interno* — RCN, CO, GR e AI — é assegurada através de uma estrutura de reporte que permite o *acesso direto à Gerência* e a *ausência de interferências* indevidas por parte das áreas operacionais. As funções de controlo atuam com *autonomia técnica e objetividade*, sendo vedado o exercício de atividades que possam comprometer a sua imparcialidade ou gerar conflitos de interesses.

No desenvolvimento da sua atividade, a IFTHENPAY assegura igualmente a *segregação adequada de funções*, prevenindo a acumulação de responsabilidades incompatíveis e reduzindo o risco de erros, irregularidades ou potenciais fraudes. As tarefas críticas associadas ao ciclo de vida do cliente, aos processos de pagamento, aos sistemas informáticos e ao cumprimento das obrigações de BCFT são distribuídas de forma a garantir que nenhuma área concentra simultaneamente poderes de decisão, execução e supervisão.

Sempre que necessário, a instituição recorre à externalização de funções, de forma proporcional e devidamente controlada, assegurando que os prestadores externos atuam em conformidade com os padrões de qualidade e os requisitos legais aplicáveis. A IFTHENPAY adota mecanismos de monitorização contínua dos serviços externalizados que possam impactar a prevenção do BCFT ou a integridade do sistema de controlo interno.

A combinação adequada de recursos, independência e segregação funcional constitui um elemento essencial do sistema de governo interno da IFTHENPAY, permitindo a identificação, mitigação e resposta eficaz aos riscos associados à sua atividade e garantindo o cumprimento das obrigações legais e regulamentares em matéria de prevenção do BCFT.

1.9 Apreciação e revisão periódica das políticas

A IFTHENPAY assegura a revisão da atualidade das políticas, procedimentos e controlos com intervalos *não superiores a 12 meses*. Este prazo pode ser alargado até 24 meses apenas quando a natureza, dimensão e complexidade da atividade o justifiquem e exista comprovadamente uma menor exposição ao risco, mediante decisão fundamentada da Gerência. A revisão extraordinária ocorre sempre que existam alterações legislativas ou falhas detetadas em auditorias, na regulamentação setorial ou nas melhores práticas do setor.

Compete à *Gerência aprovar as versões atualizadas* das políticas internas, *garantindo* que incorporam eventuais *ajustamentos necessários à evolução do quadro jurídico e regulamentar*, à introdução de novos produtos ou serviços, ou à identificação de vulnerabilidades operacionais resultantes da atividade diária, de auditorias, de inspeções ou de recomendações das funções de controlo interno. A *Gerência assegura* igualmente que a *atualização* das políticas *é comunicada* de forma clara aos colaboradores e que são implementadas ações de formação ou sensibilização sempre que tal se revele necessário.

O RCN desempenha um papel essencial na *monitorização das alterações legislativas e regulamentares relevantes*, propondo atualizações à presente Política sempre que necessário, e avaliando a sua conformidade e adequação face às exigências legais em vigor. O RCN pode, ainda, recomendar revisões extraordinárias sempre que identifique novas tendências de risco, alterações estruturais na organização ou necessidades operacionais que justifiquem ajustamentos imediatos.

A IFTHENPAY assegura que todas as versões anteriores da Política são devidamente arquivadas, permitindo a rastreabilidade das alterações efetuadas, e que a Política em vigor está sempre acessível às funções relevantes e a todos os colaboradores, contribuindo para a robustez e continuidade do sistema de governo interno.

II. CONCEITOS E DEFINIÇÕES ESSENCIAIS

Para efeitos da presente Política, aplicam-se os conceitos abaixo descritos, os quais se encontram alinhados com a legislação e regulamentação aplicáveis em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo.

Branqueamento de capitais

Entende-se por branqueamento de capitais qualquer ato ou operação que tenha por finalidade dissimular ou ocultar a origem ilícita de bens ou produtos, integrando-os no sistema económico e financeiro como se fossem legítimos. Engloba as fases de colocação, circulação e integração, podendo envolver a utilização de contas, serviços de pagamento, estruturas empresariais ou outras formas de movimentação de fundos. A IFTHENPAY deve adotar medidas que impeçam que os seus serviços sejam utilizados para esse fim.

Financiamento do terrorismo

Consiste na disponibilização, recolha, entrega ou utilização de fundos ou outros bens, direta ou indiretamente, com a intenção ou sabendo que serão utilizados para a prática de atos terroristas ou para apoiar indivíduos, organizações ou atividades relacionadas com o terrorismo. A prevenção deste risco implica especial atenção a padrões transacionais, comportamentos anómalos e ligações a entidades ou jurisdições sensíveis.

Financiamento da proliferação de armas de destruição em massa (ADM)

Refere-se à disponibilização, recolha ou movimentação de fundos, bens ou tecnologias destinados a apoiar a proliferação nuclear, química ou biológica, contrariando obrigações internacionais e regimes de sanções. A IFTHENPAY deve cumprir escrupulosamente as listas e medidas restritivas definidas pela União Europeia e pelas Nações Unidas aplicáveis a este domínio.

Relação de negócio

Considera-se relação de negócio qualquer relação profissional ou comercial estabelecida entre a IFTHENPAY e um cliente, no âmbito da prestação continuada de serviços de pagamento. A relação inicia-se no momento da aceitação do cliente e mantém-se ativa enquanto houver serviços prestados ou contas abertas, independentemente da frequência de operações.

Operação ocasional

Entende-se por operação ocasional uma transação efetuada fora do âmbito de uma relação de negócio contínua, desde que enquadrada na legislação aplicável. Considerando que a IFTHENPAY opera exclusivamente com clientes previamente aceites e titulares de relação de negócio, a realização de operações ocasionais é, na prática, residual ou inexistente.

Beneficiário Efetivo (BEf)

É a pessoa singular que, em última instância, detém ou controla o cliente, ou em nome de quem a relação de negócio é estabelecida ou a operação é realizada. A identificação e verificação do BEf incluem a análise da cadeia de participações, estruturas societárias, poderes de gestão e controlos indiretos. O BEf deve ser sempre identificado e verificado antes do início da relação de negócio.

Pessoa Politicamente Exposta (PEP)
Pessoa singular que desempenha ou desempenhou funções públicas proeminentes nos últimos 12 meses. O conceito estende-se obrigatoriamente aos **membros próximos da família** (cônjuges, unidos de facto, pais, filhos e respetivos cônjuges) e às **pessoas reconhecidas como estreitamente associadas** (co-detentores de empresas ou pessoas com relações comerciais próximas). A classificação como PEP implica a adoção de medidas de diligência reforçada.

Titular de outros cargos políticos ou públicos
Pessoa que exerce funções políticas ou públicas relevantes mas não abrangidas pela definição de PEP, exigindo, ainda assim, medidas acrescidas de diligência quando se encontrem presentes fatores de risco que assim o justifiquem.

Entidade de risco elevado
Cliente, operação, produto, serviço, canal ou geografia cuja avaliação de risco, segundo a metodologia da IFTHENPAY, revele um nível de risco significativo. A classificação como risco elevado implica a aplicação de medidas reforçadas de identificação, diligência e monitorização, nos termos da legislação e desta Política.

Medidas simplificadas, normais e reforçadas
Conjuntos de medidas de identificação, verificação, diligência e monitorização aplicáveis aos clientes e operações, proporcionais ao risco identificado.

- **Medidas normais:** aplicáveis à generalidade dos clientes.
- **Medidas simplificadas:** permitidas apenas quando exista evidência clara de risco reduzido.
- **Medidas reforçadas:** obrigatórias em situações de risco elevado, incluindo PEPs, estruturas complexas, geografias sensíveis ou padrões operacionais anómalos.

Monitorização contínua
Sempre que a presente Política se refere a 'monitorização contínua', tal expressão deve ser entendida como acompanhamento da relação de negócio ao longo do tempo, baseado em reapreciações periódicas, análise humana e mecanismos proporcionais ao risco, não pressupondo deteção automática contínua ou em tempo real.

III. ACEITAÇÃO DE CLIENTES

A política de Aceitação de Clientes da IFTHENPAY, consagrada no presente capítulo, estabelece o enquadramento, os princípios e os critérios que orientam a Instituição na decisão de iniciar e/ou manter relações de negócio com clientes, de forma prudente, documentada e alinhada com o seu apetite de risco, com o seu modelo de negócio e com as obrigações legais e regulamentares aplicáveis em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo.

A IFTHENPAY adota uma abordagem baseada no risco, estruturada de acordo com a legislação nacional e europeia, as diretrizes das autoridades de supervisão e as boas práticas internacionalmente reconhecidas, assegurando que os seus serviços não são utilizados para a prática de crimes financeiros ou para atividades suscetíveis de gerar riscos legais, operacionais ou reputacionais elevados.

A instituição define, de forma sustentável e em coerência com o seu sistema de controlo interno, as *categorias de clientes que está disposta a aceitar*, garantindo a obtenção rigorosa da informação necessária à sua identificação, à caracterização da sua atividade, ao conhecimento da estrutura de propriedade e controlo, e à compreensão da finalidade e natureza da relação de negócio pretendida. Esta informação é fundamental para a avaliação do risco inerente e residual associado ao cliente e à sua atividade, bem como para a tomada de decisão informada quanto à sua aceitação.

O presente capítulo tem, assim, como objetivos:

- estabelecer critérios claros e proporcionados para a aceitação, recusa ou aprovação condicionada de clientes;
- assegurar que o nível de risco identificado é devidamente documentado, analisado e refletido na decisão;
- identificar atividades proibidas, modelos de negócio incompatíveis e fatores de risco agravado;
- garantir que clientes sensíveis, como Pessoas Politicamente Expostas (PEP), são sujeitos a medidas acrescidas de diligência e aprovação de direção de topo;
- proteger a IFTHENPAY contra práticas que possam comprometer a integridade, continuidade ou reputação da instituição.

1 Elementos fundamentais no processo de aceitação e conhecimento de clientes

A aceitação de um cliente depende sempre da *verificação prévia da sua identidade* e, quando aplicável, da *identidade dos respetivos representantes e beneficiários efetivos*, em conformidade com os deveres de identificação e diligência previstos na legislação aplicável. No âmbito do processo de aceitação e de conhecimento do cliente (KYC), a IFTHENPAY assegura, entre outros, os seguintes elementos:

- a obtenção de informação sobre a finalidade da conta de pagamento e a natureza da relação de negócio pretendida;
- a definição do perfil transacional expectável, incluindo, quando necessário, informação adicional sobre a origem e destino dos fundos;

- a recolha de comprovativos documentais sobre a origem dos fundos e das fontes de rendimento do cliente, sempre que justificado por fatores de risco;
- a verificação da coerência e consistência da informação recolhida, incluindo cruzamento com bases internas, externas e listas de sanções;
- o pedido de justificações adicionais e de documentação complementar sempre que se detetem discrepâncias relevantes ou padrões operacionais atípicos.

No caso de pessoas coletivas ou centros de interesses coletivos sem personalidade jurídica, a IFTHENPAY procede, de forma sistemática, à:

- identificação e verificação da própria entidade (denominação, objeto, sede, NIPC, país de constituição, CAE, etc.);
- identificação dos titulares de participações no capital e/ou direitos de voto de valor igual ou superior a 5%;
- identificação dos titulares do órgão de administração ou órgão equivalente, bem como de outros quadros superiores relevantes com poderes de gestão;
- identificação e verificação do(s) beneficiário(s) efetivo(s), incluindo consulta ao Registo Central do Beneficiário Efetivo (RCBE) e reação adequada em caso de discrepâncias.

Quando o cliente é pessoa singular ou empresário em nome individual, a IFTHENPAY identifica e verifica, além da identidade do próprio, os respetivos representantes (quando existam), bem como quaisquer outras pessoas que, em nome do cliente, atuem no âmbito da relação de negócio.

A IFTHENPAY reserva-se o direito de utilizar prestadores externos de verificação de identidade, bases de dados independentes, listas de sanções e outras fontes idóneas, desde que em conformidade com a legislação aplicável, para reforçar a fiabilidade da informação utilizada na decisão de aceitação.

2 Categorias de clientes cuja aceitação deve ser recusada

Em conformidade com o modelo de risco da IFTHENPAY e com o disposto no **ANEXO I – Lista de Atividades e Produtos Não Admitidos** do Contrato de Adesão, a instituição **recusará obrigatoriamente** propostas de adesão que se enquadrem nas seguintes situações:

2.1 Risco legal, sancionatório ou criminal grave

- Clientes (ENI ou pessoas coletivas), incluindo beneficiários efetivos, acionistas e representantes, constantes de listas de sanções (ONU, UE, OFAC ou outras reconhecidas);
- Clientes cuja reputação pública revele associação a atividades criminosas, BCFT ou outras infrações graves;
- Clientes relativamente aos quais existam indícios suficientemente credíveis de envolvimento em atividades ilícitas.

2.2 Opacidade, anonimato e falta de colaboração

- Clientes cuja origem de fundos ou riqueza não possa ser compreendida ou demonstrada;
- Clientes que pretendam operar em anonimato, com identidades fictícias ou estruturas artificiais sem justificação económica;
- Clientes que não colaborem na entrega de documentação requerida, impossibilitando o cumprimento dos deveres de identificação e diligência.

2.3 Entidades financeiras ou quase financeiras de risco intolerável

- Bancos de fachada ou entidades equivalentes, incluindo instituições sem presença física efetiva;
- Instituições financeiras ou similares não autorizadas;
- Bancos de correspondência ou entidades equivalentes incompatíveis com o modelo de risco.

2.4 Jurisdições de risco elevado

- Clientes domiciliados em jurisdições offshore não cooperantes ou países terceiros de risco elevado;
- Clientes com atividade, origem de fundos ou relações comerciais relevantes em jurisdições sancionadas.

2.5 Atividades e produtos proibidos (ANEXO I – Contrato de Adesão)

A IFTHENPAY **não aceita** entidades que exerçam, promovam, comercializem ou intermedeiem atividades enquadráveis nas seguintes categorias:

a) Produtos

- Estupefacientes e derivados;
- Derivados da cannabis, incluindo CBD, fora dos circuitos autorizados;
- Álcool sem licença;
- Tabaco, plantas de fumar, cigarros eletrónicos ou consumíveis não autorizados;
- Software de hacking, spyware e software malicioso;
- Produtos contrafeitos ou de origem duvidosa;
- Armas, munições, acessórios correlatos, réplicas e dispositivos Airsoft.

b) Serviços

- Plataformas de encontros, namoro ou "charmosas";
- Streaming de vídeo não autorizado;
- Pornografia, erotismo, webcams, serviços de acompanhantes;
- Emissão ou gestão de cartões pré-pagos;
- File sharing ou hosted file transfer;
- Intermediação de mercados de capitais, FOREX, CFDs ou modelos de trading de alto risco;
- Compra, venda ou troca de moedas;

- Atividades relacionadas com criptoativos ou moedas virtuais, incluindo compra, venda, intermediação, troca ou facilitação de pagamentos com cripto;
- Caução ou bloqueio de valores por cartão;
- Cobrança ou gestão de fundos de terceiros;
- Utilização ou fornecimento de VPN para fins que comprometam a rastreabilidade;
- Cobrança de dívidas por terceiros (exceto crowdfunding regulado);
- Promoção de terrorismo, atividades ilícitas, ou proselitismo extremista;
- Estudos de credibilidade, renegociação de crédito, consultoria financeira sem enquadramento regulatório;
- Casinos, apostas, jogos online ou offline não licenciados;
- Vendas de seguidores, esquemas piramidais, marketing multinível dissimulado;
- Lotarias, rifas ou outros jogos de sorte não licenciados.

c) Crowdfunding

- Movimentos extremistas, seitas ou campanhas radicais;
- Causas associadas a atividades proibidas;
- Financiamento de multas criminais;
- Investimentos em diamantes, metais ou pedras preciosas fora de circuitos regulados.

