



MODELO GLOBAL DE GESTÃO DE RISCOS DE BRANQUEAMENTO DE CAPITAIS E FINANCIAMENTO DO TERRORISMO

Visto e Aprovado pela Gerência

Data: ____ / ____ / ____

Assinaturas:

Carimbo:

Modelo Global de Gestão de Riscos de Branqueamento de Capitais e Financiamento do Terrorismo

O presente “Modelo Global de Gestão de Riscos de Branqueamento de Capitais e Financiamento do Terrorismo” institui os princípios seguidos pela SUNPAY no âmbito da Avaliação dos Riscos inerentes à atividade desenvolvida pela empresa, saber:

- Princípios de Aceitação de Clientes;
- Princípios de Identificação de Clientes;
- Princípios de Análise e Monitorização de Entidades de Risco Elevado;
- Princípios de Gestão de Risco de Branqueamento de Capitais e de Financiamento de Terrorismo;
- Princípios de Execução de Ordens;
- Princípios de Conflitos de Interesses.

NOTA: entenda-se no presente contexto que a designação “cliente” compreende todas as entidades utilizadoras dos nossos serviços de pagamento, i.e., e conforme definição:

«Utilizador de serviços de pagamento» a pessoa que utiliza um serviço de pagamento a título de ordenante, de beneficiário ou em ambas as qualidades

Índice

1. INTRODUÇÃO.....	4
2. PRINCÍPIO DE ACEITAÇÃO DE CLIENTES	4
2.1. ENQUADRAMENTO.....	4
2.2. OBJECTIVO DO PRINCÍPIO DE ACEITAÇÃO DE CLIENTES	5
2.3. CATEGORIAS DE POTENCIAIS CLIENTES CUJA ACEITAÇÃO DEVE SER RÉCUSADA	6
2.4. CATEGORIAS DE POTENCIAIS CLIENTES CUJA ACEITAÇÃO DEVE SER CONDICIONADA A PROCESSO ESPECIAL DE AUTORIZAÇÃO	6
2.5. PESSOAS POLITICAMENTE EXPOSTAS.....	7
2.6. CRITÉRIOS PARA A ATRIBUIÇÃO DE GRAU DE RISCO ELEVADO NO MOMENTO DA ACEITAÇÃO DE CLIENTES	8
2.7. ELEMENTOS FUNDAMENTAIS NOS PRINCÍPIOS DE IDENTIFICAÇÃO E DE CONHECIMENTO DOS NOVOS CLIENTES (KYC).....	9
3. PRINCÍPIO DE IDENTIFICAÇÃO DE CLIENTES.....	10
3.1. ENQUADRAMENTO.....	10
3.2. OBJECTIVO E ÂMBITO DE APLICAÇÃO	10
3.3. VERIFICAÇÃO DA IDENTIDADE.....	11
3.3.1. Princípios básicos.....	11
3.3.2. Elementos a obter	12
3.3.3. Qualidade dos documentos exigíveis	13
4. PRINCÍPIO DE ANÁLISE E MONITORIZAÇÃO DE ENTIDADES DE RISCO ELEVADO.....	13
4.1. ENQUADRAMENTO.....	13
4.2. OBJECTIVO/ÂMBITO DO PRINCÍPIO DE ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO	13
4.3. METODOLOGIAS E PROCEDIMENTOS UTILIZADOS NA ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO	14
4.4. CRITÉRIOS DE ATUAÇÃO NA ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO	14
4.4.1. Abertura/cadastro de cliente de risco elevado	14
4.4.2. Pessoas politicamente expostas (PEP)	15
4.4.3. Beneficiários efetivos	16
4.4.4. Gestão de risco e execução das operações	16
4.4.5. Ações de controlo ativo reforçado	16
5. PRINCÍPIO DE GESTÃO DE RISCO DE BRANQUEAMENTO DE CAPITAIS E DE FINANCIAMENTO DE TERRORISMO	17

5.1. ENQUADRAMENTO.....	17
5.2. OBJECTIVO E ÂMBITO DO PRINCÍPIO	18
5.3. MÉTODOS E PROCEDIMENTOS DE PREVENÇÃO DO BRANQUEAMENTO DE CAPITALS E DO.....	18
FINANCIAMENTO DO TERRORISMO	18
5.3.1. Normativos internos	18
5.3.2. Due Diligence/Know Your Customer (KYC).....	18
5.3.3. Risk Based Approach	19
5.3.4. Metodologia utilizada no processo de monitorização e controlo.....	20
5.3.5. Monitorização e controlo	21
5.3.6. Comunicação de transações suspeitas	22
5.3.7. Formação	22
5.3.8. Bancos correspondentes	23
6. PRINCÍPIO DE CONFLITOS DE INTERESSES.....	23
6.1. ENQUADRAMENTO.....	23
6.2. PRINCÍPIO DE CONFLITOS DE INTERESSES.....	23

Modelo Global de Gestão de Riscos de Branqueamento de Capitais e Financiamento do Terrorismo

1. INTRODUÇÃO

O presente documento reúne um conjunto de Princípios denominados “Princípios de Compliance” que definem os aspetos básicos de atitude e de atuação dos colaboradores, através dos quais se pretende que as atividades da SUNPAY sejam orientadas.

A razão da sistematização adotada para estes Princípios é baseada:

- a) por um lado, atenta a necessidade de proporcionar aos colaboradores documentos concisos e mais acessíveis, favorecendo a respetiva utilização;
- b) e por outro lado, reconhece-se que a definição sectorial de Princípios de Compliance enfoca mais adequadamente cada uma das realidades especificamente em causa;

Este documento não esgota o universo de instrumentos de Compliance, integrando um sistema de fontes onde se destacam as fontes de origem externa e interna e que serviu de base para a elaboração das normas internas relativas à matéria.

2. PRINCÍPIO DE ACEITAÇÃO DE CLIENTES

2.1. ENQUADRAMENTO

De acordo com os princípios gerais de prevenção e combate ao Branqueamento de Capitais e Financiamento do Terrorismo e em cumprimento da legislação nacional, das boas práticas internacionais e das recomendações do GAFI, e tendo em conta as melhores práticas em termos de atuação nos mercados, a SUNPAY implementa princípios, práticas e procedimentos, cumprindo elevados padrões de ética e profissionalismo de forma a evitar que a instituição possa ser utilizada ou sujeita, intencionalmente ou não, a práticas criminosas e de outra natureza que possam sujeitar a SUNPAY a níveis de risco operacional ou reputacional significativos.

Os elementos fundamentais dessas práticas incluem as regras de controlo e gestão dos riscos mais relevantes e, especificamente no que respeita ao relacionamento com os clientes, respetivos representantes ou operações, incluem programas de conhecimento dos seus Clientes (KYC - Know Your Customer) e são incluídas em quatro Princípios fundamentais neste domínio:

- (1) Princípio de Aceitação de Clientes;

- (2) Princípio de Identificação dos Clientes;
- (3) Princípio de Análise e Monitorização de Clientes de Risco Muito Elevado e Elevado;
- (4) Princípio de Gestão de Risco de Branqueamento de Capitais (Money Laundering) e de Financiamento do Terrorismo (Counter Terrorism Financing).

Neste sentido, a SUNPAY:

- i. Tem definido o tipo de Clientes que está disposta a aceitar;
- ii. Assume como obrigação especial de diligência, procurar obter informações sobre a verdadeira identidade da pessoa por conta e em nome de quem o cliente atua, sempre que exista suspeita fundada de que os montantes tenham uma proveniência decorrente de atividades criminosas, nomeadamente, dos crimes de furto, roubo, burla, fabrico, importação e exportação, comércio de armas e explosivos, terrorismo, extorsão, corrupção, peculato, contrabando, tráfico e consumo de estupefacientes, substâncias psicotrópicas, precursores e preparados ou outras substâncias de efeitos similares
- iii. Obtém com objetividade e rigor a sua identificação e mantém atualizados os elementos de identificação e de informação que recolhe no decurso da relação de negócio, uma vez esta iniciada;
- iv. Monitoriza as transações processadas pelos clientes de forma a verificar a conformidade daquelas com o perfil expectável do tipo de cliente em causa;
- v. Estabelece medidas de gestão de risco e de controlo de procedimentos que envolvem, entre outros aspetos, auditorias e revisões regulares e extensivas.

