Open Banking

Guia de recomendações para participantes do Open Banking Brasil

Prevenção a Fraudes & PLD-FT

Versão 4.0. 24.08.2021

Sumário

1. Histórico de Revisão

Data	Versão	Descrição das alterações
30/03/2021	0.1	Criação do documento
30/04/2021	1.0	Revisão do documento – Febraban (1.1)
30/05/2021	2.0	Revisão do documento – Convenção (1.1/1.2/1.3/2.1/2.2/2.3)
30/07/2021	3.0	Revisão final do documento pela convenção
23/08/2021	4.0	Revisão final do GT de Prevenção

2. **Apresentação**

Este manual descreve as principais ameaças e recomendações de Prevenção a Fraude, Lavagem de Dinheiro e Financiamento ao Terrorismo para os participantes do Open Banking no Brasil.

Tem como objetivo descrever como devem ser implementadas as estratégias de mitigação dos riscos identificados na análise feita pelo GT de Prevenção a Fraudes da convenção OPB, do escopo da fase 3 sobre iniciação de transação de pagamento.

3. **Escopo**

Estas especificações fazem parte de um trabalho em desenvolvimento, e novos conceitos e definições serão abordados em versões futuras deste documento. Dessa maneira, nenhuma informação aqui apresentada deve ser considerada final para qualquer propósito.

Este documento não busca alterar nenhum tipo de norma ou legislação a respeito do tema, e sim recomendar melhores práticas para criarmos um ecossistema seguro.

4. **Referências**

Estas especificações baseiam-se, referenciam, e complementam onde aplicável, os seguintes documentos:

Referência[1]	Considerações
Especificação OAuth	Protocolos Open Source utilizados no Open Banking Brasil
Protocolo OpenId	Protocolos Open Source utilizados no Open Banking Brasil – importante atenção ao protocolo de Redirect
Protocolo FAPI	Protocolos Open Source utilizados no Open Banking Brasil
Protocolo CIBA	Protocolos Open Source utilizados no Open Banking Brasil
Protocolo PSD2	Protocolos Open Source utilizados no Open Banking Brasil
Lei 9.613/98 e 12.683/12	Lei federal referentes à prevenção a lavagem de dinheiro
Lei 13810/19, Resolução 44 e Carta Circular 3977	Leis e normas de atendimento à CSNU
Lei 13260/16	Lei federal referentes à prevenção de atos terroristas
Circulares BCB nº 3.978/20 e 4.001/20	Norma referentes à prevenção a lavagem de dinheiro
Resolução Conjunta nº 1, de 4 de maio de 2020, conforme em vigor (“Resolução Conjunta”)	Resolução Open Banking Brasil – dispõe sobre a implementação do Sistema Financeiro Aberto
Instruções Normativas BCB para o Open Banking	Regras gerais do Open Banking
FAQ e Base normativa	FAQ do Banco Central

1: Ou qualquer norma ou lei que venha a substituí-las

4. **Referências**

Os itens abaixo são leituras indispensáveis para o entendimento do funcionamento do Open Banking e dos mecanismos propostos nesse Guia

Referência	Considerações
Portal do Cidadão	Site do Open Banking voltado para o cidadão
Área do Desenvolvedor	Site do Open Banking voltado para o desenvolvedor, com definições técnicas e especificações
Guia de UX	Guia de Experiência do Usuário – importante atenção ao o fluxo de autenticação e de validação de CPF
Processo sistêmico de devolução de fundos (PIX)	Definição do Banco Central para Processo de Devolução Sistêmica em Fraudes envolvendo PIX
Temporizador transacional PIX	Definição do Banco Central para processo de temporização das transações em casos com suspeitas de fraudes envolvendo PIX
Processo de resolução de disputas	Regulamento de Resolução de Disputas no âmbito do Open Banking – importante atenção ao *liability* da instituição detentora em casos de suspeita de fraude
LGPD - Lei Geral de Proteção aos Dados	Importante atenção ao Artigo 11, II, g
Canal no Youtube	Página do Open Banking com vídeos explicativos sobre infraestruturas e processos

5. **Introdução**

A segurança da infraestrutura, a prevenção a fraudes e a PLD/FT são elementos primordiais a serem observados pelas Participantes.

A questão de combate a fraudes mostra-se tão relevante no OBB que (i) demandas de clientes decorrentes de fraudes devem ser identificadas e reportadas pelas Participantes nos relatórios semestrais de compartilhamento de dados (cf. art. 33, §1º, I, da Resolução Conjunta) e (ii) casos de sua suspeita justificada podem levar à proposta ao cliente de revogação do consentimento pelas Participantes transmissoras de dados ou detentoras de contas (cf. art. 15, §2º, da Resolução Conjunta).