Sempre que uma proposta de adesão seja recusada, a IFTHENPAY elabora um dossiê completo contendo todos os elementos recolhidos, bem como os fundamentos da decisão, o qual é analisado pela função de Compliance e comunicado à Gerência.

3 Categorias de clientes sujeitas a processo especial de autorização (EDD)

Determinadas categorias de clientes, embora não proibidas, exigem uma avaliação reforçada e aprovação prévia da Gerência, nomeadamente:

- clientes ou beneficiários efetivos classificados como de risco elevado;
- entidades que operam no comércio de metais preciosos, desde que devidamente autorizadas;
- casas de câmbio ou atividades similares, quando enquadráveis no modelo de risco;
- clientes identificados como PEP, membros próximos da família ou pessoas estreitamente associadas;
- clientes com histórico de sanções, medidas restritivas ou investigações;
- entidades com estruturas societárias complexas ou opacas;
- clientes envolvidos em operações com jurisdições de alto risco;
- atividades de dropshipping com cadeias de fornecimento pouco transparentes.

O processo especial de autorização inclui análise detalhada pelo Compliance e Gestão de Risco, consulta de informação adicional e decisão fundamentada por parte da Gerência.

4 Pessoas Politicamente Expostas (PEP), titulares de outros cargos políticos ou públicos e associados

A aceitação de uma relação de negócio com PEPs, seus membros próximos da família, pessoas estreitamente associadas ou titulares de cargos políticos ou públicos exige:

4.1 verificação rigorosa da identidade e estatuto;
4.2 aplicação de medidas reforçadas de diligência;
4.3 recolha adicional de informações sobre origem de fundos, património e finalidade da relação de negócio;
4.4 monitorização reforçada;
4.5 aprovação expressa da direção de topo.

A IFTHENPAY enceta os seus melhores esforços na deteção tempestiva de PEPs, titulares de outros cargos políticos ou públicos, membros próximos da família e pessoas reconhecidas como estreitamente associadas, registando as decisões tomadas em consequência dessa deteção.

5 Fatores de risco na aceitação e classificação inicial

A IFTHENPAY utiliza metodologia própria de risco para avaliar a exposição a BCFT no momento da aceitação, considerando fatores como:

- geografia de residência, atividade ou origem de fundos;
- natureza da atividade e enquadramento regulatório;
- estatuto de PEP ou outras figuras sensíveis;
- perfil reputacional;
- ligação a setores, produtos ou serviços de risco elevado;
- indicadores internos definidos pelo Compliance ou Gestão de Risco.

A classificação de risco é atribuída através de ferramenta interna, com atualização diária, podendo ser ajustada manualmente mediante análise casuística.

IV. IDENTIFICAÇÃO E DILIGÊNCIA (KYC)

1 Princípios gerais do dever de identificação

A identificação rigorosa do cliente, dos seus representantes e dos respetivos beneficiários efetivos constitui a primeira linha de defesa da IFTHENPAY na prevenção do branqueamento de capitais e do financiamento do terrorismo. O cumprimento deste dever é *condição prévia e absolutamente indispensável* para o estabelecimento de qualquer relação de negócio, refletindo os princípios de diligência, transparência e proporcionalidade previstos na legislação aplicável.

A IFTHENPAY assegura que *todos os clientes* — pessoas singulares, pessoas coletivas, centros de interesses coletivos sem personalidade jurídica, bem como empresários em nome individual — *são devidamente identificados antes da abertura da relação de negócio*, verificando a autenticidade e a consistência dos elementos apresentados. Esta identificação abrange igualmente os representantes legais ou contratuais, bem como, quando aplicável, (i) os beneficiários efetivos e (ii) os titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5%, sem prejuízo da identificação dos titulares do órgão de administração e de outros quadros superiores relevantes com poderes de gestão.

Dado que a IFTHENPAY realiza 100% das suas relações de negócio através de *processos não presenciais*, a instituição adota medidas adequadas para assegurar o nível de fiabilidade e segurança exigido pela lei, combinando *análise documental formal e material, validações automáticas, consultas a bases de dados externas e procedimentos de verificação independente* sempre que o risco assim o determine. A instituição garante que a ausência de contacto presencial não reduz o rigor do processo de identificação nem o grau de confiança atribuído à documentação recebida.

A identificação é proporcional ao risco, sendo *reforçada sempre que se detetem fatores de risco acrescido* — nomeadamente no caso de estruturas societárias complexas, presença de beneficiários efetivos difíceis de identificar, jurisdições sensíveis ou potenciais PEP, seus membros próximos da família ou pessoas estreitamente associadas. Estas situações implicam a *aplicação de medidas complementares de diligência*, a *recolha adicional de informação* e, quando necessário, a *intervenção da Gerência*.

A IFTHENPAY assegura que os elementos de identificação obtidos antes do início da relação de negócio são suficientes, fiáveis e atualizados, podendo solicitar documentação adicional sempre que existam dúvidas sobre a veracidade, integridade ou adequação da informação fornecida. A instituição mantém procedimentos destinados a garantir que a informação obtida permanece atualizada ao longo da relação de negócio, mediante *monitorização ao longo da relação de negócio, baseada numa abordagem proporcional ao risco, assente em reapreciações periódicas e análise humana*.

A verificação da identidade e a qualidade dos documentos apresentados estão sempre intrinsecamente ligadas à decisão de aceitação do cliente. A relação de negócio não é estabelecida enquanto não for possível concluir a identificação e verificação com grau de certeza compatível com o risco. Da mesma forma, a deteção de inconsistências, omissões ou

riscos não mitigáveis determina a recusa da proposta de adesão, nos termos definidos no capítulo III desta Política.

Em consonância com uma abordagem baseada no risco e com os deveres previstos na legislação aplicável, a IFTHENPAY compromete-se a manter elevados padrões de rigor na identificação e verificação dos seus clientes e respetivos intervenientes, contribuindo para a integridade da sua atividade e para a prevenção do uso indevido dos seus serviços para fins ilícitos.

2 Verificação da identidade

A verificação da identidade constitui um momento crítico do processo de KYC, assegurando que os elementos fornecidos pelo cliente, pelos seus representantes e pelos beneficiários efetivos são *autênticos*, *suficientes e coerentes* com a informação recolhida ao longo da análise. A IFTHENPAY adota um conjunto de *procedimentos formais e materiais* destinados a *confirmar a veracidade* dos dados apresentados, reforçando o nível de confiança exigido pela legislação aplicável e pelo seu modelo de risco.

2.1 Princípios gerais da verificação documental

A verificação da identidade é efetuada exclusivamente por *meios documentais*, uma vez que a IFTHENPAY desenvolve a sua atividade através de processos integralmente não presenciais. Para esse efeito, a instituição exige que os clientes apresentem documentos de identificação *válidos*, *legíveis e completos*, bem como os *comprovativos adicionais* necessários à caracterização da entidade e da sua atividade económica.

A verificação documental inclui:

- análise formal do documento (validade, integridade, legibilidade e correspondência dos dados);
- análise material (coerência da informação com outros elementos recolhidos, padrões de risco e perfis esperados);
- validação da autenticidade aparente, incluindo confrontação com listas de documentos inaceitáveis ou com indícios de manipulação digital;
- cruzamento com bases de dados internas e externas, bem como consultas obrigatórias ao RCBE, quando aplicável.

Quando existam *suspeitas* quanto à autenticidade, alteração ou fiabilidade dos documentos apresentados, a IFTHENPAY solicita *documentação adicional*, recorre a *fontes independentes* ou, caso não seja possível confirmar a identidade, procede à recusa da relação de negócio.

2.2 Processo de identificação não presencial

O processo de identificação e verificação decorre integralmente à distância, devendo o cliente fornecer todos os elementos solicitados através dos canais definidos pela IFTHENPAY.

A autenticidade dos documentos recebidos é avaliada através da combinação de:

- análise humana especializada realizada pelo Helpdesk e/ou Compliance Officer;

- sistemas tecnológicos de filtragem e validação automática;
- comparações cruzadas com informação disponível em bases oficiais, registos públicos e listas de sanções.

A IFTHENPAY implementa controlos internos destinados a garantir que a ausência de contacto presencial não compromete o rigor, a fiabilidade ou a segurança do processo de verificação da identidade.

2.3 Receção do contrato preenchido, rubricado e assinado

A relação de negócio apenas pode ser proposta mediante o envio, por parte do cliente, do:

- contrato de adesão devidamente preenchido;
- páginas não assinadas rubricadas;
- página final assinada de forma manual ou por meio equivalente juridicamente admissível.

A conferência manual e automática da assinatura e das rubricas inclui:

- verificação da correspondência entre assinatura no contrato e nos documentos de identificação;
- verificação de integridade formal (sem rasuras, omissões ou modificações não admissíveis);
- validação de que todos os campos obrigatórios se encontram preenchidos.

Qualquer incongruência relevante determina devolução do processo para correção ou, em caso de incumprimento reiterado, recusa da proposta de adesão.

2.4 Checklist documental obrigatória

O processo de verificação da identidade exige a apresentação, conforme aplicável, de:

- documento de identificação válido (pessoas singulares);
- recolha de NIF para ENI sem NIPC;
- comprovativo de morada;
- comprovativo de atividade económica (quando aplicável);
- certidão de registo comercial atualizada (pessoas coletivas);
- estatutos ou pacto social (quando necessário);
- identificação de titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5%;
- identificação dos titulares dos órgãos de administração e quadros superiores relevantes;
- RCBE e documentação complementar sobre beneficiários efetivos;
- comprovativo de existência de estabelecimento em Portugal ou na UE, quando exigido pelo modelo de negócio.

A IFTHENPAY pode exigir documentação adicional sempre que tal se revele necessário para confirmar a identidade ou para mitigar fatores de risco detetados.

2.5 Validação da conformidade formal e material dos documentos

A validação dos documentos apresentados segue dois níveis:

a) *Validação formal*, que inclui:

- verificação da validade e data de emissão;
- conferência de elementos obrigatórios constantes do documento;
- legibilidade e ausência de manipulação;
- integridade da informação fornecida.

b) *Validação material*, que inclui:

- coerência entre documentos de identificação, contrato, RCBE e outras fontes;
- análise da plausibilidade dos dados fornecidos (ex.: naturalidade, nacionalidade, NIF, morada, data de nascimento);
- confirmação da identidade e existência do cliente através de bases públicas e privadas;
- verificação da legitimidade do representante perante a entidade (pessoas coletivas).

Quando existam inconsistências ou dúvidas fundamentadas, são solicitados esclarecimentos adicionais, documentos substitutivos ou comprovativos independentes.

2.6 Métodos de verificação: análise humana + sistemas automáticos

O processo de verificação da identidade combina:

- *análise humana especializada*, executada pelo Helpdesk, Compliance Officer e, quando necessário, pelo RCN;
- *sistemas automáticos*, que incluem:
  - filtragem de sanções e listas restritivas;
  - deteção de PEP e associados;
  - validação automática de elementos estruturais dos documentos;
  - identificação de padrões atípicos ou indícios de tentativa de fraude documental.

A combinação destes métodos assegura maior fiabilidade, reduz o risco operacional e permite escalonamento eficiente de casos complexos.

2.7 Critérios para aceitação, devolução ou pedido de documentação adicional

A IFTHENPAY avalia todos os documentos apresentados pelos clientes com vista à verificação da identidade, representatividade e estrutura de controlo, analisando a sua conformidade formal e material. Esta avaliação incide exclusivamente sobre a suficiência, consistência e integridade dos documentos recebidos, independentemente da sua natureza ou origem.

São somente aceites documentos que:

- apresentem adequada legibilidade, integridade e atualidade;
- permitam verificar, com grau de certeza suficiente, a identidade declarada ou a qualidade invocada;
- sejam coerentes com os restantes elementos do processo (contrato, RCBE, declarações, informação societária, etc.);

- não revelem indícios de adulteração, manipulação digital, omissões relevantes ou desconformidades internas.

Os documentos são devolvidos ou considerados insuficientes quando:

- apresentem qualidade que impossibilite a verificação;
- se encontrem caducados ou fora de prazo de validade;
- existam divergências relevantes entre vários documentos apresentados;
- não permitam confirmar a legitimidade da representação ou a titularidade das participações societárias;
- surjam inconsistências injustificadas com a informação obtida de fontes independentes.

Sempre que necessário, a IFTHENPAY solicita documentação suplementar, esclarecimentos adicionais ou comprovativos independentes, especialmente em situações que envolvam risco acrescido, estruturas complexas ou informação insuficiente.

A insuficiência ou a impossibilidade de verificação adequada da documentação constitui motivo para recusa da proposta de adesão, nos termos definidos no capítulo III desta Política.

2.8 Condições para abertura da conta de pagamentos

A conta de pagamentos só pode ser aberta após:

- conclusão bem-sucedida da verificação da identidade;
- análise de risco inicial (incluindo risco geográfico, ocupacional, societário e reputacional);
- validação do BEf e ausência de discrepâncias relevantes no RCBE;
- filtragem automática sem alertas impeditivos;
- inexistência de ligações a atividades proibidas ou incompatíveis com o apetite de risco;
- aprovação manual por parte do Helpdesk e/ou CO;
- aprovação da Gerência quando exigido (EDD ou risco elevado).

Sem estas condições, a relação de negócio *não pode ser estabelecida*.

2.9 Tratamento de situações que exigem diligência reforçada e escalonamento interno

Quando a verificação da identidade revele fatores de risco acrescido — tais como:

- estruturas societárias complexas;
- beneficiários efetivos difíceis de confirmar;
- potenciais PEP, membros próximos ou pessoas estreitamente associadas;
- ligação a jurisdições de risco elevado;
- atividade económica atípica ou sensível;
- inconsistências materiais ou reputacionais —

o processo deve ser escalonado de forma sequencial:

1. Helpdesk →
2. Compliance Officer →
3. Responsável pelo Cumprimento Normativo →
4. Gerência (quando a decisão exija aprovação de topo).

A *diligência reforçada* inclui recolha de documentação adicional, pedido de esclarecimentos, pesquisas adversas, confirmação externa de informação e análise aprofundada da finalidade e natureza da relação de negócio.

Caso os riscos não sejam mitigáveis, a proposta é recusada.

3 Elementos identificativos e meios comprovativos de identidade

A recolha de elementos identificativos constitui um requisito legal essencial à verificação da identidade dos clientes, dos seus representantes e dos beneficiários efetivos. A IFTHENPAY assegura que todos os elementos recolhidos são suficientes, fiáveis, atualizados e adequados ao nível de risco identificado, em conformidade com os artigos 26.º, 27.º, 29.º e 30.º da Lei n.º 83/2017.

3.1 Pessoas singulares

No caso de clientes pessoas singulares, são obrigatoriamente recolhidos e registados os seguintes elementos identificativos:

- fotografia constante do documento de identificação;
- nome completo;
- assinatura;
- data de nascimento;
- nacionalidade inscrita no documento de identificação;
- naturalidade;
- outras nacionalidades conhecidas e não constantes do documento;
- tipo, número, data de validade e entidade emitente do documento de identificação;
- número de identificação fiscal (ou, na sua falta, número equivalente emitido por autoridade estrangeira competente);
- endereço completo da residência permanente e, quando diferente, domicílio fiscal;
- profissão e entidade patronal, quando aplicável.

A IFTHENPAY solicita comprovativos suplementares sempre que a informação fornecida não seja suficiente ou apresente inconsistências relevantes, nomeadamente comprovativos de morada ou de atividade profissional.