2.2. OBJECTIVO DO PRINCÍPIO DE ACEITAÇÃO DE CLIENTES

No âmbito dos procedimentos de combate ao branqueamento de capitais e ao financiamento do terrorismo e no cumprimento dos normativos regulamentares e das recomendações das entidades internacionais relevantes, a SUNPAY desenvolve princípios e procedimentos claros de aceitação de Clientes, incluindo a descrição dos tipos de clientes que provavelmente possam envolver um risco mais elevado para a própria empresa.

No âmbito destes Princípios e Procedimentos são tomados em consideração fatores relevantes para a definição do nível de risco dos clientes, designadamente, o país de origem, o perfil profissional e a sua eventual participação em atividades políticas, o ramo de negócio do Cliente e as transações que com ele podem estar associadas;

Neste sentido, este documento tem como objetivo definir o conjunto de critérios que devem orientar a empresa na aceitação ou recusa de relacionamento com potenciais clientes, na

definição de critérios de aceitação condicionada de clientes e na definição de critérios de classificação do nível de risco dos clientes.

2.3. CATEGORIAS DE POTENCIAIS CLIENTES CUJA ACEITAÇÃO DEVE SER RECUSADA

Tendo como objetivo proteger a SUNPAY de práticas que possam colocar em risco as suas atividades e de forma a proteger a sua reputação, a SUNPAY recusa o estabelecimento e/ou manutenção com quaisquer potenciais/já existentes clientes que se enquadrem em alguma das seguintes categorias:

- i) Pessoas cuja reputação, na comunicação social ou no mercado, surge habitualmente associada a atividades criminosas;
- ii) Pessoas cuja atividade ou modo de vida levante suspeitas relativamente à origem do respetivo património;
- iii) Pessoas que não colaborem com a SUNPAY na disponibilização da informação requerida;
- iv) Casinos, estabelecimentos de jogo de fortuna e azar ou outros de natureza afim, desde que não autorizados de acordo com a legislação sobre a matéria;
- v) Bancos de Fachada (instituição financeira que não tem presença física e que não se encontre integrado a nenhum grupo financeiro regulamentado no país).

Relativamente às entidades cuja aceitação como cliente seja recusada, a SUNPAY prepara um processo de recusa que inclui todas as informações recolhidas sobre a entidade, bem como uma nota fundamentada dos motivos que originaram a não-aceitação. O processo é elaborado pelo Compliance Officer que equacionará, em face das informações recebidas, possíveis ações subsequentes no âmbito da legislação em vigor.

2.4. CATEGORIAS DE POTENCIAIS CLIENTES CUJA ACEITAÇÃO DEVE SER CONDICIONADA A PROCESSO ESPECIAL DE AUTORIZAÇÃO

A SUNPAY tem um processo especial de aceitação de potenciais clientes, fazendo depender de especial autorização por parte da Administração da empresa a aceitação de clientes que se enquadrem em alguma das seguintes categorias:

- i) Pessoas relativamente às quais a SUNPAY tenha classificado com nível elevado de risco de branqueamento de capitais;

ii) agências de câmbio ou quaisquer outros estabelecimentos que efetuem o comércio de divisas;

iii) Pessoas Politicamente Expostas, nos termos do número seguinte.

O processo de aceitação condicionada abrange os casos em que o potencial Cliente seja gestor, acionista ou proprietário de qualquer entidade que prossiga qualquer das atividades vindas de enunciar.

2.5. PESSOAS POLITICAMENTE EXPOSTAS

O processo de aceitação condicionada de clientes referido no número anterior abrange, de forma especial:

i) As Pessoas Politicamente Expostas (PEP) que pretendam ser clientes da SUNPAY no País ou fora do país de que são Nacionais;

ii) Os membros da família dos PEP, incluindo as pessoas que com estes convivam em situação de facto;

iii) Outras pessoas que reconhecidamente tenham com os PEP ou respetivos familiares estreitas relações de natureza comercial ou societária;

iv) Outras pessoas titulares de outros cargos públicos relevantes;

Por PEP «Pessoas politicamente expostas» entende-se pessoas singulares a quem estão ou foram cometidas funções públicas proeminentes, a saber e resumidamente:

a) Chefes de Estado, chefes de Governo, ministros, ministros-adjuntos e secretários de Estado;

b) Deputados ou membros de órgãos legislativos similares;

c) Membros dos órgãos de direção de partidos políticos;

d) Membros dos supremos tribunais, dos tribunais constitucionais e de outros órgãos judiciais de alto nível cujas decisões não sejam passíveis de recurso, salvo em circunstâncias excecionais;

e) Membros dos tribunais de contas e dos órgãos de administração dos bancos centrais;

f) Embaixadores, encarregados de negócios e oficiais de alta patente das forças armadas;

g) Membros de órgãos de administração, de direção ou de supervisão de empresas públicas;

h) Diretores, diretores-adjuntos e membros do conselho de administração ou pessoas que exercem funções equivalentes numa organização internacional.

Nenhuma função pública enumerada nas alíneas a) a h) pode ser interpretada no sentido de que inclui funcionários em posições ou categorias intermédias ou mais baixas;

b) «Membros da família» inclui:

a) O cônjuge, ou pessoa equiparada ao cônjuge, de pessoa politicamente exposta;

b) Os filhos e respetivos cônjuges, ou pessoas equiparadas a cônjuge, de pessoa politicamente exposta;

c) Os pais de pessoa politicamente exposta;

Independentemente do processo especial de KYC aplicável a estas categorias de clientes, a aceitação de PEP como Cliente da SUNPAY depende sempre da autorização da Administração da empresa.

2.6. CRITÉRIOS PARA A ATRIBUIÇÃO DE GRAU DE RISCO ELEVADO NO MOMENTO DA ACEITAÇÃO DE CLIENTES

São nomeadamente fatores suscetíveis de agravar o grau de risco especificamente aplicável a determinado potencial Cliente:

i) A geografia de residência ou de atividade do potencial Cliente, ou a origem/destino dos fundos pretendidos movimentar no âmbito de relação de negócios ou de uma transação ocasional;

ii) A sujeição do Cliente a processo condicionado de aceitação, nos termos do nº 2.4 supra;

iii) A circunstância de determinada entidade, pela respetiva atividade ou profissão, estar sujeita à aplicação da legislação preventiva de branqueamento de capitais;

iv) A presença de quaisquer outros fatores ou circunstâncias que, para o efeito, hajam sido definidos pelo Compliance Officer.

Para efeitos do parágrafo antecedente:

A. São nomeadamente geografias de risco

i) todas aquelas objeto de embargos ou outro tipo de sanções decretados por quaisquer entidades de Direito Internacional com competência na matéria ou ainda

ii) todas aquelas insuscetíveis de poder ser qualificadas, em matéria de branqueamento de capitais ou de financiamento do terrorismo, como tendo regime equivalente ao nacional (“país terceiro equivalente”);

B. Sem prejuízo de outras, estão sujeitas à aplicação da legislação preventiva de branqueamento de capitais as seguintes entidades, atividades ou profissões:

- entidades financeiras;
- concessionários de exploração de casinos;
- entidades pagadoras de prémios de lotaria;
- entidades que exerçam atividades de mediação imobiliária;
- comerciantes que transacionem em numerário;
- revisores e técnicos oficiais de contas, auditores, consultores fiscais;
- notários, conservadores de registos, advogados, solicitadores, em prática individual ou em sociedade que intervenham em operações tipificadas na legislação preventiva de branqueamento de capitais;
- outros prestadores de serviços.

A atribuição do grau de risco é efetuada, considerando os vários fatores relevantes, pela área do Compliance Officer com a responsabilidade do combate ao branqueamento de capitais.