3.2 Pessoas coletivas e centros de interesses coletivos sem personalidade jurídica

Para pessoas coletivas e entidades equiparadas, são obrigatoriamente recolhidos e verificados os seguintes elementos:

- denominação social;
- objeto social;
- sede social e, quando aplicável, localização das sucursais ou estabelecimentos estáveis;
- moradas relevantes adicionais associadas à atividade;
- número de identificação de pessoa coletiva (NIPC) ou número equivalente estrangeiro;
- país de constituição;
- código CAE, código do setor institucional ou equivalente;

- identificação dos titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5%;
- identificação dos titulares do órgão de administração ou órgão equivalente;
- identificação de outros quadros superiores relevantes com poderes de gestão.

Além destes elementos, a IFTHENPAY recolhe os documentos necessários à comprovação da legitimidade e representatividade da entidade, nomeadamente:

- certidão permanente ou equivalente;
- pacto social, estatutos ou instrumento de constituição;
- ata ou deliberação de nomeação dos titulares de órgãos sociais;
- procurações, se aplicáveis;
- comprovativos da existência de estabelecimento no território nacional ou na União Europeia, quando exigido pelo modelo de negócio.

3.3 Representantes do cliente

Sempre que a relação de negócio seja contratada por representante legal ou contratual, a IFTHENPAY verifica:

- o documento de identificação do representante;
- o documento que confere poderes de representação (procuração, ata de nomeação, certidão, deliberação societária ou outro instrumento idóneo);
- a autenticidade e a atualidade do documento de representação.

A verificação da representação é condição indispensável para o prosseguimento do processo.

3.4 Beneficiário efetivo (BEf)

A IFTHENPAY procede à identificação e verificação do beneficiário efetivo nos termos do artigo 30.º da Lei n.º 83/2017, com recurso, designadamente, ao RCBE e a análise da cadeia de participações e de controlo. O regime aplicável encontra-se detalhado no n.º 4 do presente Capítulo.

3.5 Meios comprovativos admitidos

A IFTHENPAY aceita como válidos apenas os documentos emitidos por autoridades competentes ou entidades idóneas que permitam comprovar, de forma objetiva e suficiente, a identidade, representação, estrutura societária e demais elementos necessários ao cumprimento dos deveres de identificação e diligência.

Os meios comprovativos admissíveis variam consoante a natureza do cliente:

a) Pessoas singulares e ENI

- documento de identificação válido (Cartão de Cidadão, Título de Residência, Passaporte ou documento equivalente emitido por autoridade nacional ou estrangeira);
- comprovativo de morada de residência e, quando aplicável, domicílio fiscal, com data de emissão recente;
- certidão fiscal de enquadramento em IVA (quando aplicável ao exercício da atividade);

- comprovativo de IBAN que identifique o cliente como titular da conta.

b) Pessoas coletivas (sociedades comerciais ou civis)

- código de acesso à certidão permanente do registo comercial ou documento equivalente emitido por autoridade estrangeira;
- estatutos, pacto social ou documento constitutivo quando necessários para confirmar a estrutura e poderes de representação;
- código de acesso ao RCBE e documentação adicional que permita identificar beneficiários efetivos e titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5%;
- certidão fiscal de enquadramento em IVA;
- comprovativo de IBAN que identifique a pessoa coletiva como titular.

c) Associações, fundações, condomínios e entidades equiparadas

- estatutos atualizados da entidade;
- ata de tomada de posse dos órgãos sociais ou documento equivalente que comprove os poderes de representação;
- certidão permanente ou documento equivalente, quando aplicável;
- código RCBE;
- comprovativos de identidade e morada dos representantes e beneficiários efetivos;
- comprovativo de IBAN que identifique o cliente como titular da conta.

d) Pessoas coletivas de direito público

- documentos oficiais que comprovem a existência, estrutura e poderes de representação, incluindo despachos ou atas de nomeação;
- estatutos ou diploma orgânico, quando aplicável;
- documentos de identificação dos representantes;
- comprovativo de IBAN que identifique o cliente como titular da conta.

A IFTHENPAY pode exigir documentação suplementar quando:

- subsistam dúvidas quanto à autenticidade, integridade ou suficiência dos documentos apresentados;
- a estrutura societária envolva cadeias multinível ou jurisdições de risco elevado;
- existam discrepâncias entre as fontes consultadas;
- seja necessário reforçar o nível de certeza face ao risco identificado.

4 Beneficiário Efetivo (BEf)

A identificação e verificação do beneficiário efetivo constitui uma obrigação legal essencial para assegurar a transparência das estruturas societárias e prevenir a utilização de entidades coletivas ou veículos jurídicos para ocultação de património, dissimulação de identidade ou práticas de branqueamento de capitais e financiamento do terrorismo. A IFTHENPAY assegura que, antes de estabelecer qualquer relação de negócio com pessoas coletivas ou centros de interesses coletivos sem personalidade jurídica, é identificada e verificada a pessoa singular

que, em última instância, detém ou controla a entidade, nos termos do artigo 30.º da Lei n.º 83/2017.

Para efeitos da presente Política, a identificação de titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5% constitui uma medida de conhecimento alargado do cliente e não altera o conceito legal de beneficiário efetivo, o qual se mantém nos termos do artigo 30.º da Lei n.º 83/2017.

4.1 Identificação do beneficiário efetivo

A IFTHENPAY identifica obrigatoriamente:

- as pessoas singulares que detenham, direta ou indiretamente, uma participação no capital ou direitos de voto iguais ou superiores a 25%;
- as pessoas singulares que controlem a entidade por outros meios, incluindo acordos parassociais, poderes especiais de gestão ou influência dominante;
- na ausência de identificação por via das alíneas anteriores, o(s) dirigente(s) de topo (senior managing official), nos termos legalmente aplicáveis, sem prejuízo de diligências adicionais para identificar a pessoa singular que exerça controlo efetivo.

Para assegurar a exaustividade da identificação, a IFTHENPAY analisa a cadeia de participações, incluindo:

- entidades intermédias nacionais ou estrangeiras;
- percentagens detidas em cascata;
- relações de controlo indireto;
- participações dispersas que, no conjunto, permitam inferir controlo significativo.

A identificação do beneficiário efetivo é sempre proporcional ao risco identificado e pode exigir esclarecimentos adicionais quando existam estruturas complexas, jurisdições sensíveis ou entidades interpostas.

4.2 Verificação do beneficiário efetivo

A IFTHENPAY verifica a informação fornecida pelo cliente através de:

- consulta obrigatória ao Registo Central do Beneficiário Efetivo (RCBE);
- análise documental, incluindo certidões comerciais e registos públicos;
- pesquisa de relações societárias em bases de dados idóneas;
- validação da coerência da cadeia societária com o perfil, dimensão e natureza da atividade.

Quando existam indícios de que a estrutura apresentada pode ocultar a identidade do beneficiário efetivo, a IFTHENPAY:

- exige documentação adicional (estatutos, pactos sociais e/ou parassociais, organogramas societários, atas, acordos parassociais, declarações adicionais);
- verifica fontes independentes nacionais ou estrangeiras;

- pode recorrer a ferramentas tecnológicas de mapeamento societário, quando necessário.

A verificação do beneficiário efetivo é *condição indispensável à decisão de aceitação* da entidade cliente.

4.3 Documentação admissível

São considerados *meios comprovativos adequados* para a verificação do beneficiário efetivo:

- certidão permanente do registo comercial ou certidão equivalente emitida por autoridade competente;
- informação constante do RCBE;
- declaração formal da entidade cliente, devidamente assinada por quem tenha poderes para o efeito;
- organogramas societários atualizados, acompanhados de documentação que comprove a titularidade das participações;
- documentos oficiais de registo de participações em entidades estrangeiras;
- atas ou deliberações que demonstrem a composição dos órgãos sociais.

A IFTHENPAY pode solicitar documentação adicional quando:

- a cadeia societária seja complexa ou inclua jurisdições de risco elevado;
- exista discrepância entre várias fontes;
- a estrutura de controlo não seja evidente;
- subsistam dúvidas quanto à existência de controlo indireto.

4.4 Consulta obrigatória ao RCBE e reação a discrepâncias

A consulta ao RCBE é obrigatória antes do estabelecimento da relação de negócio. Caso a entidade apresente um RCBE desatualizado (mais de 12 meses sem confirmação), a IFTHENPAY tem o *dever de recusar a operação* ou o início da relação até à sua regularização. Discrepâncias materiais não justificadas entre o RCBE e os estatutos devem ser comunicadas ao IRN no prazo legal.

A relação de negócio *só pode ser estabelecida* quando, após a análise efetuada, a IFTHENPAY:

- disponha de informação completa e coerente que permita identificar com segurança o beneficiário efetivo;
- tenha obtido uma explicação satisfatória para discrepâncias formais ou irrelevantes;
- não identifique riscos não mitigáveis ou indícios de ocultação da verdadeira estrutura de propriedade e controlo.

Quando subsistam *dúvidas fundadas* sobre a identidade, legitimidade ou controlo efetivo da entidade, a proposta de adesão deve ser *recusada*, sem prejuízo das obrigações de reporte da discrepância ao IRN e da eventual avaliação de comunicação de suspeita, nos termos legais aplicáveis.

4.5 Atualização contínua do beneficiário efetivo

A IFTHENPAY assegura a *atualização dos dados* relativos ao beneficiário efetivo:

- em revisões periódicas proporcionais ao risco do cliente;
- sempre que ocorram alterações societárias detetadas internamente ou através de bases externas;
- sempre que procedimentos internos de monitorização identifiquem alterações materiais no perfil da entidade;
- quando a qualidade de PEP seja adquirida por proprietário, administrador, gestor ou BE.

A instituição reserva-se o direito de solicitar documentação atualizada sempre que necessário para manter um nível de certeza adequado quanto ao titular último da entidade.

5 Pessoas Politicamente Expostas (PEPs), Titulares de Outros Cargos Políticos ou Públicos, Membros Próximos da Família e Pessoas Estreitamente Associadas

A identificação e tratamento de PEPs, titulares de outros cargos políticos ou públicos relevantes, membros próximos da família e pessoas estreitamente associadas constitui uma componente essencial do *processo de diligência reforçada*. A IFTHENPAY assegura o cumprimento rigoroso dos artigos 19.º e 20.º da Lei n.º 83/2017, bem como das orientações nacionais e internacionais aplicáveis, tendo em conta a exposição acrescida destes perfis a riscos de corrupção, abuso de funções públicas e utilização do sistema financeiro para fins ilícitos.

A existência da qualidade de PEP, ou de relação próxima com PEP, não implica, por si só, a recusa da relação de negócio. Contudo, determina a *adoção obrigatória* de *medidas reforçadas de identificação, verificação e monitorização*, associadas a um processo interno de *aprovação* que envolve a *Direção de Topo*.

5.1 Identificação de PEPs e afins

A IFTHENPAY implementa procedimentos e sistemas adequados para detetar, antes do estabelecimento da relação de negócio e ao longo da sua vigência, se o cliente, os seus representantes, beneficiários efetivos, titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5% ou outros intervenientes relevantes:

- são PEPs;
- são titulares de outros cargos políticos ou públicos relevantes;
- são membros próximos da família de PEP;
- são pessoas reconhecidas como estreitamente associadas a PEP.

A identificação resulta da combinação de:

- análise documental;
- questionário específico de recolha de informação;
- pesquisas em bases de dados especializadas e listas atualizadas;
- pesquisas adicionais sempre que o risco ou a estrutura de envolvimento o justifique.

A IFTHENPAY assegura a deteção da aquisição superveniente da qualidade de Pessoa Politicamente Exposta, de titular de outro cargo político ou público relevante, de membro próximo da família ou de pessoa estreitamente associada, através de mecanismos proporcionais ao risco, baseados em reapreciações periódicas, reapreciações por evento e análise humana suportada por informação interna e externa disponível, não dispondo, à data, de mecanismos automáticos de deteção contínua da aquisição superveniente dessas qualidades.

5.2 Tratamento da informação e avaliação do risco

Sempre que um potencial cliente ou interveniente relevante seja identificado como PEP, associado de PEP ou titular de cargo político ou público, a IFTHENPAY:

- reavalia o risco da relação de negócio, considerando fatores como origem de fundos, origem de riqueza, natureza da atividade, histórico reputacional, jurisdições associadas e modelo operacional previsto;
- recolhe informação suficiente para compreender a exposição pública, duração das funções e eventual risco de corrupção, abuso de cargo ou influência indevida;
- determina se a relação de negócio é compatível com o apetite de risco da instituição.

Se for identificado risco não mitigável, a proposta é recusada.

5.3 Medidas de diligência reforçada obrigatórias

Quando a relação de negócio é admissível, a IFTHENPAY aplica obrigatoriamente medidas reforçadas de diligência, incluindo:

- confirmação da identidade através de fontes independentes ou documentação adicional;
- recolha e verificação da origem do património e da origem dos fundos, com grau de detalhe proporcional ao risco;
- análise da finalidade e natureza da relação de negócio;
- monitorização reforçada e contínua da relação, incluindo padrões transacionais e atualização periódica da informação;
- verificação frequente de listas de sanções e fontes reputacionais.

A aceitação ou manutenção de relações com PEPs e associados integra-se sempre num regime de *controlo reforçado entre a 1.ª e a 2.ª linhas*, com documentação adequada no processo interno.

5.4 Aprovação prévia pela Direção de Topo

Em conformidade com a Lei n.º 83/2017, a relação de negócio com PEPs, membros próximos da família, pessoas estreitamente associadas e titulares de cargos políticos ou públicos relevantes depende sempre de:

- análise técnica efetuada pelo Compliance Officer;
- validação pelo Responsável pelo Cumprimento Normativo (RCN);
- aprovação expressa da Direção de Topo.

A decisão deve ser formal, documentada e baseada na avaliação de risco, incluindo:

- justificação para a aceitação;
- medidas de mitigação aplicadas;
- periodicidade da reavaliação;
- grau de monitorização reforçada aprovado.

5.5 Monitorização contínua reforçada

As relações de negócio com PEPs e associados são sujeitas a monitorização reforçada ao longo da relação de negócio, concretizada através de:

- revisão periódica da origem dos fundos e atualização da informação;
- controlo da coerência das operações com o perfil declarado;
- análise humana especializada;
- verificação regular de listas de sanções, bases reputacionais e fontes independentes;
- reapreciações desencadeadas por eventos relevantes:
  - mudança de cargo,
  - dissolução de funções públicas,
  - aquisição superveniente da qualidade de PEP,
  - alterações societárias significativas.

A monitorização reforçada subsiste durante pelo menos 12 meses após o término das funções públicas ou enquanto se mantiver risco relevante.

5.6 Registo e documentação

Todos os casos envolvendo PEPs e associados são registados e documentados de forma adequada, incluindo:

- identificação clara da qualidade existente;
- documentação que comprove a verificação da origem dos fundos e património;
- fundamentação da decisão de aceitação ou recusa;
- medidas reforçadas aplicadas;
- plano de monitorização contínua;
- decisões formais da Direção de Topo.

Este registo possibilita auditoria eficaz e resposta célere a pedidos das autoridades competentes.

6 Atualização de Dados

A atualização da informação e dos elementos de identificação constitui um dever permanente no âmbito da relação de negócio. A IFTHENPAY assegura que os dados relativos aos clientes, seus representantes e beneficiários efetivos permanecem *exatos, completos e atualizados*, permitindo uma avaliação contínua do risco e garantindo que as operações realizadas se mantêm coerentes com o perfil declarado e com a atividade económica desenvolvida.

A atualização dos dados decorre de uma abordagem baseada no risco, sendo tanto mais frequente e exigente quanto maior for o risco inerente à relação de negócio. Para esse efeito, a IFTHENPAY implementa *mecanismos regulares de monitorização*, *procedimentos internos de deteção* de alterações relevantes e *processos formais de revisão periódica*, ajustados à tipologia e ao perfil de risco de cada cliente.