2.7. ELEMENTOS FUNDAMENTAIS NOS PRINCÍPIOS DE IDENTIFICAÇÃO E DE CONHECIMENTO DOS NOVOS CLIENTES (KYC)

A SUNPAY exige a verificação da identidade do Cliente e, sendo o caso, dos respetivos representantes e/ou beneficiários efetivos, para efeitos da aceitação de qualquer Cliente e a realização de qualquer transação ocasional.

A SUNPAY nunca permite a realização de quaisquer transações sem que se ache cabalmente verificada a identidade do Cliente.

No âmbito do processo de identificação e de conhecimento do Cliente, a SUNPAY avaliará necessariamente, sem prejuízo de outros aspetos relevantes:

- i) A finalidade e o propósito da(s) transação(ões) pretendidas efetuar;
- ii) O perfil transacional expectável;
- iii) As fontes de rendimento;
- iv) A coerência e consistência de toda a informação existente sobre o Cliente.

3. PRINCÍPIO DE IDENTIFICAÇÃO DE CLIENTES

3.1. ENQUADRAMENTO

No cumprimento da legislação, em matéria de prevenção e combate ao branqueamento de capitais e ao financiamento do terrorismo, a SUNPAY implementa um conjunto de Princípios e procedimentos que previnem a utilização das suas operações para práticas de natureza criminosa e que possam ser indutoras de riscos operacionais e reputacionais acrescidos.

Neste sentido, o ato de identificação dos Clientes é um elemento da maior relevância na construção do processo de KYC - Know Your Customer que a SUNPAY implementa no seu seio, de forma a proteger-se contra os riscos reputacional, operacional e legal e, ao mesmo tempo, como instrumento necessário para o cumprimento dos requisitos legais relativos ao branqueamento de capitais e financiamento do terrorismo.

3.2. OBJECTIVO E ÂMBITO DE APLICAÇÃO

Do conjunto dos Princípios implementados de forma a promover elevados padrões éticos e profissionais na sua atuação, inclui-se o Princípio de Identificação de Clientes, em que ficam estabelecidos os elementos fundamentais a respeitar nos procedimentos de identificação dos seus clientes, seus representantes e beneficiários efetivos, que em conjugação com a aplicação dos princípios de KYC - Know Your Customer criam condições para uma correta aplicação da Princípio de Aceitação de Clientes e sua subsequente monitorização.

Este princípio determina que:

- i) Os princípios básicos a que deve obedecer a identificação de todas as entidades com quem a SUNPAY se relaciona em termos de negócio cumprem obrigatoriamente com os requisitos do estabelecido legalmente;
- ii) O conjunto de documentos a obter, pessoas físicas ou entidades colectivas, que realizem transações com o SUNPAY, nos termos legalmente definidos;
- iii) Os requisitos de qualidade exigíveis a todos os documentos presentes à SUNPAY comprovativos dos diversos elementos dos clientes que procuram atestar;
- iv) A regularidade da atualização dos documentos inerentes ao Princípio de Identificação de Cliente em poder da SUNPAY, relativamente aos clientes com quem tem relações continuadas de negócio e os períodos mínimos de manutenção e arquivo daqueles documentos.

Todos os colaboradores da SUNPAY estão sujeitos ao cumprimento deste princípio, segundo os mais elevados padrões de ética e respeito pela confidencialidade da informação manuseada no desempenho das suas funções.

3.3. VERIFICAÇÃO DA IDENTIDADE

3.3.1. Princípios básicos

A identificação dos Clientes, no âmbito da atuação da SUNPAY, implica o conhecimento de um conjunto de características, a seguir detalhadas, que estão muito para além dos elementos de identificação pessoal, em sentido estrito. Deste modo, o Princípio de Identificação de Clientes tem que ser entendido sempre na perspetiva lata potenciadora da anulação dos riscos antes referidos, e não numa abordagem minimalista e estrita, que não seja capaz de evitar as perdas resultantes desses riscos.

Os princípios da veracidade, da comprovação, da especialidade e da atualidade são elementos fundamentais do princípio de identificação de Clientes. Neste sentido, independentemente da tipologia e qualidade dos documentos requeridos aos Clientes para confirmação da sua identidade, em sentido lato, o princípio da veracidade refere a necessidade de, em cada momento, se conhecer que não existe qualquer suspeita de que os elementos e informações que estão a ser fornecidos à SUNPAY sofram de falsidade, real ou provável, nem procuram esconder realidades que, de outra forma, pudessem obstar a que a relação comercial se estabelecesse nos moldes propostos.

Consequentemente, o princípio da comprovação obriga a que as informações obtidas e recolhidas no ato de constituição da relação de clientela e os elementos fornecidos pelos Clientes tenham como suporte os documentos necessários e suficientes para criar a prova efetiva da veracidade do processo.

Tanto no momento do início da relação comercial, como no decorrer da mesma, se se mantiver de forma duradoura, o princípio da atualidade impõe que os documentos constantes do processo de identificação tenham sido redigidos ou obtidos em tempo oportuno, o mais próximo possível do ato e das informações que procuram comprovar, não sendo admissível que se considerem de algum modo caducos para os objetivos que pretendem suprir. Neste sentido, deve ser identicamente entendido que o ato de identificação e comprovação dos elementos de identificação não se esgota no momento do estabelecimento da relação inicial, mas antes corresponde a um processo permanente de atualização das novas realidades e características de identificação dos Clientes e de comprovação desses mesmos elementos sempre que a caducidade dos documentos se aproxima ou a relação de negócio evolui para novas categorias de operações.

3.3.2. Elementos a obter

Os elementos informativos a obter e os respetivos documentos comprovativos, têm diferente natureza em função das diversas qualidades e naturezas dos Clientes com quem a SUNPAY estabelece relações de negócio.

Neste sentido, a própria legislação nacional estabelece um conjunto de deveres de identificação que devem ser integrados na operação diária de todos os funcionários, rigorosamente seguidos no momento em que se torna necessária a identificação dos Clientes e escrupulosamente espelhados/refletidos no sistema informático de suporte à operativa da SUNPAY (Trader) .

A SUNPAY nos seus normativos internos e em consonância com a legislação em vigor, estabelece os elementos fundamentais a obter no início do relacionamento de negócio com cada um dos tipos de Clientes com quem se relaciona e a manter na continuação dessa relação.

Os elementos fundamentais do ato de identificação dos clientes são os constantes na legislação em vigor a cada momento, transcritos/sistematizados no Manual de Procedimentos da SUNPAY e refletidos no sistema informático da empresa.

Complementarmente, no âmbito da constituição do processo de KYC-Know Your Customer, a SUNPAY deve ainda obter informação clara e verdadeira sobre:

- i) a finalidade da relação de negócio que se pretende estabelecer;
- ii) a origem e o destino dos fundos que se quer movimentar, quando e sempre que legalmente exigível;
- iii) as fontes de rendimento e de património do Cliente, criando a convicção da sua licitude e
- iv) o perfil transaccional expectável, de forma a aferir o respetivo grau de risco de branqueamento de capitais ou o enquadramento do Cliente na Princípio de Aceitação de Clientes definida.

No caso de tal ser entendido relativamente aos Clientes e às transações que pela sua natureza ou características possam suscitar um maior risco de branqueamento de capitais ou financiamento do terrorismo, a SUNPAY promove um conjunto de procedimentos especiais e prepara um processo de KYC e acompanhamento reforçados. Estão nesta situação, designadamente, as relações estabelecidas com Pessoas Politicamente Expostas (PEP).

3.3.3. Qualidade dos documentos exigíveis

Os documentos e elementos de confirmação das informações de identificação definidos pelas leis, pelos regulamentos e pelos normativos internos aplicáveis serão sempre documentos originais, quer porque foram emitidos originariamente pelas entidades com capacidade para tal, quer porque resultam de cópias devidamente autenticadas com força pública.

No caso de documentos com origem fora do país (emitidos por outros países) deve ser reforçado o cuidado na análise da sua veracidade e da natureza respetiva. Os documentos apresentados devem ser originais ou, tal como quanto aos documentos nacionais, cópias devidamente autenticadas por entidades com natureza pública neste domínio.

Em caso algum, serão aceites documentos que apresentem rasuras, estragos ou danos visíveis em partes fundamentais ou, por qualquer razão, possam sugerir a suspeita de falsificação ou violação de elementos.

No caso de documentos redigidos em língua estrangeira deverá ser solicitada uma tradução oficial.

4. PRINCÍPIO DE ANÁLISE E MONITORIZAÇÃO DE ENTIDADES DE RISCO ELEVADO

4.1. ENQUADRAMENTO

O Princípio de Aceitação de Clientes da SUNPAY remete a atuação da empresa para as melhores práticas em termos de atuação nos mercados, as quais vinculam a empresa a elevados padrões de ética e deontologia profissional.

A adoção de medidas eficazes de Know Your Customer (KYC) constitui uma parte essencial de gestão de risco de branqueamento de capitais e financiamento do terrorismo por parte do SUNPAY, minimizando riscos significativos, especialmente no que concerne ao risco reputacional.

4.2. OBJECTIVO/ÂMBITO DO PRINCÍPIO DE ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO

O presente documento tem como objetivo definir o conjunto de critérios que deverão orientar a SUNPAY acerca dos procedimentos de aceitação, análise e monitorização daqueles que são os clientes considerados de alto risco exigindo um intensivo “Due Diligence” ou a aplicação de medidas reforçadas de “vigilância” e monitorização contínua, com base na avaliação de risco, devendo ainda abranger os mecanismos de controlo de execução que garantam a efetiva implementação dos procedimentos, tais como o processo

de identificação e registo dos beneficiários efetivos e das Pessoas Expostas Politicamente (PEP), a filtragem de operações e ainda a monitorização de transações dos Clientes através dos aplicativos informáticos da SUNPAY, com o objetivo último de mitigar o risco da SUNPAY ser utilizada intencionalmente ou involuntariamente para as atividades de branqueamento de capitais.

4.3. METODOLOGIAS E PROCEDIMENTOS UTILIZADOS NA ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO

Uma abordagem baseada no risco é o método utilizado pela SUNPAY com o intuito de identificar, gerir e mitigar o risco de branqueamento de capitais e financiamento do terrorismo e inclui métodos e sistemas de controlo adequados para avaliar e prevenir os mesmos. Ao mesmo tempo, complementarmente, contribui para a redução do risco de fraude, reduzindo o potencial de perdas financeiras assumido.

Assim, relativamente aos Clientes identificados com risco elevado, a SUNPAY:

- i) Define no seu Princípio de Aceitação, categorias de Clientes em que o estabelecimento de relações de negócio deva ser recusado ou condicionado a processo especial de autorização, estando nesta última incluídas as Pessoas Politicamente Expostas. Estas, em observância ao exposto na lei, e desde que averiguado o seu estatuto deverão ser submetidas a um processo KYC com informação detalhada, estando previsto a obrigatoriedade de requerer autorização da Administração;
- ii) Desenvolve uma operativa de validação de clientes, que consiste na confirmação por parte do Compliance Officer, da conformidade documental do processo de Cliente;
- iii) O sistema informático possibilita a qualquer Colaborador comunicar ao Compliance Officer situações ou operações com elevado índice de suspeição, merecedoras por natureza de acompanhamento especialmente determinado. A informação deste repositório e a sua consulta estão disponíveis apenas para Colaboradores do Compliance Officer, na proporção das suas funções.

4.4. CRITÉRIOS DE ATUAÇÃO NA ANÁLISE E MONITORIZAÇÃO DE CLIENTES DE RISCO ELEVADO

4.4.1. Abertura/cadastro de cliente de risco elevado

Dado que uma parte da avaliação e prevenção dos riscos atrás referidos se baseiam na monitorização contínua do Cliente e das suas atividades, com base em critérios de risco estabelecidos, a SUNPAY define que serão submetidas a pré-validação do Compliance Officer todas as propostas de início de estabelecimento de relações de negócio de clientes

cujo risco seja classificado como elevado, independentemente de outros critérios que possam vir a ser definidos a cada momento.

No caso dos PEP e dos Ultimate Beneficial Owners (últimos beneficiários efetivos), a não obtenção ou recusa no fornecimento dos elementos considerados necessários, deverão determinar a recusa por parte da SUNPAY da aceitação da relação comercial, devendo a ocorrência originar a constituição de um processo de análise aprofundado.

4.4.2. Pessoas politicamente expostas (PEP)

Sempre que se constate o estatuto de “PEP” de um cliente (conforme definido em 2.5), serão adotados procedimentos enunciados seguidamente.

Relativamente às operações realizadas com pessoas politicamente expostas e no seguimento do Dever de Diligência Reforçada, ao iniciar uma relação comercial, no âmbito do desenvolvimento da relação de negócio ou na execução de qualquer operação, a SUNPAY:

- a) Questionará o Cliente por forma a determinar se o mesmo se enquadra na classificação de PEP;
- b) Na presença de um PEP, assegurará um processo reforçado de diligência com o objetivo de obter informações detalhadas acerca da origem do património e dos fundos envolvidos, devendo ser claramente indicados, entre outros:
 - i) O motivo de estabelecimento de relação de negócio;
 - ii) A origem dos fundos;
 - iii) Montante exato do(s) valor(es) que vão ser transacionados via SUNPAY;
 - iv) Discriminação do rendimento.

Tratando-se de um Cliente que no decurso da relação comercial com a SUNPAY se torna num PEP, deve ser alterado em consonância com o atrás exposto, o cadastro do cliente.

Refira-se por último que, considerando o risco acrescido de branqueamento ou de financiamento do terrorismo, devido ao seu perfil ou à natureza das operações que possam ser desenvolvidas, deverão os PEP ser objeto de um acompanhamento contínuo acrescido por parte da SUNPAY ao longo da relação de negócio, que deverá continuar aplicar-se a quem, tendo deixado de ter a qualidade de PEP, continue a representar um risco acrescido para o SUNPAY.

A SUNPAY estende ainda, na generalidade e proporcionalmente, as diligências supra enunciadas para as Pessoas Expostas Politicamente aos TITULARES de elevados cargos públicos.

4.4.3. Beneficiários efetivos

Entende-se como BEF, abreviatura da designação “Beneficiário Efetivo”, a pessoa singular por conta de quem é realizada uma transação ou atividade ou que, em última instância, detém ou controla o cliente.

4.4.4. Gestão de risco e execução das operações

As operações detetadas cuja desconformidade não seja justificada ou em que existam relevantes indícios ou suspeitas de ilícito originam por parte da SUNPAY, independentemente de outras medidas, uma atuação imediata sobre o cliente.

As ações a desenvolver incluem, sem prejuízo de outras medidas adequadas, a comunicação às autoridades prevista na Lei.

Também no caso de proposta de aceitação de potenciais Clientes e em conformidade com o Princípio de Aceitação de Clientes:

- i) Será recusado o início de relação de negócio às entidades previstas no ponto 2.3. do presente documento;
- ii) Será suspensa até obtenção de especial aceitação por parte do Compliance Officer, no caso dos Clientes cuja aceitação deva ser condicionada.

4.4.5. Ações de controlo ativo reforçado

A SUNPAY define um conjunto de procedimentos que pretendem assegurar a monitorização e acompanhamento especialmente atento de entidades consideradas de risco elevado.

Além das situações anteriormente enumeradas, sempre que tome conhecimento através de fontes de informação consideradas com a credibilidade suficiente, no âmbito da prevenção e combate ao branqueamento de capitais e financiamento do terrorismo e de forma a preservar e defender a sua reputação, reservar-se-á o direito de, entre outras acções possíveis:

- i) Suspender transações em que existam dúvidas relevantes da sua legitimidade ou conformidade, não procedendo à sua execução sem que estejam reunidas as condições consideradas necessárias;

- ii) Proceder a diligências reforçadas e ao exame de operações solicitando documentação comprovativa da justificação económica apresentada, procedendo à sua recusa no caso da informação e documentação consideradas necessárias não ser facultada;
- iii) Proceder à devolução de transações à sua origem sempre que entenda não estarem reunidas as condições de conformidade legal ou regulamentar, bem como aquelas, cujo envolvimento possam entender colocar em perigo a sua reputação;
- iv) Recusar a execução de transações nas quais entenda estarem a ser violados princípios e valores genericamente aceites pelo sistema financeiros como fazendo parte integrante das boas práticas recomendadas;
- v) Recusar o estabelecimento de relações comerciais sempre que entendam ser tal estabelecimento potencialmente provocador de danos reputacionais para o SUNPAY;
- vi) Comunicar às autoridades competentes qualquer operação ou situação suspeita, sempre que os indícios que contribuíram para a formação dessa convicção não sejam anulados pelas informações ou documentação disponibilizada pelos Clientes.