6.1 Atualização desencadeada pelo cliente

A IFTHENPAY exige que os clientes *comuniquem tempestivamente* qualquer alteração relevante que afete a relação de negócio, nomeadamente:

- mudança de identidade ou validade dos documentos de identificação;
- alteração da residência, domicílio fiscal ou sede social;
- modificação da atividade económica, incluindo início de novas atividades ou alteração de enquadramento fiscal;
- alteração da estrutura de propriedade ou controlo, incluindo mudanças em participações no capital e/ou nos direitos de voto iguais ou superiores a 5%;
- substituição de representantes legais ou membros dos órgãos sociais;
- alteração da qualidade de beneficiário efetivo;
- circunstâncias que impliquem a aquisição da qualidade de PEP por parte do cliente, representante, administrador ou beneficiário efetivo.

O *incumprimento* deste dever pode determinar a *suspensão da relação de negócio ou a sua cessação*, quando inviabilize o cumprimento dos deveres legais da IFTHENPAY.

6.2 Atualização desencadeada pela IFTHENPAY: revisões periódicas proporcionais ao risco

A IFTHENPAY realiza *revisões periódicas* da informação dos clientes, cuja periodicidade é definida com base no respetivo nível de risco:

- **Clientes de risco elevado → revisão periódica, pelo menos, anual (1 ano)**, podendo incluir recolha de documentação atualizada, comprovação adicional da origem dos fundos e nova análise da estrutura societária.
- **Clientes de risco médio → revisão periódica, pelo menos, trienal (3 anos)**, com validação de elementos essenciais e reconfirmação de beneficiário efetivo, atividade e poderes de representação.
- **Clientes de baixo risco → revisão periódica, pelo menos, quinquenal (5 anos)**, de forma focada e proporcional, com base em verificações documentais e nos mecanismos internos de suporte à análise.

Estas revisões permitem identificar incoerências, alterações não comunicadas, comportamentos atípicos ou novos fatores de risco.

6.3 Atualização desencadeada por eventos

Independentemente da periodicidade definida, a IFTHENPAY desencadeia um processo de atualização *sempre que*:

- os sistemas automáticos detetem alertas relevantes (sanções, PEP, listas restritivas, monitorização de operações);
- sejam verificadas alterações no RCBE ou no registo comercial;
- sejam detetadas divergências significativas entre operações realizadas e perfil declarado;
- existam mudanças repentinas na atividade económica ou estrutura da entidade;
- surjam notícias, publicações reputacionais ou informações provenientes de autoridades que afetem o risco do cliente.

Nestes casos, a IFTHENPAY pode solicitar:

- documentos de identificação atualizados;
- comprovativos de morada;
- documentos societários atualizados;
- nova informação sobre beneficiários efetivos;
- declarações formais de esclarecimento;
- documentação que ateste a origem dos rendimentos dos beneficiários efetivos da entidade.

6.4 Atualização do beneficiário efetivo

A IFTHENPAY atualiza os dados relativos ao beneficiário efetivo sempre que:

- ocorram alterações na estrutura de propriedade ou controlo;
- sejam detetadas discrepâncias com o RCBE;
- existam novas participações qualificadas (≥ 25%);
- seja identificada, supervenientemente, qualidade de PEP ou ligação a jurisdições de risco elevado.

A instituição pode exigir documentação adicional para verificar a alteração, nomeadamente organogramas atualizados, atas, certidões recentes ou documentos equivalentes.

6.5 Inexistência ou insuficiência de atualização

Quando o cliente não fornece a informação ou documentação necessária para manter os dados atualizados, a IFTHENPAY avalia:

- o impacto no risco da relação de negócio;
- a eventual necessidade de aplicar medidas reforçadas;
- a possibilidade de suspensão da relação de negócio;
- a cessação da relação quando não seja possível cumprir de forma adequada os deveres de identificação e diligência.

A *persistência de falta de colaboração* pode determinar a *recusa de operações*, a *suspensão do serviço* ou o *encerramento da conta*, em conformidade com a lei e com o risco concreto observado.

6.6 Registo e documentação

Todos os processos de atualização de dados são registados e documentados, assegurando:

- rastreabilidade das alterações analisadas;
- evidência das diligências realizadas;
- fundamentação das decisões tomadas;
- suporte documental adequado para auditoria interna e supervisão externa.

7 Medidas Simplificadas

Nos termos do artigo 35.º da Lei n.º 83/2017, as medidas simplificadas de identificação e diligência apenas podem ser aplicadas quando, após avaliação baseada no risco, se conclua pela existência de um risco comprovadamente reduzido de branqueamento de capitais ou financiamento do terrorismo.

Contudo, considerando que:

- a IFTHENPAY estabelece todas as relações de negócio exclusivamente por meios não presenciais,
- o artigo 38.º da Lei n.º 83/2017 autonomiza a contratação à distância como situação que exige a adoção de medidas reforçadas,
- o artigo 35.º n.º 2 proíbe a aplicação de medidas simplificadas sempre que devam ser aplicadas medidas reforçadas,
- a natureza da atividade e o modelo tecnológico da instituição exigem níveis acrescidos de diligência, transparência e validação documental,

a IFTHENPAY conclui que *não se verificam, na sua atividade, circunstâncias que permitam classificar o risco como reduzido* de forma a justificar a adoção de medidas simplificadas.

Assim, a *IFTHENPAY* ***não prevê, como regra****, a aplicação medidas simplificadas de identificação e diligência*, aplicando sempre medidas normais ou reforçadas, em conformidade com o risco identificado.

8 Medidas Reforçadas (EDD – Enhanced Due Diligence)

Quando, na sequência da avaliação baseada no risco, a IFTHENPAY conclua que o cliente, a estrutura societária, a atividade económica, a geografia associada, o comportamento observado ou a finalidade da relação de negócio envolvem risco elevado de branqueamento de capitais ou financiamento do terrorismo, são obrigatoriamente aplicadas medidas reforçadas de identificação, verificação e monitorização, em conformidade com o disposto nos artigos 28.º e 29.º da Lei n.º 83/2017.

As medidas reforçadas têm por objetivo assegurar um grau acrescido de segurança, transparência e compreensão da relação de negócio, garantindo que a IFTHENPAY dispõe de informação sólida e fiável sobre:

- quem é o cliente e os seus intervenientes relevantes;
- qual a origem dos fundos e, quando necessário, a origem do património;
- qual a natureza económica da atividade exercida;
- qual a finalidade da relação de negócio e a expectativa transacional;
- se a estrutura societária ou cadeia de controlo é legítima, transparente e consistente;

- se os riscos identificados podem ser mitigados de forma adequada.

A aplicação de medidas reforçadas é cumulativa e ajustada à natureza e à materialidade do risco identificado.

8.1 Situações que obrigam à aplicação de medidas reforçadas

A IFTHENPAY aplica medidas reforçadas, designadamente, quando:

- o cliente, representante, beneficiário efetivo ou titular de participação qualificada seja PEP, membro próximo da família ou pessoa estreitamente associada;
- o cliente seja classificado internamente como de risco elevado, nos termos da matriz de risco adoptada pela IFTHENPAY;
- existam ligações a jurisdições de risco elevado, países sancionados, países terceiros não cooperantes ou geografias com deficiências estratégicas em matéria de BCFT;
- a estrutura societária seja complexa, multinível, dispersa, envolva entidades interpostas sem substância económica, ou seja difícil identificar o beneficiário efetivo;
- haja inconsistências significativas entre a informação fornecida pelo cliente e a obtida em fontes independentes;
- o cliente exerça atividade económica com risco intrínseco elevado;
- o perfil transacional expectável seja atípico, desproporcional ou incoerente com o enquadramento declarativo;
- existam indícios de tentativa de fraude documental, manipulação ou ocultação de identidade;
- o cliente exerça ou desempenhe funções em sectores sensíveis a BCFT;
- se identifiquem alertas provenientes dos sistemas de filtragem relativos a potenciais correspondências com listas de sanções, listas restritivas ou media adversa, até que a correspondência seja confirmada ou descartada.

A existência de alertas de sanções determina a adoção de medidas reforçadas de verificação. A confirmação de correspondência verdadeira/positiva determina recusa obrigatória.

8.2 Recolha de informação adicional sobre o cliente, estrutura e atividade

A IFTHENPAY recolhe informação suplementar proporcional ao risco, incluindo, sempre que necessário:

- documentação adicional sobre a constituição da entidade, estatutos, atas, acordos parassociais ou organogramas;
- clarificação da estrutura de propriedade e controlo, incluindo entidades intermédias;
- informação mais detalhada sobre a atividade económica efetivamente exercida;
- comprovativos adicionais relativos ao estabelecimento físico ou presença económica;
- análise de fontes independentes para confirmar informações reputacionais e societárias.

8.3 Verificação reforçada da origem dos fundos e, quando necessário, da origem do património

Dependendo do risco, a IFTHENPAY pode exigir:

- comprovativos documentais da origem dos fundos (i.e. faturas, contratos, extratos bancários, demonstrações financeiras, contratos de prestação de serviços, etc.);
- informação sobre as fontes de rendimento do cliente ou da entidade;
- documentos que permitam verificar a origem do património, quando adequado ao perfil e risco (ex.: venda de empresa, herança, poupança acumulada, rendimento empresarial).

Este processo visa garantir que os fundos movimentados são compatíveis com a atividade conhecida e não representam risco não mitigável.

8.4 Compreensão reforçada da finalidade e natureza da relação de negócio

A IFTHENPAY recolhe informação adicional sobre:

- o propósito concreto da adesão aos serviços de pagamento;
- o modelo operacional do cliente;
- os fluxos financeiros esperados;
- os países envolvidos na cadeia operacional;
- a forma como o serviço da IFTHENPAY será utilizado;
- a compatibilidade entre a finalidade declarada e a atividade económica real.

Quando a finalidade não possa ser esclarecida de forma satisfatória, a relação de negócio não poderá ser estabelecida.

8.5 Validação reforçada dos intervenientes relevantes

A IFTHENPAY reforça a verificação:

- da identidade dos titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5%;
- da identidade e legitimidade dos representantes legais;
- da identidade do beneficiário efetivo e respetiva cadeia de controlo;
- da existência de controlos indiretos, acordos de voto, estruturas fiduciárias ou situações de influência dominante.

Sempre que existam dúvidas, são exigidos comprovativos adicionais.

8.6 Monitorização reforçada da relação de negócio

Após aceitação, a IFTHENPAY sujeita o cliente a monitorização contínua reforçada, que inclui:

- análise humana qualificada;
- revisão periódica mais frequente dos elementos de identificação;
- atualizações regulares da informação sobre origem dos fundos e operações;
- análise de padrões transacionais e deteção de desvios significativos;
- revisão independente da consistência das operações com o perfil declarado;
- filtragem contínua em listas de sanções e de PEP;
- reavaliação do risco sempre que ocorram eventos relevantes.

Em caso de deteção de risco não mitigável, a relação pode ser suspensa ou cessada.

8.7 Escalonamento (CO → RCN → Direção de Topo)

Nos casos que exijam medidas reforçadas:

1. O *Helpdesk* identifica o fator de risco e encaminha o processo.
2. O CO conduz as diligências reforçadas iniciais, recolhe documentação adicional e avalia a coerência da informação.
3. O RCN reavalia a informação, valida a análise e emite parecer técnico.
4. A Direção de Topo decide sobre a aceitação ou recusa, quando exigido por lei ou pelo modelo de risco.

Nenhuma relação de negócio de risco elevado pode ser estabelecida sem a intervenção das 2.ª e 3.ª linhas, e sem aprovação formal da Gerência quando aplicável.

8.8 Decisão e documentação

A decisão final deve ser documentada de forma completa, incluindo:

- fatores de risco identificados;
- diligências adicionais realizadas;
- documentação recolhida;
- fundamentação da decisão;
- medidas de mitigação aplicadas;
- plano de monitorização reforçada.

A falta de informação suficiente ou a impossibilidade de mitigar adequadamente os riscos determina a recusa da relação de negócio.

9 Dever de Recusa por Incumprimento do KYC

A IFTHENPAY deve *recusar* o estabelecimento da relação de negócio sempre que *não seja possível cumprir*, de forma adequada e satisfatória, os deveres de *identificação e diligência* previstos na Lei n.º 83/2017, no Aviso do Banco de Portugal n.º 1/2022 e nas presentes políticas internas.

A recusa constitui um *dever legal* e não uma faculdade, aplicável sempre que subsistam dúvidas fundadas quanto à identidade do cliente, dos seus representantes, dos titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5% ou do(s) beneficiário(s) efetivo(s), ou quando não seja possível compreender adequadamente a natureza e finalidade da relação de negócio.

9.1 Situações que determinam obrigatoriamente a recusa

A IFTHENPAY deve recusar a adesão quando se verifique qualquer um dos seguintes cenários:

a) Falta de identificação adequada

- inexistência de documentação de identificação válida;
- apresentação de documentos ilegíveis, caducados, incoerentes ou cuja autenticidade seja duvidosa;

- impossibilidade de verificar a identidade através de meios independentes ou complementares.

b) Falta de verificação do beneficiário efetivo

- impossibilidade de identificar ou verificar o beneficiário efetivo;
- discrepâncias materiais entre RCBE, documentos apresentados e informação prestada;
- ocultação deliberada da estrutura societária ou de controlo.

c) Falta de informação necessária sobre a finalidade e natureza da relação

- ausência de elementos suficientes para compreender a atividade económica do cliente;
- incoerências entre a atividade declarada e os documentos fornecidos;
- falta de resposta a pedidos de esclarecimento considerados essenciais.

d) Falta de colaboração ou resposta insuficiente

- omissão reiterada de documentos exigidos;
- respostas evasivas, contraditórias ou incompletas;
- recusa expressa ou implícita em fornecer informação relevante.

e) Impossibilidade de mitigar risco elevado

Mesmo após aplicação de medidas reforçadas, deve ocorrer recusa quando:

- persistem riscos não mitigáveis;
- a origem dos fundos ou do património não é esclarecida;
- a atividade ou modelo de negócios é incompatível com o apetite de risco da instituição.

f) Deteção de indícios de criminalidade ou suspeição

- indícios de branqueamento, financiamento do terrorismo, fraude documental ou atividade ilícita;
- evidência de ligação a jurisdições sancionadas, não cooperantes ou de risco elevado;
- associação a listas de sanções internacionais.

9.2 Procedimento interno de recusa

A recusa deve obedecer ao seguinte fluxo:

1. *Helpdesk* identifica o incumprimento ou risco não mitigável e encaminha o processo.
2. *CO* analisa o caso, solicita elementos adicionais e fundamenta a recomendação.
3. *RCN* valida a análise e emite parecer final.
4. *Gerência* intervém quando o caso envolve matérias de risco elevado ou clientes sujeitos a aprovação superior.
5. A decisão é comunicada ao proposto cliente por meios formais e adequados.

9.3 Documentação e registo

Cada decisão de recusa deve ser:

- integralmente documentada;
- fundamentada em elementos verificáveis;
- arquivada em suporte duradouro;
- acompanhada da informação recolhida durante o processo de diligência.

Este registo assegura rastreabilidade e permite auditoria interna e supervisão externa.

9.4 Avaliação de suspeição

A recusa por incumprimento do KYC **não invalida**, quando aplicável, a análise de eventual comunicação de suspeita ao abrigo do artigo 43.º da Lei n.º 83/2017.

Sempre que a recusa resulte de:

- ocultação de identidade,
- inconsistências graves,
- risco elevado não mitigável,
- sinais de criminalidade,

o caso deve ser avaliado nos termos da Política de Comunicação de Operações Suspeitas.

9.5 Proibição de "início condicionado"

Em linha com a legislação aplicável **não é permitido iniciar a relação de negócio antes da conclusão integral e satisfatória do processo de identificação e diligência.**

Em nenhum caso se admite ativar serviços, funcionalidades ou meios de pagamento antes da verificação completa do cliente e respetiva aprovação interna, quando aplicável.

V. POLÍTICA DE ANÁLISE E MONITORIZAÇÃO DE ENTIDADES DE RISCO ELEVADO

A monitorização das entidades classificadas como de risco elevado constitui uma componente essencial do sistema de prevenção do BCFT da IFTHENPAY, permitindo detetar, avaliar e reagir de forma proporcional a operações, comportamentos ou alterações que possam indiciar risco acrescido.

Esta política assegura que os clientes de risco elevado são objeto de controlo reforçado, contínuo e documentado, fundamentado numa abordagem baseada no risco e alinhado com a legislação e regulamentação aplicável.

1 Princípios da abordagem baseada no risco

A IFTHENPAY aplica uma *abordagem baseada no risco* a todas as relações de negócio, reforçando os mecanismos de monitorização nos casos em que, pela natureza da atividade, perfil do cliente, estrutura de propriedade, geografia associada, finalidade da relação ou padrões transacionais, se conclua pela existência de risco elevado de branqueamento de capitais ou financiamento do terrorismo.

Os princípios aplicáveis são:

- *Proporcionalidade*: a intensidade da monitorização aumenta de acordo com o risco identificável;
- *Continuidade*: a monitorização é permanente, não se esgotando no momento de onboarding;
- *Atualização dinâmica*: o nível de risco pode ser revisto quando surgem novos elementos relevantes;
- *Rastreabilidade*: todas as decisões e análises são documentadas em suporte duradouro;
- *Intervenção escalonada*: quanto maior o risco, maior o envolvimento das funções de controlo e da Direção de Topo.

2 Classificação de risco

A classificação de risco elevado resulta da combinação de fatores inerentes ao cliente, à atividade, à geografia, ao canal e ao comportamento transacional, incluindo, designadamente:

- ligação a jurisdições de risco elevado, sancionadas ou não cooperantes;
- qualidade de PEP, titular de outro cargo político ou público, membro próximo da família ou pessoa estreitamente associada;
- estrutura societária complexa ou opaca, sem racional económico evidente;
- atividade económica sensível ou inserida em setores altamente expostos;
- histórico reputacional negativo;
- utilização de modelos operacionais suscetíveis de ocultação de origem de fundos;
- incoerências nos documentos ou nas informações prestadas;
- alterações repentinas no padrão operativo esperado.

A classificação é determinada por modelo interno automatizado, complementado pela avaliação humana (CO e RCN), sendo revista periodicamente ou sempre que surjam novos fatores de risco.

3 Pré-aprovação e Enhanced Due Diligence (EDD)

Nenhum cliente classificado como de risco elevado pode ser aceite sem:

1. análise técnica do CO;
2. validação pelo RCN;
3. aprovação da Direção de Topo nos casos previstos na Lei 83/2017 e nesta Política.

A EDD aplicável a entidades de risco elevado segue os princípios definidos no Capítulo IV, incluindo verificação reforçada da identidade, estrutura societária, beneficiários efetivos, origem dos fundos e finalidade da relação de negócio.

4 Monitorização contínua

Os clientes de risco elevado são sujeitos a um regime de *monitorização reforçada ao longo da relação de negócio*, concretizada através de:

a) Alertas automáticos

O sistema interno (ifprod e módulos de filtragem) avalia diariamente:

- correspondências com listas de sanções, PEPs e listas restritivas;
- operações fora do padrão esperado;
- alertas de risco gerados pelas regras parametrizadas/indicadores do ifprod acerca de perfis transacionais.

b) Análise humana qualificada

Sempre que um alerta automático é gerado:

- o CO analisa a pertinência, gravidade e contexto;
- solicita documentação adicional ao cliente sempre que necessário;
- determina se existe fundamento para escalonamento.

c) Reavaliação periódica obrigatória

Clientes de risco elevado são reavaliados com maior frequência do que os restantes, incluindo:

- reconfirmação da identidade e estrutura societária;
- atualização de beneficiários efetivos;
- revisão da atividade económica e do perfil transacional;
- validação de origem e destino dos fundos quando aplicável.

5 Escalonamento interno (CO → RCN → Direção de Topo)

A monitorização reforçada pode originar escalonamento interno quando:

- haja sinais de risco agravado;
- se detete incoerência grave entre operações e perfil declarado;
- resulte suspeita de branqueamento ou financiamento do terrorismo;
- se identifique necessidade de comunicar operação suspeita (COS) ou atividade suspeita (CAS).

Fluxo:

1. CO reúne os elementos e emite parecer.
2. RCN valida e determina a ação adequada.
3. Direção de Topo intervém nos casos que envolvam decisões estruturantes, aprovação de PEPs ou eventuais cessões de relação.

6 Ações de controlo ativo reforçado

Dependendo do risco, a IFTHENPAY pode aplicar uma ou mais das seguintes medidas:

- intensificação da monitorização transacional;
- solicitação periódica de comprovativos adicionais;
- limitação de funcionalidades ou de volume transacional;
- suspensão temporária de operações;
- recomendação de atualização de informação ou documentação;
- realização de revisões temáticas focadas;
- imposição de medidas adicionais de mitigação caso a caso.

7 Fatores de risco inerentes ao cliente, produto, geografia ou canal

Os fatores abaixo elencados aplicam-se exclusivamente a *atividades e modelos de negócio admitidos pela IFTHENPAY*, mas que, pela sua natureza, estrutura ou operacionalização, podem justificar a classificação do cliente como de risco elevado e a aplicação de medidas de controlo e monitorização reforçadas.

São, designadamente, suscetíveis de agravar o risco:

- modelos de negócio assentes em elevado volume de microtransações, com grande dispersão de ordenantes e beneficiários finais, dificultando a leitura agregada dos fluxos financeiros;
- atividades com forte componente internacional, incluindo a realização frequente de pagamentos transfronteiriços, ainda que envolvendo jurisdições não classificadas como de risco elevado;
- clientes que operem em setores caracterizados por elevada rotatividade de fundos, ciclos financeiros curtos ou margens reduzidas, potenciando uma circulação acelerada de valores;
- estruturas societárias que integrem entidades em múltiplas jurisdições, mesmo quando cooperantes, sempre que tal dificulte a identificação clara e imediata do beneficiário efetivo ou da cadeia de controlo;

- recurso sistemático a intermediários, agentes ou parceiros comerciais, quando esse recurso reduza a visibilidade direta da IFTHENPAY sobre a relação económica subjacente ou sobre os intervenientes finais;
- alterações frequentes ou pouco transparentes ao modelo operacional, à atividade declarada ou à estrutura societária, sem justificação económica clara;
- crescimento rápido, inesperado ou desproporcional do volume transacional, face ao perfil inicialmente declarado e validado;
- comportamentos transacionais atípicos, ainda que não ilícitos, mas incompatíveis com o padrão esperado para o setor, a atividade ou o perfil do cliente.

A verificação de um ou mais destes fatores determina a aplicação de medidas reforçadas de monitorização, sem prejuízo da eventual reavaliação da admissibilidade da relação de negócio sempre que o risco se revele não mitigável.

8 Medidas restritivas e sanções

Se a monitorização identificar correspondência confirmada com:

- listas de sanções internacionais;
- medidas restritivas europeias ou das Nações Unidas;
- medidas setoriais que proíbam a prestação de serviços financeiros;

então:

- a relação de negócio não poderá ser estabelecida ou deverá ser imediatamente cessada;
- os fundos eventualmente envolvidos devem ser congelados, se aplicável;
- as autoridades competentes devem ser notificadas nos termos da lei.

VI. DEVERES OPERACIONAIS

Os deveres operacionais constituem o núcleo funcional do sistema de prevenção do BCFT da IFTHENPAY, traduzindo-se em obrigações permanentes de controlo, identificação, diligência, monitorização, comunicação, conservação e colaboração com as autoridades competentes. A atuação operacional decorre da Lei n.º 83/2017, do Aviso do Banco de Portugal n.º 1/2022 e das presentes políticas internas.

1 Dever de controlo

A IFTHENPAY assegura o cumprimento do Regulamento (UE) 2023/1113 (aplicável desde 30-12-2024, revogando o Regulamento (UE) 2015/847 a partir dessa data), designadamente no que respeita à transmissão, conservação e disponibilização de informações sobre o ordenante e o beneficiário das transferências de fundos, através dos sistemas internos e da articulação com prestadores de serviços de pagamento parceiros.

A IFTHENPAY assegura mecanismos de controlo proporcionais ao risco e adequados ao seu modelo de negócio, incluindo:

a) Modelos de risco

Modelos automáticos de avaliação e classificação de risco de clientes e transações, ajustados às orientações setoriais e às boas práticas internacionais.

b) Ferramentas tecnológicas

Sistemas de filtragem e monitorização integrados (sanções, PEPs, listas restritivas, perfis transacionais), operando 24/7 e gerando alertas categorizados.

c) Decisões documentadas

Todas as decisões relevantes em matéria de controlo (aceitação, recusa, suspensão, escalonamento) são devidamente registadas e armazenadas em suporte duradouro.

2 Dever de identificação e diligência

A IFTHENPAY cumpre os deveres de identificação e diligência previstos na Lei n.º 83/2017, no Aviso do Banco de Portugal n.º 1/2022 e no Capítulo IV da presente Política, assegurando que ambos são aplicados de forma coerente, adequada e proporcional ao risco associado a cada relação de negócio.

O dever de identificação e diligência:

- aplica-se antes do estabelecimento da relação de negócio e mantém-se ao longo de toda a sua duração;
- é atualizado sempre que ocorram alterações relevantes;
- é reforçado quando se identifiquem fatores de risco acrescido.

Qualquer incumprimento, insuficiência ou impossibilidade de cumprimento adequado destes deveres determina a aplicação das medidas previstas no Capítulo IV, incluindo a recusa,

suspensão ou cessação da relação de negócio, sem prejuízo das obrigações de comunicação às autoridades competentes, quando aplicável.

3 Dever de recusa

A recusa é obrigatória sempre que a IFTHENPAY não consiga, de forma adequada e satisfatória, cumprir os deveres de identificação e diligência, ou quando subsistam dúvidas fundadas sobre:

- a identidade do cliente, do(s) seu(s) representante(s) ou do(s) beneficiário(s) efetivo(s) e/ou titulares de participações no capital e/ou nos direitos de voto iguais ou superiores a 5%;
- a legitimidade, transparência ou coerência da estrutura societária e dos poderes de representação;
- a origem dos fundos ou do património, quando aplicável;
- a compatibilidade da atividade exercida ou do modelo operacional com o apetite de risco da instituição;
- a possibilidade de mitigar adequadamente um risco classificado como elevado;
- a falta de colaboração do cliente na prestação de informação ou documentação essencial;
- a confirmação de inclusão do cliente ou de intervenientes relevantes em listas de sanções internacionais que proíbam a prestação de serviços financeiros.

A recusa segue o procedimento previsto no Capítulo IV, secção 9, sem prejuízo da avaliação da eventual necessidade de comunicação às autoridades competentes, nos termos legais aplicáveis.

4 Dever de exame

A IFTHENPAY procede à análise, com especial atenção, de quaisquer operações ou comportamentos transacionais que, pela sua natureza, complexidade, irregularidade, ausência de fundamento económico aparente ou incoerência com o perfil conhecido do cliente, possam indiciar risco de branqueamento de capitais ou de financiamento do terrorismo.

O dever de exame é exercido de forma contínua e proporcional ao risco, incidindo, designadamente, sobre:

- a análise da operação no contexto do histórico e do perfil transacional do cliente;
- a solicitação de esclarecimentos ou informações adicionais ao cliente, quando adequado;
- a verificação documental, sempre que aplicável;
- o registo fundamentado da análise efetuada e da decisão adotada.

Sempre que, após o exame, subsistam dúvidas fundadas quanto à licitude da operação ou à sua compatibilidade com o perfil do cliente, deve ser ponderada, de forma fundamentada, a comunicação de suspeita às autoridades competentes, nos termos legais aplicáveis.

A decisão final resulta sempre de apreciação humana fundamentada.

5 Dever de comunicação (COS, CAS e comunicações sistemáticas)

A IFTHENPAY informa de imediato o Departamento Central de Investigação e Ação Penal (DCIAP) e a Unidade de Informação Financeira (UIF) sempre que saiba, suspeite ou tenha razões suficientes para suspeitar que determinados fundos ou outros bens provêm de atividade criminosa ou estão relacionados com o financiamento do terrorismo, nos termos do artigo 43.º da Lei n.º 83/2017.

A comunicação é efetuada logo que a suspeita se forme, preferencialmente no momento em que a operação é proposta, assegurando-se um circuito interno simples, ágil e com o mínimo de intervenientes.

a) Comunicação de Operações Suspeitas (COS)

A IFTHENPAY comunica todas as *operações propostas*, bem como quaisquer operações *tentadas*, *em curso ou executadas*, relativamente às quais existam indícios ou suspeitas fundadas de branqueamento de capitais ou de financiamento do terrorismo, através dos canais definidos pelas autoridades competentes e com o conteúdo mínimo legalmente exigido.

b) Comunicação de Atividade Suspeita (CAS)

Sempre que a suspeita incida não apenas sobre uma operação isolada, mas sobre a *atividade, o padrão comportamental, o modelo de negócio ou a estrutura operacional do cliente*, suscetíveis de enquadrar uma tipologia penal relevante, a IFTHENPAY procede à comunicação de atividade suspeita (CAS), enquanto modalidade prática de comunicação efetuada ao abrigo do artigo 43.º da Lei n.º 83/2017, nos termos adotados pela Unidade de Informação Financeira.

c) Comunicação sistemática de operações

Sem prejuízo das comunicações baseadas em suspeita, a IFTHENPAY cumpre igualmente, quando legal ou regulamentarmente aplicável, a obrigação de comunicação *numa base sistemática* ao DCIAP e à UIF de tipologias de operações definidas por portaria competente, nos termos do artigo 45.º da Lei n.º 83/2017, observando os requisitos de forma, prazo e conteúdo legalmente estabelecidos.

d) Confidencialidade, registo e conservação

As comunicações efetuadas ao abrigo do presente dever são tratadas de forma confidencial, sendo proibida qualquer divulgação ao cliente ou a terceiros da sua existência ou conteúdo.

A IFTHENPAY conserva cópias das comunicações efetuadas e mantém-nas permanentemente disponíveis para as autoridades competentes, nos termos do artigo 51.º da Lei n.º 83/2017.

6 Dever de abstenção

A IFTHENPAY abstém-se de executar operações sempre que, existindo suspeitas fundadas de branqueamento de capitais ou de financiamento do terrorismo, a respetiva execução seja suscetível de frustrar a comunicação às autoridades competentes ou comprometer a investigação em curso, pelo período estritamente necessário.

O dever de abstenção aplica-se, designadamente, quando:

- estejam em curso diligências de exame ou análise que justifiquem a suspensão da execução da operação;
- o risco identificado se revele não mitigável por outras medidas adequadas;
- a execução imediata da operação possa prejudicar a eficácia da comunicação ou da investigação criminal.

Em casos excecionais, a operação pode ser executada quando a abstenção seja suscetível de frustrar a investigação ou quando tal seja expressamente determinado pelas autoridades competentes, devendo a decisão ser precedida de consulta ao RCN e devidamente fundamentada e registada.

7 Dever de colaboração

A IFTHENPAY presta, de forma pronta, completa e diligente, a colaboração que lhe seja requerida pelo DCIAP, pela UIF, pelas demais autoridades judiciárias e policiais, pelas autoridades setoriais competentes e pela Autoridade Tributária e Aduaneira, no âmbito das respetivas atribuições.