A SUNPAY continuará a adotar progressivamente as medidas e Princípios que entenda serem as adequadas à preservação da sua imagem e do seu ativo reputacional, reafirmando o seu forte empenho na prevenção e combate ao branqueamento de capitais e financiamento do terrorismo.

5. PRINCÍPIO DE GESTÃO DE RISCO DE BRANQUEAMENTO DE CAPITAIS E DE FINANCIAMENTO DE TERRORISMO

5.1. ENQUADRAMENTO

A SUNPAY aceita de forma séria e responsável o desafio do combate ao branqueamento de capitais e financiamento ao terrorismo, dedicando esforços em ações e instrumentos de combate a este crime, na convicção que este tipo de atitude estará sempre associada aquilo que se considera ser a defesa da integridade da SUNPAY e da sua reputação, bem como a manutenção de elevados padrões de ética profissional.

A SUNPAY dá prioridade máxima aos Princípios direcionados para a prevenção do seu envolvimento ou utilização em possíveis ações de branqueamento de capitais e financiamento do terrorismo, que possam prejudicar a sua reputação e estabilidade.

Assim sendo, a SUNPAY adota medidas internas, procedimentos e programas de formação e controlo destinados a garantir a conformidade de todos os seus Colaboradores com o enquadramento legal existente sobre a matéria.

5.2. OBJECTIVO E ÂMBITO DO PRINCÍPIO

Prevenir o uso do sistema financeiro para efeitos do branqueamento de capitais e financiamento do terrorismo é um dos meios mais eficazes de oposição ao crime organizado e uma ferramenta importante na identificação e combate á atividade criminal.

A SUNPAY considera ser um dever de todos os seus Colaboradores, na sua atividade diária e no âmbito das suas funções, agir em conformidade com a legislação sobre branqueamento de capitais assim como com as orientações e Princípios internos da SUNPAY nesta matéria, no sentido de prevenirem a utilização dos serviços disponibilizados para efeitos de branqueamento de capitais e financiamento do terrorismo.

5.3. MÉTODOS E PROCEDIMENTOS DE PREVENÇÃO DO BRANQUEAMENTO DE CAPITAIS E DO FINANCIAMENTO DO TERRORISMO

5.3.1. Normativos internos

As medidas detalhadas de natureza preventiva estão refletidas nos diversos documentos existentes de procedimentos internos. Todos os Colaboradores deverão agir de acordo com estes documentos, bem como os princípios e procedimentos normalizados neles definidos - Código de Conduta, Manual de Procedimentos.

5.3.2. Due Diligence/Know Your Costumer (KYC)

A SUNPAY adota todos os procedimentos necessários no sentido de determinar a verdadeira identidade dos seus Clientes, representantes e/ou beneficiários efetivos (Princípio de Identificação de Clientes), assim como de obter toda a informação relevante e pertinente à abertura e manutenção de uma relação comercial.

No âmbito do processo de identificação e conhecimento do Cliente, a SUNPAY avalia necessariamente, sem prejuízo de outros aspetos que possam ser considerados relevantes:

- i) A finalidade e o propósito da relação que se pretende estabelecer;
- ii) O perfil transaccional expectável;
- iii) As fontes de rendimento dos Clientes;
- iv) A coerência e consistência de toda a informação existente.

Os princípios de Due Diligence são aplicados não só aos procedimentos de identificação de Clientes mas também à deteção, monitorização e acompanhamento de transações que não sejam conformes ao seu perfil.

Todos os registos e evidências documentais são mantidos em vários suportes, pelo prazo legalmente definido.

5.3.3. Risk Based Approach

A SUNPAY desenvolve um sistema de classificação de risco de branqueamento de capitais (risco BCFT) aplicável a todos os Clientes, o qual se baseia na ponderação das características do Cliente, conhecidas no decurso do procedimento KYC (atividade profissional, país de residência, perfil transacional expectável, estatuto de Pessoa Politicamente Exposta, entre outros).

A SUNPAY atribui a cada Cliente um dos níveis de risco ajustado e diferenciado, a saber:

- Nível de Risco 1 - Muito Reduzido (0 a 7 pontos)
- Nível de Risco 2 - Reduzido (8 a 10 pontos)
- Nível de Risco 3 - Médio (11 a 13 pontos)
- Nível de Risco 4 - Elevado (14 a 16 pontos)
- Nível de Risco 5 - Muito Elevado (17 a 18 pontos)

Foi ainda claramente definido um Princípio de Aceitação de Clientes, que estipula os princípios orientadores sobre o tipo de Clientes com que está disposta a iniciar ou manter relações comerciais, designadamente para efeitos de risco de branqueamento (BC).

Embora as orientações acerca da matéria de branqueamento de capitais e financiamento do terrorismo sejam aplicadas a todos os novos Clientes, são as mesmas de igual forma aplicadas aos Clientes existentes com base em critérios ponderados de materialidade e risco.

Sendo o processo de classificação de risco BCFT dos Clientes dinâmico, os procedimentos adequados deverão ser aplicados a todos os Clientes existentes conforme o risco que lhes seja atribuído ou que vejam o seu risco agravado de acordo com os critérios decididos em sintonia com a legislação e regulamentação em vigor, em cada momento, relativa a esta matéria. É necessário garantir que, todas as operações de clientes já existentes sejam continuamente monitorizadas e qualquer padrão incomum ou não adequado no funcionamento das mesmas desencadeie um processo de reavaliação da classificação do Cliente com base na atualização do respetivo “due dilligence”.

Os processos de defesa reputacional da SUNPAY e de combate ao branqueamento de capitais e ao financiamento do terrorismo, enquadrados numa lógica de diferenciação e graduação do risco BCFT, apenas se tornam verdadeiramente eficazes com a aplicação das

Princípios de classificação, análise e monitorização que permitam perceber, em permanência, o nível de risco da entidade. Nestas circunstâncias, todos os Clientes da SUNPAY são classificados como:

i) **Risco Normal**, se as entidades, fontes de riqueza ou origem de fundos são facilmente identificáveis ou cujas operações usualmente se apresentam adequadas e em aparente conformidade com o perfil conhecido do Cliente.

ii) **Risco Vigiar**, quando se verifica a existência de fatores suscetíveis de conduzir ao agravamento de um risco considerado não negligenciável para a empresa, tais como a profissão ou atividade do Cliente, o objeto do negócio da entidade, ou ainda para todas aquelas entidades que se enquadrem nos critérios que a empresa definira para considerar a aceitação dos Clientes como condicionada, sempre que se esteja na presença de fatores considerados como fortemente potenciadores de agravamento do risco, tais como critérios geográficos, estatuto de pessoas expostas politicamente (PEP), situações em que se verifique que as fontes de financiamento, identidades e operações não se mostrem claras, sempre que os Clientes recusem ou não colaborem na prestação das informações requeridas ou ainda, aquelas que pela sua natureza possam revelar direta ou indiretamente, um maior risco para a prática de ilícitos.

5.3.4. Metodologia utilizada no processo de monitorização e controlo

Esta abordagem baseada no risco, como método utilizado pela SUNPAY com o intuito de identificar, gerir e mitigar o risco de branqueamento de capitais e financiamento do terrorismo, inclui métodos e sistemas de controlo adequados para avaliar e prevenir a concretização daquele risco.