Em cumprimento deste dever, a IFTHENPAY assegura, designadamente:

- a resposta completa, fidedigna e no prazo fixado a pedidos de informação relativos a relações de negócio mantidas ou cessadas, à sua natureza e às operações associadas;
- a disponibilização, nos termos legalmente exigidos, de todas as informações, documentos e elementos relevantes que lhe sejam solicitados, independentemente do respetivo suporte;
- o acesso remoto ou local à informação conservada, sempre que legalmente requerido;
- a cooperação plena no exercício de ações inspetivas, abstendo-se de quaisquer condutas obstrutivas ilegítimas e garantindo o acesso às instalações, sistemas e colaboradores relevantes;
- o cumprimento, integral e atempado, de determinações, ordens, instruções ou recomendações que lhe sejam dirigidas pelas autoridades competentes.

O dever de colaboração é exercido com observância das exigências de confidencialidade, segurança da informação e proteção de dados pessoais, nos termos legais aplicáveis, não estando condicionado ao exercício prévio do dever de comunicação de operações suspeitas.

8 Dever de não divulgação (tipping-off)

A IFTHENPAY, bem como os membros dos seus órgãos sociais, colaboradores, mandatários e quaisquer pessoas que lhe prestem serviços, a título permanente, temporário ou ocasional,

estão sujeitos ao dever de não divulgação, sendo-lhes vedado revelar ao cliente ou a terceiros, designadamente:

- que foi, está a ser ou poderá vir a ser efetuada qualquer comunicação legalmente devida às autoridades competentes, incluindo comunicações de operações ou atividades suspeitas;
- quaisquer informações relacionadas com essas comunicações, ainda que resultem de análises internas ou de pedidos formulados por autoridades judiciais, policiais ou setoriais;
- que se encontra ou possa vir a encontrar-se em curso uma investigação, inquérito, averiguação ou qualquer outro procedimento legal relacionado com a prevenção ou repressão do branqueamento de capitais ou do financiamento do terrorismo.

A IFTHENPAY atua com a necessária prudência na interação com clientes relacionados com operações potencialmente suspeitas, evitando diligências ou comunicações que possam, direta ou indiretamente, suscitar a perceção da existência de procedimentos internos de análise ou de comunicações às autoridades.

As exceções ao dever de não divulgação apenas são admissíveis nos casos expressamente previstos na lei, nomeadamente para efeitos de cooperação entre entidades e autoridades legalmente habilitadas, ou quando impostas por dever legal ou regulamentar, devendo, sempre que aplicável, ser objeto de enquadramento jurídico adequado e de registo interno.

Sempre que, por força do dever de não divulgação, a IFTHENPAY se deva abster da realização de diligências adicionais junto do cliente, procede de imediato ao cumprimento do dever de comunicação às autoridades competentes, com base na informação disponível no momento.

9 Dever de conservação

A IFTHENPAY conserva, pelo período legalmente exigido, os elementos e documentação obtidos ou produzidos no âmbito do cumprimento dos deveres previstos na presente Política e na Lei n.º 83/2017, designadamente:

- os elementos, cópias, registos ou dados eletrónicos relativos à identificação e diligência dos clientes, dos seus representantes, beneficiários efetivos e demais intervenientes relevantes, por um período de sete anos após o momento em que a identificação se processou ou, no caso de relações de negócio, após o respetivo termo;
- os documentos, registos e demais elementos comprovativos das operações realizadas, de forma a permitir a sua integral reconstituição, por um período de sete anos a contar da respetiva execução, ainda que a relação de negócio já tenha cessado;
- as análises, relatórios, comunicações, pareceres e demais documentação interna ou externa que formalize o cumprimento das obrigações em matéria de BCFT, por um período de sete anos ou por prazo superior, sempre que tal seja imposto por autoridade competente ou resulte de outras obrigações legais aplicáveis.

A conservação é efetuada em suporte duradouro, com preferência por meios eletrónicos, em condições que assegurem a integridade, confidencialidade, rastreabilidade e controlo de acessos, garantindo a adequada conservação, fácil localização e o acesso imediato aos

elementos conservados sempre que solicitados pela UIF, pelas autoridades judiciárias, policiais e setoriais competentes ou pela Autoridade Tributária e Aduaneira (AT).

10 Dever de formação

A IFTHENPAY assegura que os membros dos seus órgãos sociais, dirigentes, trabalhadores e demais colaboradores cujas funções sejam relevantes para efeitos da prevenção do branqueamento de capitais e do financiamento do terrorismo dispõem de conhecimento adequado das obrigações legais, regulamentares e internas aplicáveis, em função da natureza das suas funções e do risco associado.

Para o efeito, a IFTHENPAY garante, designadamente:

- formação inicial adequada, ministrada no momento da admissão ou do início de funções relevantes, abrangendo as políticas, procedimentos e controlos internos em matéria de BCFT;
- formação periódica obrigatória, ajustada às funções desempenhadas e ao perfil de risco da instituição;
- ações formativas específicas e temáticas, incluindo, entre outras, matérias relativas a PEPs, sanções e medidas restritivas, RCBE, diligência reforçada, deteção de operações e atividades suspeitas e deveres de comunicação;
- a realização de ações de formação internas ou externas asseguradas por pessoas ou entidades com reconhecida competência e experiência no domínio do BCFT, precedidas, quando aplicável, de parecer favorável do RCN;
- a manutenção de registos completos e atualizados das ações de formação realizadas, incluindo conteúdos, datas, participantes, assiduidade e, quando aplicável, avaliação, conservados nos termos do dever de conservação e disponibilizados às autoridades setoriais sempre que solicitado.

O plano de formação é definido com base no mapa de riscos BCFT da IFTHENPAY e revisto sempre que se verifiquem alterações relevantes nesse perfil.

11 Proteção de dados pessoais (RGPD)

O tratamento de dados pessoais efetuado pela IFTHENPAY no âmbito da prevenção do branqueamento de capitais e do financiamento do terrorismo assenta no cumprimento de obrigações legais a que a instituição se encontra sujeita e prossegue uma finalidade de interesse público importante, nos termos da Lei n.º 83/2017 e do Regulamento (UE) 2016/679.

O tratamento de dados pessoais no âmbito do sistema BCFT:

- tem fundamento jurídico no cumprimento de obrigações legais e regulamentares;
- tem como finalidade exclusiva a prevenção do branqueamento de capitais, do financiamento do terrorismo e do financiamento da proliferação de armas de destruição em massa, não podendo ser utilizado para fins comerciais;
- obedece aos princípios da licitude, minimização, adequação, integridade, confidencialidade e segurança;

- limita-se aos dados estritamente necessários ao cumprimento dos deveres preventivos legalmente previstos, incluindo dados de identificação, dados financeiros, dados relativos à atividade económica, estrutura de controlo, beneficiário efetivo, operações realizadas e, quando aplicável, informação sobre suspeitas ou comunicações às autoridades;
- é efetuado sob responsabilidade da IFTHENPAY, enquanto responsável pelo tratamento, que adota medidas técnicas e organizativas adequadas para garantir a proteção física e lógica dos dados tratados.

O exercício do direto de apagamento dos dados pessoais tratados no âmbito BCFT encontra-se limitado enquanto subsistirem *deveres legais de conservação*, sendo eliminados após o decurso dos prazos legalmente aplicáveis, sem prejuízo de outras obrigações legais de retenção.

O exercício dos direitos de acesso e retificação pelos titulares dos dados é efetuado nos termos legalmente previstos, através da Comissão Nacional de Proteção de Dados (CNPD), podendo tais direitos ser limitados nas situações legalmente previstas, designadamente quando tal se revele necessário para salvaguardar investigações, análises ou comunicações às autoridades competentes.

Os dados pessoais tratados ao abrigo da presente Política podem ser comunicados, transmitidos ou objeto de interconexão, nos termos da lei, com o DCIAP, a UIF, a AT, as autoridades judiciais, policiais e setoriais competentes, bem como com outras entidades legalmente habilitadas, incluindo entidades do mesmo grupo, quando aplicável.

VII. SISTEMAS DE INFORMAÇÃO, MONITORIZAÇÃO E SEGURANÇA TECNOLÓGICA

1 Arquitetura de sistemas

A IFTHENPAY suporta a execução do serviço de pagamentos e o cumprimento das obrigações preventivas em matéria de BCFT através de um sistema central de informação e registo operacional (ifprod), no qual se encontram consolidados, designadamente, os dados de identificação e caracterização dos clientes, os elementos relevantes das operações processadas, bem como informação de suporte à monitorização, filtragem e análise, em linha com a abordagem baseada no risco.

O sistema ifprod permite, em particular:

- o registo estruturado dos dados dos clientes e respetivos perfis, incluindo a manutenção e atualização de informação relevante para efeitos de identificação e diligência;
- o registo e consulta de operações, estatísticas e tabelas de monitorização, de forma a suportar a deteção de padrões atípicos e a análise de eventos de risco;
- a execução de mecanismos automáticos de filtragem associados a sanções e PEPs, bem como o registo do tratamento e fundamentação de alertas;
- a manutenção de registos internos associados a processos de exame e decisões adotadas no âmbito BCFT, assegurando evidência suficiente e rastreabilidade.

O processo de estabelecimento de relação de negócio é efetuado de forma não presencial, através de receção de contrato e documentação comprovativa, com validação humana por equipas internas, incluindo a verificação de completude, coerência e conformidade formal dos elementos apresentados, e, quando necessário, a solicitação de documentação adicional junto do cliente por canais de comunicação adequados.

A arquitetura de sistemas e os mecanismos de registo e evidência são concebidos e mantidos de forma a assegurar a integridade da informação, a rastreabilidade das operações e decisões relevantes e a capacidade de demonstração perante as autoridades competentes.

2 Segurança, acessos e segregação

O acesso aos sistemas de informação relevantes para a prestação do serviço de pagamentos e para o cumprimento das obrigações em matéria de BCFT é concedido de forma restrita, controlada e proporcional às funções efetivamente exercidas por cada colaborador.

Em particular, a IFTHENPAY assegura que:

- o acesso ao sistema central ifprod e a outros sistemas de suporte é limitado a utilizadores previamente autorizados;
- os perfis de acesso são definidos com base em critérios funcionais, garantindo que cada utilizador apenas dispõe das permissões estritamente necessárias ao desempenho das suas funções;
- os acessos atribuídos são objeto de revisão periódica, bem como sempre que ocorram alterações relevantes nas funções, responsabilidades ou vínculo do colaborador;

- se encontra assegurada a segregação funcional entre atividades operacionais, de controlo e de decisão, prevenindo situações de acumulação indevida de funções suscetíveis de gerar conflitos de interesses ou comprometer a eficácia dos controlos internos.

A gestão de acessos integra-se no sistema global de controlo interno da IFTHENPAY, contribuindo para a proteção da informação, a integridade dos dados e a fiabilidade dos processos de monitorização, exame e decisão em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo.

3 Backups e continuidade de negócio

A IFTHENPAY assegura a implementação de mecanismos adequados de salvaguarda da informação e de continuidade da atividade, tendo em conta a natureza, dimensão e complexidade do serviço de pagamentos prestado e os riscos operacionais associados.

Em particular, a IFTHENPAY garante que:

- são efetuadas cópias de segurança (backups) regulares da informação crítica, incluindo dados de clientes, operações, registos de monitorização, exame e decisões relevantes em matéria de BCFT;
- os backups são armazenados em condições que asseguram a sua integridade, confidencialidade e disponibilidade, permitindo a reposição da informação em caso de incidente técnico, falha de sistema ou outro evento disruptivo;
- a arquitetura tecnológica contempla mecanismos de redundância adequados aos sistemas essenciais ao funcionamento do serviço, mitigando o risco de indisponibilidade prolongada;
- existe um plano de continuidade de negócio e de recuperação em caso de desastre, que define responsabilidades, prioridades de reposição, procedimentos de resposta e comunicação interna;
- o plano de continuidade e recuperação é objeto de revisão periódica e de testes adequados, de forma proporcional, com vista a verificar a sua eficácia e a identificar oportunidades de melhoria.

Estas medidas visam assegurar a resiliência operacional da IFTHENPAY, a continuidade do serviço de pagamentos e a preservação da informação necessária ao cumprimento dos deveres legais e regulamentares, incluindo os deveres de conservação, monitorização, exame e comunicação previstos na legislação de prevenção do BCFT.

4 Filtragem e parametrização de alertas

A IFTHENPAY dispõe de mecanismos de filtragem e geração de alertas integrados nos seus sistemas de informação, concebidos para apoiar a deteção atempada de situações potencialmente relevantes em matéria de prevenção do branqueamento de capitais e do financiamento do terrorismo, de forma proporcional ao risco e à natureza do serviço prestado.

Em particular, os sistemas utilizados permitem a monitorização ao longo da relação de negócio, através do registo de operações, geração de alertas e apoio à análise humana, não substituindo a intervenção e decisão humanas, nomeadamente:

- a definição e ajustamento de parâmetros e limiares de alerta (thresholds), tendo em conta fatores como o perfil de risco do cliente, o tipo de operação, os montantes envolvidos, a frequência transacional e outros elementos relevantes para a análise de risco;
- a categorização dos alertas gerados, distinguindo, designadamente, entre alertas associados a filtragem de listas de sanções, PEPs e outros eventos operacionais ou transacionais relevantes;
- a gestão e priorização dos alertas, permitindo a sua análise faseada e fundamentada, com vista à redução de falsos positivos, sem prejuízo da deteção de situações efetivamente suscetíveis de constituir risco acrescido de BCFT;
- a integração necessária com a intervenção humana, assegurando que todos os alertas relevantes são objeto de análise por colaboradores competentes, que avaliam o respetivo contexto, solicitam esclarecimentos adicionais quando necessário e registam as conclusões e decisões adotadas.

A parametrização dos sistemas e a gestão dos alertas assentam numa *abordagem baseada no risco*, sendo ajustadas sempre que se verifiquem alterações relevantes no perfil do cliente, no padrão das operações ou no quadro normativo e regulamentar aplicável. As decisões tomadas na sequência da análise de alertas são devidamente documentadas e conservadas em suporte duradouro, garantindo a rastreabilidade e a possibilidade de auditoria.

5 Rastreabilidade e evidência digital

A IFTHENPAY assegura a *rastreabilidade adequada* das suas atividades relevantes para efeitos de prevenção do branqueamento de capitais e do financiamento do terrorismo, através do registo e conservação estruturada de evidência digital nos sistemas de informação utilizados, em especial no sistema ifprod.

São objeto de registo, de forma proporcional e adequada à natureza da atividade, designadamente:

- os acessos aos sistemas críticos, incluindo a identificação do utilizador, data e hora de acesso, sempre que tecnicamente aplicável;
- as alterações relevantes efetuadas nos dados de clientes, no perfil de risco, nos parâmetros operacionais ou em elementos essenciais da relação de negócio;
- as decisões tomadas no âmbito dos deveres de identificação e diligência, de exame, de aceitação, recusa, suspensão ou cessação da relação de negócio;
- a análise de alertas gerados pelos sistemas, incluindo o respetivo enquadramento, os elementos considerados e as diligências efetuadas;
- as justificações que fundamentam as decisões adotadas, em particular quando resulte a não comunicação, a continuidade da relação de negócio ou a execução de operações após análise.

Os registos efetuados permitem a reconstituição cronológica e lógica dos factos relevantes, assegurando a transparência dos processos internos e a possibilidade de verificação posterior por funções de controlo interno, auditoria ou autoridades competentes.

A evidência digital é conservada em suporte duradouro, de forma segura e com controlo de acessos, nos termos legais aplicáveis, garantindo a sua integridade, confidencialidade e disponibilidade durante os prazos de conservação previstos na legislação em vigor.

X. DISPOSIÇÕES FINAIS

1 Aprovação e entrada em vigor

A presente Política é aprovada pela Gerência da IFTHENPAY e entra em vigor na data da sua assinatura, sendo de cumprimento obrigatório para todos os colaboradores, membros dos órgãos sociais, mandatários e demais pessoas que atuem, a qualquer título, no âmbito da atividade da Instituição. Em caso de conflito interpretativo, prevalece a presente Política sobre procedimentos operacionais.

2 Revisão periódica e extraordinária

A Política é objeto de revisão periódica, pelo menos uma vez por ano, e pode ser revista extraordinariamente sempre que se verifique, designadamente:

- alteração relevante do enquadramento legal ou regulamentar aplicável;
- emissão de orientações, recomendações ou determinações pelas autoridades de supervisão ou setoriais;
- alterações significativas na estrutura organizativa, modelo de negócio, sistemas, produtos ou perfil de risco da IFTHENPAY;
- identificação de deficiências, incidentes ou falhas relevantes no sistema de controlo interno.

As revisões são propostas pelo Responsável pelo Cumprimento Normativo, sujeitas a apreciação da Gerência e devidamente documentadas.

3 Hierarquia normativa interna

A presente Política prevalece sobre quaisquer normas, procedimentos, instruções ou práticas internas que com ela sejam incompatíveis, sem prejuízo do cumprimento da legislação e regulamentação aplicáveis.

Em caso de divergência interpretativa, prevalecerá a interpretação mais conforme com o quadro legal e regulamentar em vigor e com as orientações das autoridades competentes.

4 Articulação com outros documentos internos

A presente Política integra o sistema interno de prevenção do BCFT da IFTHENPAY e articula-se, designadamente, com:

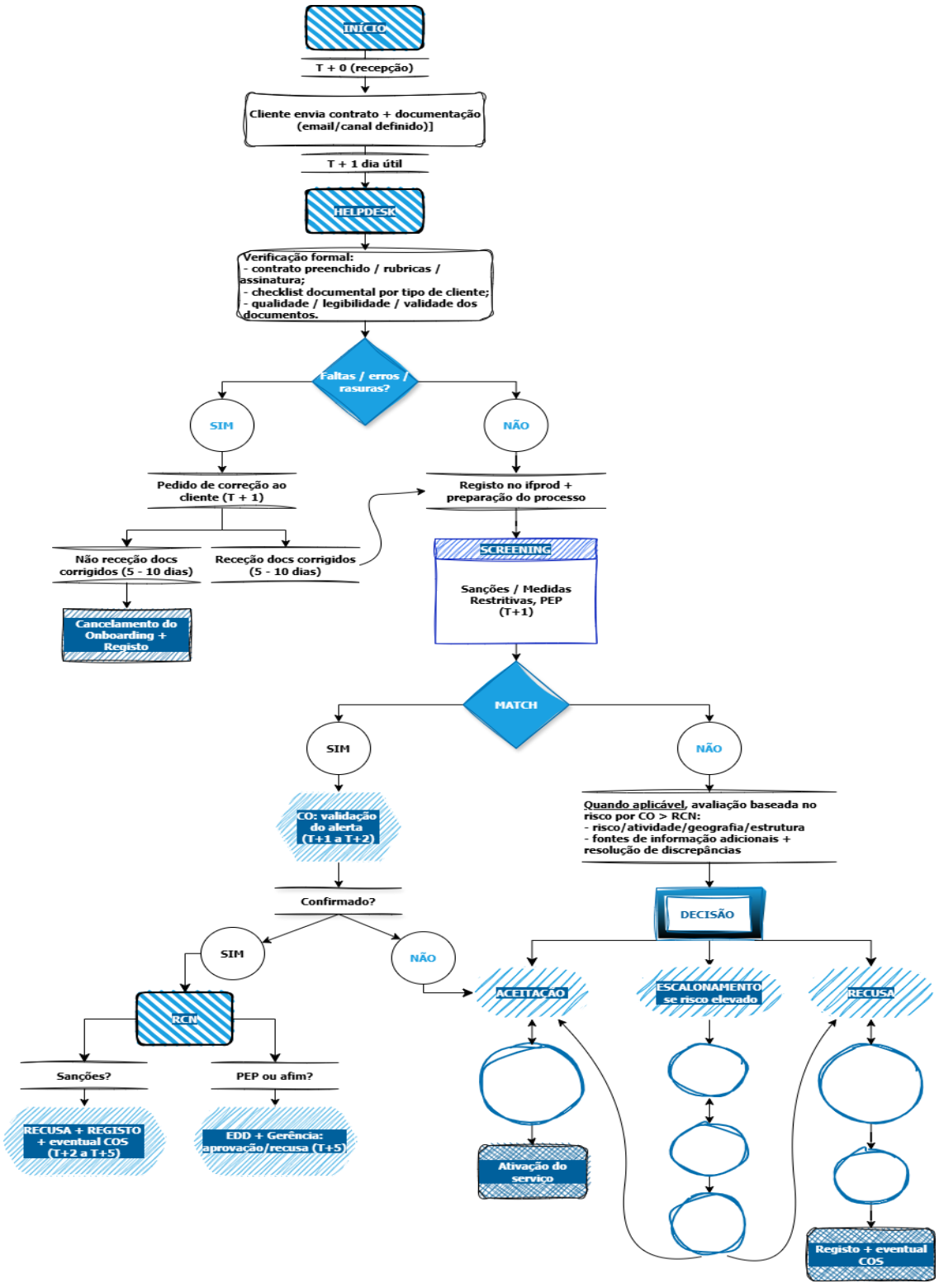
- o Código de Conduta;
- as políticas de Aceitação de Clientes e de Identificação e Diligência;
- a Política de Análise e Monitorização de Entidades de Risco Elevado;
- o Manual de Controlo Interno e Procedimentos Operacionais;
- a Política de Incidentes Operacionais;
- os procedimentos internos de comunicação de operações suspeitas e comunicações sistemáticas (COS/CAS).

5 Anexos

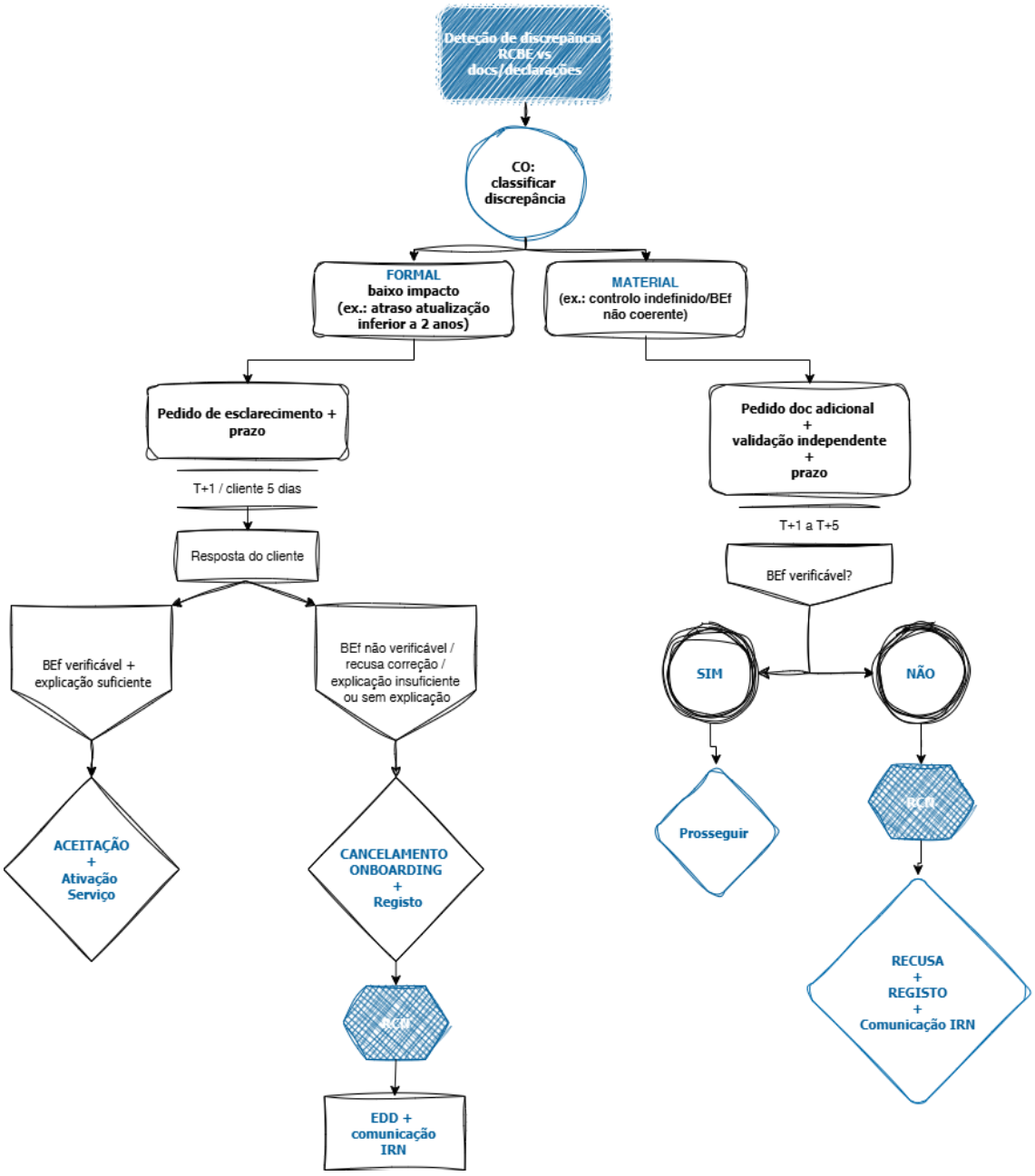
ANEXO A — FLUXOGRAMA DE ATIVIDADES BCFT

! Nota: prazos "T+" são indicativos (SLA interno), ajustáveis por volume/riscos.

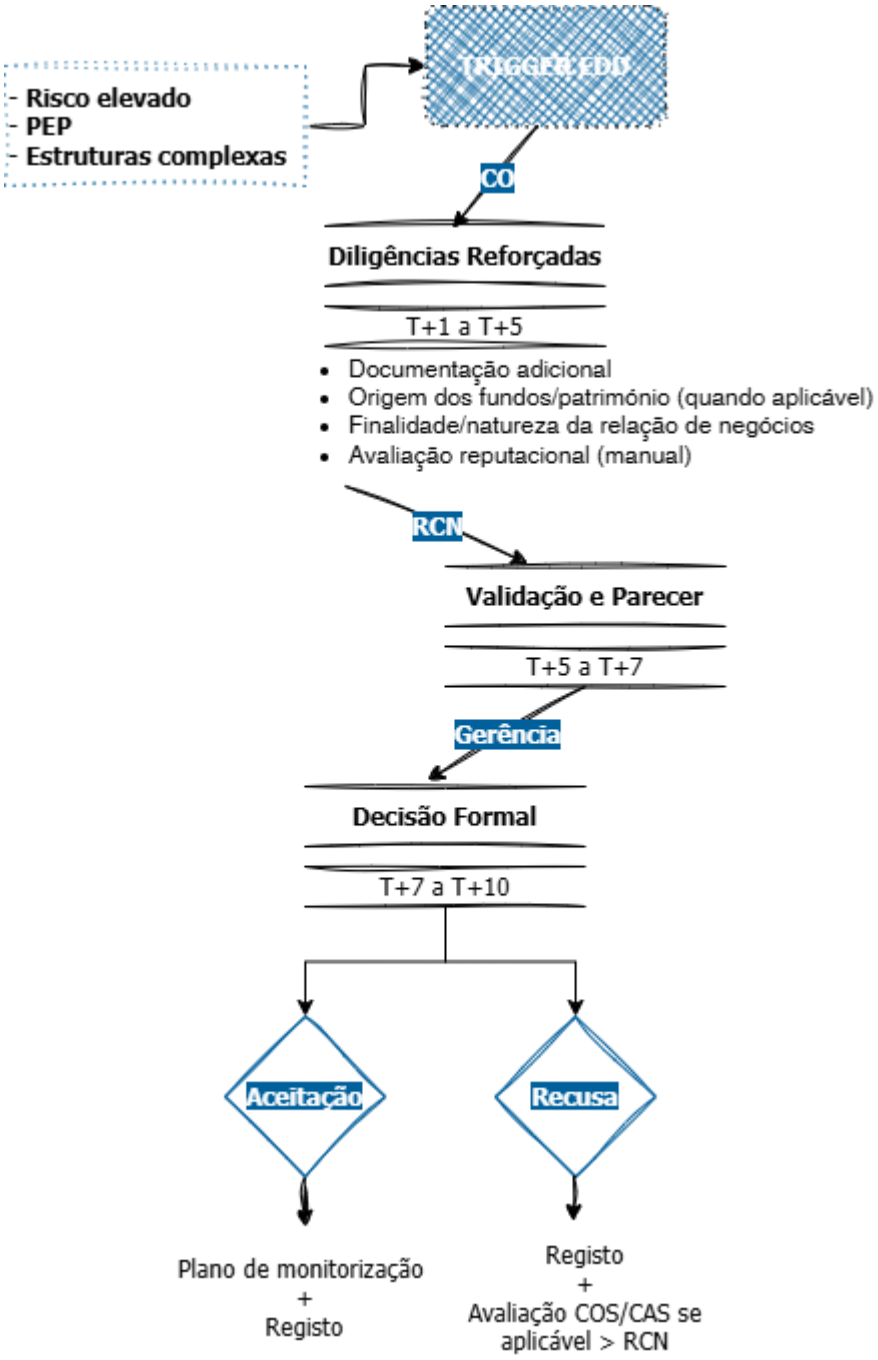
1. Fluxo de Onboarding e Aceitação (CDD)