Para isso:

i) Com base nos normativos legais e em fatores que contribuem para a definição do nível de risco, a SUNPAY procede à classificação dos Clientes através de notação de Risco BCFT, considerando a existência de 2 níveis de risco, processo em permanente atualização e que permite a classificação de todas as entidades, fator preponderante e com impacto direto em todas as atividades de monitorização e controlo baseado no risco;

ii) Com base na utilização do sistema informático da empresa, procede-se, em tempo real, à monitorização de alertas de entidades (“black-lists”), com o objetivo de verificar a “coincidência” ou não, com as entidades constantes naquelas listas. No caso de se verificar a concordância exata com alguma das entidades constantes nas listas internacionais e mandatórias a SUNPAY não estabelece qualquer relação de negócio; nos restantes casos, em que não se verifique concordância absoluta, procede-se a diligências reforçadas de controlo;

iii) A SUNPAY mantém um investimento contínuo na formação de todos os seus funcionários, incluindo ações presenciais, genéricas ou específicas, o fornecimento de informação regular através da divulgação da informação na rede interna.

5.3.5. Monitorização e controlo

O objetivo do controlo implementado é proteger a SUNPAY dos diversos riscos e monitorizar de forma permanente a execução das operações, assegurando a sua conformidade com o enquadramento legal, os Princípios e procedimentos internos pré-definidos tendo em conta o perfil do Cliente envolvido, permitindo a deteção de transações com indícios ou suspeitas relevantes para efeitos de branqueamento de capitais e financiamento do terrorismo.

As atividades de monitorização e controlo incluem, mas não estão a elas limitadas, as seguintes práticas:

- i) Monitorização e controlo de Clientes e transações;
- ii) Monitorização e controlo de transações envolvendo países de risco;
- iii) Monitorização e controlo de transações fora do comum;
- iv) Monitorização da consistência entre as transações e a informação recolhida sobre a atividade do Cliente, perfil de risco e património financeiro numa base permanente. Esta atividade envolve não só transações pontuais mas também a análise temporal do perfil transacional do Cliente em termos de montantes médios e quantidade de transações executadas;
- v) Controlo, por meios informáticos, de transações de montante superior a 15.000€, e se as mesmas são consistentes com o perfil do Cliente;
- vi) Monitorização e controlo de transações pontuais relacionadas que, no seu todo, excedam o o montante de 15.000USD;
- vii) Monitorização e controlo de transações envolvendo entidades sujeitas a sanções e embargos diversos, constantes nas listas de entidades suspeitas (com o objetivo do controlo do cumprimento dessas restrições decretadas internacionalmente);
- viii) Controlo da conclusão e atualização da informação e documentos do Cliente que deverão ser mantidos em suporte (papel ou informático), assim como informação adicional que deverá ser incluída em transferências eletrónicas de fundos;

ix) controlo de transações apresentadas por meios não fidedignos ou de forma não presencial.

Independentemente dos critérios supra enunciados, deve ser dada especial atenção a todas as condutas e/ou atividades cujos elementos caracterizadores possam agravar o risco ou suscetibilidade de relacionamento com os crimes de branqueamento de capitais ou financiamento do terrorismo, sendo recolhidas informações e evidências documentais, da conformidade e do racional económico das transações submetidas a análise.

A maioria das atividades de monitorização e controlo são executadas pelo Compliance Officer, o qual tem acesso a qualquer tipo de informação do SUNPAY.

5.3.6. Comunicação de transações suspeitas

A monitorização e controlo apropriados de Clientes e transações é uma atividade fundamental utilizada pela SUNPAY na deteção, identificação e acompanhamento de transações ou atividades atípicas e/ou potencialmente suspeitas.

Havendo a suspeita fundada de que um Cliente ou potencial Cliente está a usar ou pretende usar os produtos ou serviços da SUNPAY para branquear fundos provenientes de atividade ilícita ou financiar o terrorismo, a SUNPAY toma todas as medidas necessárias para assegurar o integral cumprimento da legislação existente sobre a matéria.

Os Manuais da SUNPAY definem os procedimentos a serem adotados pelas várias unidades orgânicas no caso de serem detetadas transações ou atividades que se devam considerar suspeitas. Estas transações ou atividades serão sempre reportadas pelos Colaboradores ou respetivas áreas ao Compliance Officer, a quem compete a sua análise de forma aprofundada.

Neste contexto, as transações consideradas como suspeitas são comunicadas pela SUNPAY às autoridades competentes de acordo com os procedimentos legalmente instituídos.

5.3.7. Formação

O objetivo da princípio de formação da SUNPAY é não só assegurar a conformidade da SUNPAY com o enquadramento legal, mas também desenvolver uma cultura de empresa, aumentando o sentido de responsabilidade de todos os Colaboradores.

Neste contexto, a SUNPAY tem implementadas normas rígidas e claras de Formação para todos os Colaboradores, em cumprimento com o estabelecido na legislação

É dada prioridade de formação a todos os Colaboradores que asseguram contacto direto com Clientes, bem como a todos os recém-admitidos.

O objetivo final é a sensibilização de todos os Colaboradores por forma a permitir que quando em presença de uma situação suspeita e com forte probabilidade de configurar crime de branqueamento de capitais ou financiamento do terrorismo, sejam cumpridos todos os deveres que a SUNPAY incumbe, solicitando aconselhamento às respetivas hierarquias e ao Compliance Officer sobre os procedimentos a observar, agindo em conformidade com os mesmos e no rigoroso cumprimento das disposições legais a que a SUNPAY se encontra obrigado.

5.3.8. Bancos correspondentes

A SUNPAY toma as medidas consideradas necessárias de acordo com as boas práticas existentes, quando está em causa o estabelecimento ou a manutenção de relações com Bancos correspondentes, desenvolvendo procedimentos especificamente definidos, no sentido de assegurar a Due Diligence necessária relativamente a estas entidades.

Toda a informação relevante é reunida no sentido de permitir uma decisão fundamentada sobre o estabelecimento de uma relação de correspondência.

6. PRINCÍPIO DE CONFLITOS DE INTERESSES

6.1. ENQUADRAMENTO

A SUNPAY tem implementadas medidas a nível organizativo/administrativo eficazes com vista a garantir, com um grau de certeza razoável, a identificação, gestão e controlo dos possíveis conflitos de interesses.

A integridade, a equidade, a imparcialidade e a primazia dos interesses dos Clientes ocupam um lugar principal entre as normas éticas da empresa. A todos os Colaboradores é requerida uma atuação conforme com as normas éticas e recebem a informação, o treino e a orientação apropriada a fim de atuarem de modo eficaz.

6.2. PRINCÍPIO DE CONFLITOS DE INTERESSES

Como qualquer grupo de serviços financeiros, a SUNPAY está exposta a potenciais conflitos de interesses que possam surgir nas suas diferentes áreas de atuação. Os princípios de atuação da SUNPAY assentam na necessidade de adotar todas as medidas razoáveis para identificar potenciais conflitos de interesses entre a SUNPAY e os seus Clientes e entre um e outro Cliente, assim como dispor das regras que permitam assegurar que tais conflitos não afetem adversamente os interesses dos Clientes.

MATRIZ GLOBAL - FACTORES DE RISCO

Variáveis de risco

Na análise dos riscos de branqueamento de capitais e de financiamento do terrorismo relacionados com os tipos de clientes, países ou zonas geográficas, bem como produtos, serviços, operações e canais de distribuição específicos, uma instituição financeira deveria ter em conta as variáveis de risco associadas a estas categorias de risco. Estas variáveis, consideradas de forma individual ou conjunta, podem aumentar ou reduzir o risco potencial e, conseqüentemente, ter impacto sobre o nível adequado das medidas. Entre os exemplos dessas variáveis contam-se os seguintes:

- O objeto de uma conta ou relação.
- O nível de bens depositados por um cliente ou o volume das operações efetuadas.
- A regularidade ou a duração da relação de negócios.

1. Clientes – factores de risco

Risco mais elevado

-A relação de negócio decorre em circunstâncias invulgares (por exemplo, uma distância geográfica significativa inexplicada entre a instituição financeira e o cliente).

-Clientes não residentes.

-Pessoas coletivas ou entidades sem personalidade jurídica que são estruturas de detenção de ativos pessoais.