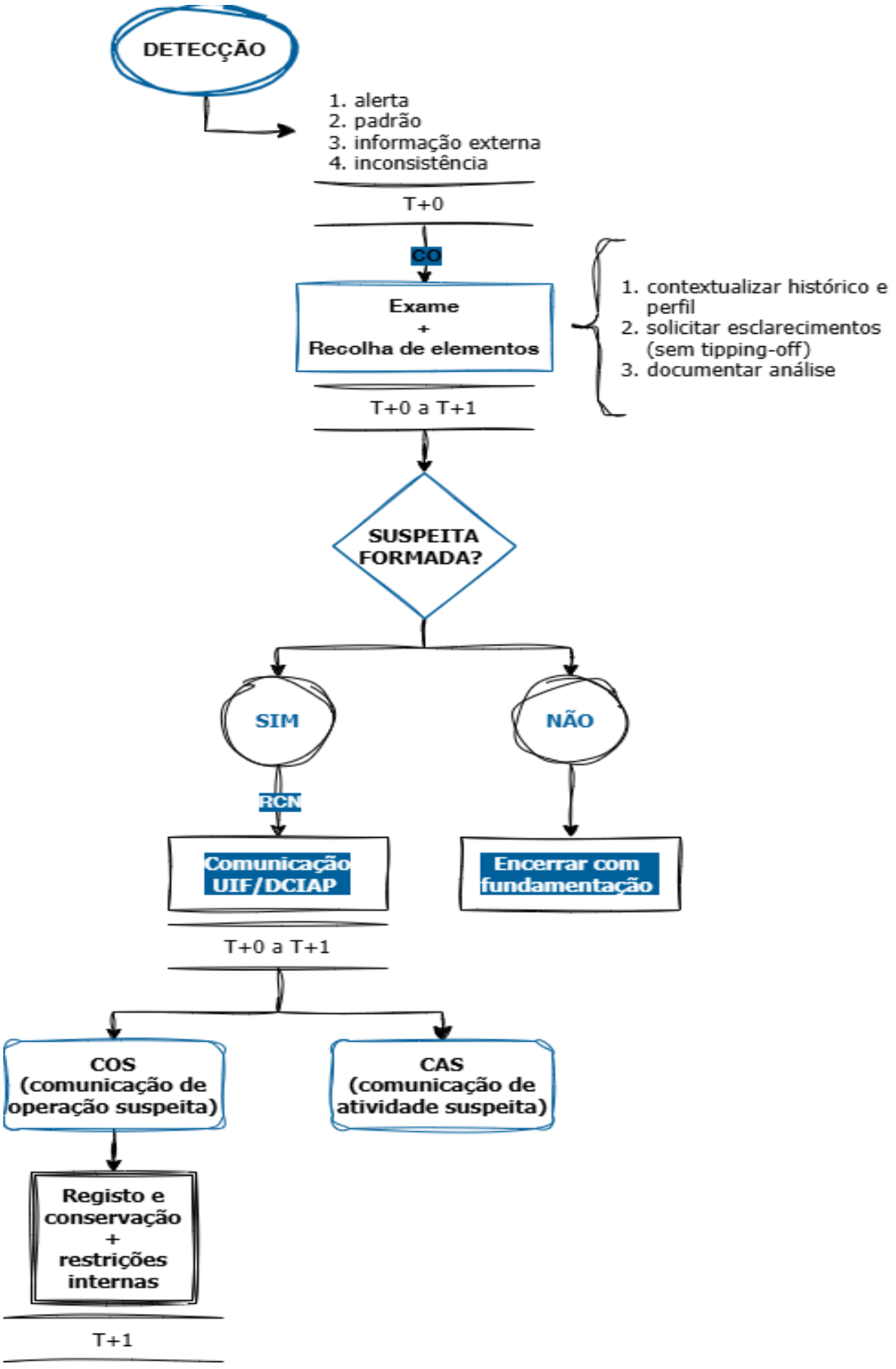
2. RCBE — tratamento de discrepâncias



3. EDD / pré-aprovação (risco elevado / PEP / estruturas complexas)



4. Dever de Exame → COS/CAS (suspeição)



ANEXO B — CHECKLISTS

B1) Checklist base (comum)

- Contrato: preenchido, rubricado (todas as páginas exceto assinatura), assinado
- IBAN: comprovativo com nome do titular (aderente)
- Triagem: qualidade/legibilidade/validade; ausência de rasuras relevantes
- Screening: sanções + PEP + listas restritivas (ifprod)
- RCBE: consulta quando aplicável + gestão de discrepâncias
- Registo: evidência da decisão (aceitação/recusa/escalonamento)

B2) Empresas (sociedades)

- Certidão permanente (código)
- Código RCBE
- Certidão fiscal IVA (quando aplicável)
- Identificação + morada dos:
  - representantes legais
  - beneficiários efetivos
  - titulares de participações no capital e/ou nos direitos de voto ≥5%

B3) ENI

- Certidão fiscal IVA (quando aplicável)
- ID + morada do ENI (e de eventuais representantes/BEf, se aplicável)

B4) Associações/Fundações/Condomínios/equiparadas

- Estatutos atualizados
- Ata de tomada de posse/representação
- RCBE (quando aplicável)
- IDs + moradas de representantes e BEf

B5) Pessoas coletivas de direito público

- Documento de nomeação/designação de representantes
- Diploma orgânico/estatutos (quando aplicável)
- IDs + moradas (representantes)

ANEXO C — KPIs / KRIs

Owners: CO (operacional), **RCN** (validação), **Gerência** (oversight), **GR** (tendências).

C.1. DEFINIÇÕES

KPI (Key Performance Indicator)

Significado: Indicador Chave de Desempenho.

Conceito: É uma métrica quantitativa que avalia a eficácia e a eficiência com que a instituição está a cumprir os seus objetivos operacionais e preventivos.

Fundamento: O Aviso n.º 3/2020 e a Política BCFT estabelecem que a instituição deve monitorizar o grau de execução das suas atividades, como o cumprimento do plano de formação e a prontidão na resposta a pedidos das autoridades.

KRI (Key Risk Indicator)

Significado: Indicador Chave de Risco.

Conceito: É uma métrica que fornece um sinal de alerta precoce sobre uma mudança no perfil de risco ou sobre a iminência de um evento de risco material.

Fundamento: O enquadramento regulamentar exige explicitamente a implementação de indicadores de alerta e indicadores de alerta precoce para identificar situações de exceção que possam afetar a solidez da instituição. Estes indicadores servem para medir a exposição a fatores de risco (clientes, produtos, geografias ou canais) e garantir que a atividade permanece dentro dos limites de apetite de risco definidos pela Gerência.

C.2. Objetivo e princípios de utilização

Os KPIs/KRIs abaixo visam:

- **medir eficiência operacional e conformidade** (KPIs);
- **detetar aumento de exposição a risco BCFT** e tendências (KRIs);
- **suportar decisões e escalonamento** (CO → RCN → Gerência), com registo da fundamentação.

A leitura destes indicadores é **proporcional ao risco** e **assente em evidência documental**, sem pressupor automatismos não existentes; os sistemas internos suportam a recolha/organização, e a decisão é **sempre humana e documentada**.

Tipo	Indicador	Definição / Fórmula	Fonte / Evidência	Frequência	Meta / Limiar (exemplos)	Ação / Escalonamento
KPI	SLA onboarding concluído	% processos de onboarding concluídos **≤ 5 dias úteis** = (nº processos ≤5d / nº processos concluídos) × 100	Registos do processo (ticket/email) + registo no **ifprod**	Semanal / Mensal	**Meta ≥ 90% (alerta < 80%)**	Se < meta: CO analisa gargalos; RCN valida medidas; Gerência define reforço de recursos se <80% por 2 meses.
KPI	Taxa de incompletude documental	% processos devolvidos por falta/erro documental = (nº devoluções / nº processos recebidos) × 100	Checklists + histórico de pedidos ao cliente (email) + notas no ifprod	Mensal	**Meta ≤ 10% (alerta > 20%)**	Se > meta: CO ajusta checklist/comunicações, templates e formação; RCN analisa causa-raiz e valida alterações; GR acompanha impacto em risco operacional
KPI	Tempo médio de EDD	Dias úteis desde "trigger EDD" até decisão final	Registo do trigger + decisão no ifprod / dossiê	Mensal	**Meta ≤ 10 dias (alerta > 15)**	Se > limiar: CO prioriza; RCN revê causas (fonte de fundos/BEf/PEP); Gerência decide reforço/capacidade
KPI	Backlog de alertas	Nº de alertas **> 48h** sem decisão registada	Registo de alertas / lista de trabalho no ifprod	Diário / Semanal	**Meta = 0 (alerta > 3)**	Se acima do limiar: CO trata fila/redistribui; RCN avalia impacto; Gerência informada, intervém se backlog persistente
KPI	Tempo de submissão COS/CAS	Horas desde "suspeita formada" até comunicação	Registo interno do momento de suspeita + comprovativo comunicação	Por ocorrência + Mensal	**Meta ≤ 24h (alerta > 48h),** salvo exceção justificada	Se exceder: CO regista justificação + lições aprendidas; RCN valida e reporta à Gerência (oversight)
KPI	Cobertura de formação anual	% colaboradores relevantes com formação anual concluída	Lista presenças + conteúdos + avaliação (se aplicável)	Trimestral + Anual	**Meta = 100% (alerta < 95%)**	Se < 100%: CO coordena plano corretivo; RCN valida e reporta; Gerência verifica (oversight)
KPI	Qualidade do registo	% processos auditados **sem falhas documentais materiais**	Amostras auditadas (RCN/AI)	Trimestral	**Meta ≥ 95% (alerta < 90%)**	Se < meta: CO enceta ações corretivas; RCN revê procedimentos; acompanhamento de AI
KPI	RCBE consultado e evidenciado	% clientes coletivos com RCBE consultado e evidenciado = (nº com evidência / nº coletivos) × 100	Print/ficheiro/nota de consulta RCBE + dossiê KYC	Mensal	**Meta = 100% (alerta < 98%)**	Se < 100%: CO correção imediata + bloqueio de ativação até evidência; RCN valida; Gerência acompanha

KPI	Atualizações KYC em dia	% clientes com revisão dentro do calendário definido por risco	Plano de revisões + registo de revisão (ifprod/dossiê)	Mensal	Meta ≥ 95% (alerta < 90%)	Se < meta: CO estabelece plano de recuperação (backlog) + priorização por risco; RCN ajusta cadência por risco; GR sinaliza tendências
KPI	Incidentes de tipping-off	N.º de ocorrências confirmadas	Registo de incidentes + investigação interna	Mensal / Por ocorrência	0	Qualquer >0: escalonamento imediato CO → RCN → Gerência + medidas disciplinares/corretivas e formação
KRI	% carteira risco elevado	(nº clientes risco elevado / nº total clientes) × 100	Classificação de risco (ifprod) + listagens	Mensal	Alerta se > 5% (definir X no RAS)	Se excede: GR analisa e reporta tendência; RCN revê critérios e propõe mitigação; Gerência decide limites/apetite ao risco/mitigação
KRI	Matches de sanções confirmados	Nº de correspondências confirmadas com listas sancionatórias/medidas restritivas	Dossiê do alerta (motor de filtragem) + decisão + evidência de verificação	Imediato + Diário	Qualquer >0 = crítico	Ação imediata: CO recusa/cessação + deveres legais aplicáveis; RCN reporte/colaboração; Gerência oversight
KRI	% PEPs na carteira e % com aprovação Gerência evidenciada	(i) % PEPs na carteira; (ii) % desses com aprovação de Direção de Topo evidenciada	Resultado de screening + dossiê PEP + evidência aprovação	Mensal	Alerta se (i) >5% ou (ii) < 100%	Se falha evidência: CO regulariza evidência; RCN valida; Gerência garante approvals e periodicidade
KRI	% clientes com discrepâncias RCBE materiais	% com discrepância material não resolvida dentro do prazo interno (n.º com discrepâncias materiais / n.º coletivos) × 100	Registo de discrepância + diligências e conclusão	Mensal	Alerta > 2% (crítico > 5%)	Se acima: CO trata/solicita correção, reforça validações; RCN decide eventual recusa/cessação e avalia reporte IRN quando aplicável; GR acompanha
KRI	% operações fora do padrão	% operações sinalizadas por regras/limiares (após filtros) (n.º operações sinalizadas fora do padrão / n.º operações) × 100	Motor de alertas/screening + tabelas/estatísticas no ifprod + registos de análise	Mensal	Alerta por variação mensal > 20%	Se acima: CO analisa tipologias; RCN recalibra parâmetros + revisão de clientes/segmentos; GR reporta tendência à Gerência

KRI	**% clientes em setores sensíveis**	% clientes enquadrados em setores sensíveis (matriz interna) (n.º clientes setores sensíveis / n.º total) × 100	CAE/atividade + matriz interna/KYC + matriz sectorial	Mensal / Trimestral	**Alerta se > 5% ou crescimento rápido**	CO e GR analisam; RCN valida mitigação; CO reforça controlos; Gerência revê apetite/limites

Notas de aplicação:

1. Os limiares/targets ("X") são definidos e aprovados pela Gerência, sob proposta RCN/GR, e revistos pelo menos anualmente (ou quando houver alteração relevante de risco/negócio).
2. Sempre que um indicador exceda limiar por 2 períodos consecutivos (ou seja crítico), deve existir plano de ação documentado com responsável e prazo.

ANEXO D — RACI

Legenda: R Responsible | A Accountable | C Consulted | I Informed

Processo / Atividade	Helpdesk	CO	RCN	Gerência	GR	IT/SI	Auditoria Interna (ext.)
Onboarding documental (triagem)	**R**	**C**	**I**	**I**	**I**	**I**	**I**
Screening sanções/PEP/listas	**R** (execução)	**R** (validação)	**C**	**I**	**I**	**C**	**I**
Classificação de risco inicial	**C**	**R**	**C**	**I**	**A** (modelo)	**C**	**I**
EDD / pré-aprovação risco elevado	**I**	**R**	**R**	**A**	**C**	**I**	**I**
Aceitação/Recusa (decisão final)	**I**	**R**	**R**	**A**	**C**	**I**	**I**
Atualização periódica KYC	**R**	**R**	**C**	**I**	**C**	**I**	**I**
Exame (operação/padrão)	**I**	**R**	**C**	**I**	**I**	**I**	**I**
Comunicação COS/CAS	**I**	**R**	**A** (oversight)	**I**	**I**	**I**	**I**
Comunicação sistemática (quando aplicável)	**I**	**R**	**A**	**I**	**I**	**I**	**I**
Medidas restritivas/sanções (procedimento interno)	**I**	**R**	**A**	**I**	**C**	**C**	**I**
Formação anual BCFT	**I**	**R**	**A**	**I**	**C**	**I**	**I**
Revisão anual da Política	**I**	**R**	**A**	**A**	**C**	**C**	**C**
Testes de eficácia / auditoria	**I**	**C**	**C**	**A**	**C**	**C**	**R**

A. QUICK GUIDE PARA AS EQUIPAS OPERACIONAIS

1) Objetivo

Garantir onboarding e monitorização **consistentes**, com evidência documental suficiente e escalonamento correto, evitando "tipping-off".

2) Regras de ouro (operacional)

- **Sem conta/ativação *antes*** de **KYC completo** e **decisão interna registada**.
- **Se tens dúvida fundada** → não "tentas resolver sozinho": **escalona** (Helpdesk→CO→RCN).
- **Tudo o que não fica escrito, não existiu** (registar no ifprod: pedido, receção, análise, decisão).
- **Proibição absoluta de tipping-off**: nunca referir "comunicação à UIF/DCIAP", "reporte às autoridades", "suspeita", "sanções", "listas", etc.

3) Onboarding em 8 passos (SLA)

1. Receber contrato + docs (T+0)
2. Triagem formal (T+1): validade, legibilidade, rubricas/assinatura, IBAN
3. Se faltas/erros: pedir correções por email (T+1)
4. Inserir dados no ifprod + anexar docs (T+1)
5. Screening sanções/PEP/listas (T+1)
6. Se alerta: enviar ao CO (T+1)
7. Se risco elevado/PEP/estrutura complexa: RCN (EDD) + Gerência (T+5 a T+10)
8. Decisão final + registo + ativação/recusa (T+5)

4) Red flags (exemplos práticos)

- Documentos rasurados, divergências de nomes, datas, assinaturas
- Estrutura societária opaca / cadeia longa / entidades em jurisdições sensíveis
- Cliente resiste a fornecer RCBE/representação/participações ≥5%
- Padrões operacionais incoerentes com CAE/atividade declarada

Purple flag: Alertas de sanções/PEP/listas restritivas

5) Quando pedir mais documentos?

- Dúvida fundada sobre identidade/representação/BEf
- Discrepância RCBE material
- EDD (origem de fundos/património quando aplicável)
- Atividade sensível / risco elevado

6) Escalonamento (quem decide o quê)

- Helpdesk: qualidade documental + completude + execução de screening + registos
- CO: verifica e valida alertas, conduz monitorização/screening, sugere mitigação
- RCN: valida parecer, conduz exame/EDD, garante conformidade, decide comunicação COS/CAS
- Gerência: aprova PEP/EDD e decisões estruturantes

7) "Script" seguro para pedir esclarecimentos (sem tipping-off)

"Para completar a análise de conformidade necessária à prestação do serviço, solicitamos os seguintes elementos adicionais (...)"

8) Evidência mínima a arquivar (checklist rápida)

- Documentos recebidos + data
- Resultado screening + decisão sobre alerta
- Justificação de aceitação/recusa
- (EDD) elementos adicionais e decisão Gerência
- (Suspeita) registo do exame + referência à comunicação (sem expor a terceiros)