-Sociedades com acionistas por conta de outra pessoa ou ações ao portador.

-Atividades que têm necessidade de fontes de financiamento consideráveis.

-A estrutura de propriedade da sociedade parece ser invulgar ou excessivamente complexa dada a natureza da atividade da sociedade.

Risco mais baixo

-As instituições financeiras e as atividades e profissões não financeiras designadas – na medida em que estão sujeitas às obrigações de combate ao branqueamento de capitais e ao financiamento do terrorismo nos termos das Recomendações do GAFI que implementaram eficazmente essas obrigações e são objeto de um controlo ou acompanhamento eficaz de acordo com as Recomendações que garantem o cumprimento dessas obrigações.

-As sociedades cotadas num mercado bolsista e sujeitas (em virtude das regras desse mercado, da lei ou de meios vinculativos) a deveres de informação que visam garantir uma transparência adequada dos beneficiários efetivos.

-As administrações ou empresas públicas.

2. Cliente / Transacções

A) risco acrescido devido a determinadas características, que incluem, entre outras

- i) Natureza do cliente (natureza jurídica, estrutura da propriedade, etc);

- ii) Natureza da actividade do cliente;
- iii) Complexidade, volume e natureza das transacções (a serem) efectuadas pelo cliente;
- iv) Origem dos fundos do cliente;
- v) Histórico do cliente;
- vi) Relacionamento do cliente com outros clientes (mesmo que estes últimos não sejam intervenientes nas respectivas relações de negócio estabelecidas com a instituição financeira).

B) maior risco de branqueamento de capitais e financiamento do terrorismo:

- i) Clientes cujas actividades sejam conhecidas por estarem associadas a corrupção (por exemplo: negociantes de armas);
- ii) Clientes que sejam pessoas politicamente expostas;
- iii) Clientes cuja origem dos fundos seja difícil de apurar;
- iv) Clientes com estruturas complexas ou pouco transparentes, que impeçam a identificação dos beneficiários efectivos;
- v) Clientes cujas actividades estejam relacionadas com negócios de grande liquidez, tais como:
 - Actividades relacionadas com serviços de pagamento (por exemplo: prestadores de remessas de valores, casas de câmbio, agentes que executam transferências de fundos ou outros negócios que visem a transferência de fundos);
 - Actividades relacionadas com a indústria do Jogo (por exemplo: casinos);
 - Negociantes de bens de valor elevado (por exemplo: negociantes de jóias, metais e pedras preciosas, negociantes de arte e antiquários, leiloeiras, agentes e corretores imobiliários);
 - Outros negócios que gerem montantes substanciais de dinheiro (por exemplo: negociantes de automóveis e agências de turismo).
- vi) Clientes que realizem as seguintes transacções:
 - Movimentos frequentes e injustificados de contas para outras instituições financeiras;
 - Movimentos frequentes e injustificados de fundos entre instituições financeiras diferentes;
- vii) Movimentos frequentes e injustificados entre diferentes jurisdições;
- viii) Transacções avultadas e de cariz complexo que não encaixam no perfil do cliente;
- ix) Clientes que solicitam produtos e serviços que não estão em conformidade com o conhecimento que a instituição financeira tem do cliente, isto é, que não se enquadram com o seu perfil.

3. Produto / Serviço / Canal de distribuição;

Os serviços de:

- i) correspondência bancária,
- ii) serviços de “*private banking*” e
- iii) serviços relacionados com depósitos ou pagamentos em numerário

iv) Operações anónimas (que podem incluir transacções em numerário).

v) Relações de negócio ou operações sem a presença física do cliente.

são geralmente considerados de risco elevado para as instituições financeiras. Existem vários exemplos de como o canal de distribuição de um serviço ou produto pode aumentar o risco da transacção porque não existe uma relação presencial com o cliente que permita aferir a veracidade dos elementos disponibilizados, nomeadamente, quando um cliente deseja abrir uma conta através da *internet*, ou quando não se encontra presente na mesma jurisdição da instituição financeira.

4. Localização geográfica.

Alguns países/jurisdições são potencialmente mais susceptíveis ao BC/FT que outros, tais como, países sem legislação apropriada de combate a estes crimes.

Este factor de risco implica que seja realizada a avaliação da localização:

i) País/jurisdição de residência do cliente;

ii) País/jurisdição de residência da empresa-mãe, subsidiárias e/ou beneficiário efectivo último;

iii) País/jurisdição onde a maioria das actividades de negócio são desempenhadas;

iv) País/jurisdição onde estão localizados os parceiros comerciais.

As seguintes categorias, entre outras, podem ser consideradas como possuindo um risco mais elevado associado à localização geográfica:

i) Países/jurisdições sujeitos a sanções, embargos ou outras medidas semelhantes emitidas pelas Nações Unidas ou por organizações internacionais semelhantes;

ii) País/jurisdição sujeito a qualquer tipo de sanção aplicada pelo Governo;

iii) Países identificados, por fontes credíveis, como países com ausência de leis, regulações e outras medidas de combate ao branqueamento de capitais e financiamento de terrorismo;

iv) Países identificados, por fontes credíveis, como países que apoiam actividades terroristas;

v) Países identificados, por fontes credíveis, como países onde existam níveis significativos de corrupção, ou de outras actividades criminosas.

Matriz de Risco - Clientes / Operações

<p>PRODUTOS/ SERVIÇOS / TRANSACÇÕES / CANAIS DE DISTRIBUIÇÃO</p> <p>CLIENTE</p>	Operações de Transferência de Fundos	Operações de Câmbio ao Balcão	Relações de negócio ou transações ocasionais estabelecidas/executadas presencialmente	Relações de negócio ou transações ocasionais estabelecidas/executadas com recurso a meios de comunicação à distância.	Pagamentos recebidos de terceiros desconhecidos ou não relacionados com o cliente ou com a atividade por este prosseguida	Produtos disponibilizados e transações realizadas num quadro de correspondência bancária com instituições de crédito estabelecidas em países terceiros.	
Clientes que mantenham relações de negócio, efetuem transações ocasionais ou realizem operações em geral que – pela sua natureza, pela sua frequência, pelos valores envolvidos ou por qualquer outro fator – se mostrem inconsistentes com o perfil daqueles.	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
<p>Clientes que, sem uma explicação plausível, movimentem numerário:</p> <p>a) Em montantes pouco usuais;</p> <p>b) Em montantes não justificados pelo perfil do cliente;</p> <p>c) Embalado ou empacotado de uma forma pouco habitual;</p> <p>d) Em mau estado de conservação; ou</p> <p>e) Representado por notas de pequena denominação, com o objetivo de proceder à sua troca por notas de denominação elevada.</p>	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
Clientes que, de algum modo, procurem persuadir os colaboradores da instituição financeira a não observar qualquer obrigação legal ou procedimento interno em matéria de prevenção do BC/FT.	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL
Clientes que mostrem relutância ou se recusem a disponibilizar os elementos identificativos/meios comprovativos/outros elementos de informação ou a promover as diligências de comprovação considerados necessárias.	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL
Clientes que mostrem relutância ou se recusem a disponibilizar documentos originais ou de valor equivalente.	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL
Clientes que mostrem relutância ou se recusem a proceder à atualização dos respetivos elementos de informação.	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
Clientes que mostrem relutância ou se recusem a estabelecer contactos presenciais	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO

Matriz de Risco - Clientes / Operações

<p>PRODUTOS/ SERVIÇOS / TRANSACÇÕES / CANAIS DE DISTRIBUIÇÃO</p> <p>CLIENTE</p>	Operações de Transferência de Fundos	Operações de Câmbio ao Balcão	Relações de negócio ou transações ocasionais estabelecidas/executadas presencialmente	Relações de negócio ou transações ocasionais estabelecidas/executadas com recurso a meios de comunicação à distância.	Pagamentos recebidos de terceiros desconhecidos ou não relacionados com o cliente ou com a atividade por este prosseguida	Produtos disponibilizados e transações realizadas num quadro de correspondência bancária com instituições de crédito estabelecidas em países terceiros.	
<p>Clientes que prestem elementos identificativos, meios comprovativos ou outros elementos de informação:</p> <p>a) Pouco credíveis quanto à sua autenticidade;</p> <p>b) Pouco explícitos quanto ao seu teor;</p> <p>c) De difícil verificação por parte da instituição financeira; ou</p> <p>d) Com características pouco usuais.</p>	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
<p>Clientes que adiem ou não efetuem a entrega de documentação suscetível de apresentação à instituição financeira em momento posterior ao estabelecimento da relação de negócio.</p>	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
<p>Clientes que procurem suspender ou alterar a relação de negócio ou a transação ocasional depois de lhes serem solicitados os elementos identificativos, os respetivos meios comprovativos ou outros elementos de informação relevantes para o conhecimento do cliente.</p>	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
<p>Clientes que, sem aparente relação entre si, apresentem moradas ou dados de contacto (número de telefone, número de fax, endereço de correio eletrónico ou outros) comuns.</p>	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
<p>Clientes cuja morada ou dados de contacto (número de telefone, número de fax, endereço de correio eletrónico ou outros) se revelem incorretos ou estejam permanentemente inoperacionais, em especial quando a tentativa de contacto da instituição financeira tiver lugar pouco tempo após o estabelecimento de uma relação de negócio.</p>	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
<p>Clientes cuja morada ou dados de contacto (número de telefone, número de fax, endereço de correio eletrónico ou outros) mudem com frequência.</p>	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
<p>Clientes que aparentem estar a atuar por conta de um terceiro, sem, contudo, o revelarem à instituição financeira ou, mesmo revelando tal circunstância, se recusem a fornecer os necessários elementos de informação sobre o terceiro por conta do qual atuam.</p>	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO

Matriz de Risco - Clientes / Operações

<p>PRODUTOS/ SERVIÇOS / TRANSACÇÕES / CANAIS DE DISTRIBUIÇÃO</p> <p>CLIENTE</p>	Operações de Transferência de Fundos	Operações de Câmbio ao Balcão	Relações de negócio ou transações ocasionais estabelecidas/executadas presencialmente	Relações de negócio ou transações ocasionais estabelecidas/executadas com recurso a meios de comunicação à distância.	Pagamentos recebidos de terceiros desconhecidos ou não relacionados com o cliente ou com a atividade por este prosseguida	Produtos disponibilizados e transações realizadas num quadro de correspondência bancária com instituições de crédito estabelecidas em países terceiros.	
Relações de negócio ou transações ocasionais que se desenrolem em circunstâncias inabituais, face ao perfil expectável do cliente e aos demais elementos caracterizadores da relação de negócio ou transação ocasional.	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
Clientes/beneficiários efetivos residentes ou que desenvolvam atividade nos países ou jurisdições referidos nos subseqüentes números 20 a 26	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
Clientes que prossigam atividades que envolvam transações em numerário de forma intensiva.	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
PEP's Pessoas politicamente expostas	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
Correspondentes bancários domiciliados em países terceiros.	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
Clientes/beneficiários efectivos que tenham sido objeto de sanções ou medidas restritivas impostas pelo Conselho de Segurança das Nações Unidas ou pela União Europeia.	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL	INACEITÁVEL
Organizações sem fins lucrativos	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO

Matriz de Risco - Transferências de Fundos

<p>GRAU DE RISCO</p> <p>EVENTO</p>	BAIXO	NORMAL	ALTO	INACEITÁVEL
Transferências segmentadas em várias operações, por forma a evitar o cumprimento de obrigações legais e regulamentares previstas para operações que atinjam um determinado montante.			X	
Transferências para o exterior que se mostrem inconsistentes com a atividade conhecida do cliente, em razão, designadamente, do montante, da frequência ou dos beneficiários das mesmas.			X	
Transferências em que não exista uma conexão aparente entre a atividade conhecida do cliente e os ordenantes/beneficiários das operações ou os países/zonas geográficas de origem/destino das mesmas.			X	
Transferências em que o cliente se recuse ou mostre relutância em dar uma explicação para a realização da operação.				X
Transferências a favor de um beneficiário ou proveniente de um ordenante acerca do qual o cliente revele dispor de pouca informação ou mostre relutância em fornecê-la.			X	
Transferências por montantes superiores àqueles que eram expectáveis aquando do estabelecimento da relação de negócio com o cliente.			X	
Transferências para o exterior efetuadas a favor de um conjunto alargado de beneficiários que, aparentemente, não tenham laços familiares com o cliente.			X	
Transferências efetuadas a favor de um conjunto alargado de beneficiários, sendo estes nacionais de países ou jurisdições reconhecidamente relacionados com atividades terroristas.				X
Transferências ordenadas regularmente pela mesma pessoa ou entidade, sendo diferentes os destinatários e iguais ou aproximados os montantes transferidos			X	
Transferências ordenadas regularmente pela mesma pessoa ou entidade, sendo comum o destinatário e diferentes os montantes transferidos.			X	
Transferências ordenadas por pessoas ou entidades diferentes e destinadas ao mesmo beneficiário, na mesma data ou em datas muito próximas.			X	
Transferências ordenadas por pessoas ou entidades diferentes que tenham em comum um ou mais elementos de informação pessoais (apelido, morada, entidade patronal, número telefónico, etc.), efetuadas na mesma data ou em datas muito próximas.			X	
Transferências ordenadas por pessoas ou entidades diferentes, sendo os respetivos fundos disponibilizados por apenas um deles.			X	
Transferências efetuadas com recurso a fundos disponibilizados por um terceiro.				X
Transferências de montantes elevados, com instruções de disponibilização dos fundos ao respetivo destinatário em numerário.			X	
Transferências do exterior em que os valores transferidos sejam imediatamente transferidos para outros beneficiários.			X	

Matriz de Risco - Transferências de Fundos

<p>GRAU DE RISCO</p> <p>EVENTO</p>	BAIXO	NORMAL	ALTO	INACEITÁVEL
Transferências acompanhadas de instruções para que os montantes transferidos sejam disponibilizados a terceiros e não aos beneficiários das operações			X	
Transferências para o exterior efetuadas de forma cruzada com transferências do exterior pelos mesmos valores ou valores aproximados			X	
Transferências em que os clientes evidenciem um interesse e uma curiosidade fora do comum sobre o sistema de transferência de fundos, designadamente procedimentos operativos, limites, etc.			X	
Transferências para o exterior efetuadas em períodos temporais aparentemente não coincidentes com o pagamento da remuneração salarial, em especial quando ordenadas por cidadãos imigrantes.			X	

Matriz de Risco - Câmbios

<p>GRAU DE RISCO</p> <p>EVENTO</p>	<p>BAIXO</p>	<p>NORMAL</p>	<p>ALTO</p>	<p>INACEITÁVEL</p>
<p>Operações segmentadas em várias compras/vendas, por forma a evitar o cumprimento de obrigações legais e regulamentares previstas para operações que atinjam um determinado montante.</p>			<p>X</p>	
<p>Operações que se mostrem inconsistentes com a atividade conhecida do cliente, em razão, designadamente do montante ou da frequência das mesmas.</p>			<p>X</p>	
<p>Operações em que os clientes pretendam trocar somas avultadas numa determinada moeda estrangeira por outra moeda estrangeira.</p>			<p>X</p>	
<p>Operações com clientes não residentes que aparentem deslocar-se ao território nacional com o expreso propósito de efetuar compras/vendas de moeda.</p>				<p>X</p>
<p>Operações frequentes com notas de valor facial reduzido ou com divisas de reduzida circulação internacional.</p>				<p>X</p>
<p>Operações em que os clientes deem instruções à sociedade financeira no sentido de o contravalor ser posteriormente entregue a um terceiro.</p>				<p>X</p>
<p>Operações em que os clientes insistam no recebimento do contravalor através de cheque da instituição financeira, não sendo esta prática usualmente adotada pela mesma.</p>				<p>X</p>
<p>Operações em que os clientes solicitem o recebimento do contravalor, em moeda estrangeira, em notas com o mais elevado valor facial possível.</p>			<p>X</p>	