Ademais, as próprias Participantes comprometem-se com procedimentos e controles internos no compartilhamento, os quais se somam a políticas, procedimentos e controles internos já adotados pelas próprias Participantes, inclusive para prevenção à utilização do Sistema Financeiro para prática de crimes de lavagem de dinheiro e financiamento ao terrorismo.

Inclusive para prevenção à utilização do Sistema Financeiro para prática de crimes de lavagem de dinheiro e financiamento ao terrorismo, os Participantes devem garantir atendimento a Lei nº 9.613/1998, que impõe obrigações para a prevenção e combate ao crime de lavagem de dinheiro e financiamento ao terrorismo, tais quais as obrigações, estabelecidas pelos artigos 10 e 11 da Lei, que estabelece o dever de identificar clientes, manter registros e comunicar operações financeiras e ainda o envio das comunicações de operações financeiras e o envio de comunicações de não ocorrência de propostas, transações ou operações passíveis de serem comunicadas. A Lei 13.260/2016 relativa a atos terroristas, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista e Lei 13.810/2019 dispõe sobre o cumprimento de sanções impostas por resoluções do Conselho de Segurança das Nações Unidas, incluída a indisponibilidade de ativos de pessoas naturais e jurídicas e de entidades, e a designação nacional de pessoas investigadas ou acusadas de terrorismo, de seu financiamento ou de atos a ele correlacionados.

5. **Introdução**

O dever de prevenção a fraudes e PLD/FT se impõe às Participantes e também à Estrutura que, em sua atuação na governança, deve ser orientadora e garantidora de um ecossistema que saiba administrar os riscos advindos da exposição a fraudes.

O compartilhamento de serviços de iniciação de pagamentos possui aspectos operacionais que podem elevar os riscos de ataques e fraudes, quando comparados com operações de compartilhamento de dados. Esses aspectos devem ser considerados na modelagem e na estratégia de prevenção a fraudes de cada Participante, e na atuação orientadora e exemplar da Estrutura nessa matéria.

Este Guia, portanto, é composto de recomendações que poderão ser observadas diretamente pelas Participantes, com monitoramento da Estrutura. Apresenta detalhes técnicos associados a requisitos de segurança a serem adotados nas diferentes estratégias de prevenção a fraudes e a tecnologias que compõem a infraestrutura do OBB, com foco no escopo da Estrutura, sem prejuízo da consequente supervisão do BCB.

6. **Dicionário**

Conta fria

O Fraudador em posse dos dados cadastrais do cliente, se passa pelo mesmo e abre contas em nome do cliente com o objetivo de movimentar valores provenientes de golpes financeiros e/ou outros crimes de natureza diversa.

Engenharia social

O fraudador utiliza a combinação de texto e contexto para colocar sua vítima em um golpe com o objetivo de causar danos financeiros ou de imagem. Os criminosos utilizam uma variedade enorme de contextos para que o cliente acredite no que ele está dizendo e concorde em passar as credenciais de pagamento ou de acesso a contas financeiras para que o mesmo possa executar a invasão da conta e subtrair valores. Também conhecido como golpes. Exemplos: Golpe do motoboy, golpe do *WhatsApp*, golpe da URA falsa e etc.

Conta Laranja

O fraudador usa conta de terceiros, pessoas que fornecem seu nome, CPF e dados bancários, para movimentar valores e adquirir bens, para prática de atos e atividades ilícitas

Phishing

Mensagens e e-mails falsos que induzem o usuário a clicar em links suspeitos e informar dados de credenciais de acesso ou pagamento, em páginas falsas ou instalar *malware* para ataques posteriores.

Golpe do falso funcionário

O fraudador entra em contato com a vítima, se passando por funcionário de central do banco ou de cartão de crédito e solicita credenciais ou que o mesmo faça transações de teste, estorno entre outras justificativas.

6. **Dicionário**

Invasão de conta

O fraudador ou criminoso em posse das credenciais de acesso do cliente, acessa a conta do Cliente com o objetivo de obter ganhos financeiros por meio de transferências, pagamentos e contratação de empréstimos.

Pushing

É um golpe de engenharia social no qual, após realizar uma invasão de contas ou abrir uma Conta Fria, o fraudador inicia a solicitação de inúmeros processos de consentimento ou iniciação de pagamentos de uma conta origem, para inúmeras contas destino. Ao se acostumarem com esse processo, os usuários podem se tornar mais vulneráveis a golpes, aprovando transações que não foram solicitadas.

***As modalidades de fraudes acima descritas podem ser praticadas de maneira independente ou também combinando diferentes tipos de ataques.**

Roubo de device

O fraudador invade a conta da vítima após roubo do celular. Com o aparelho em mãos, o fraudador tenta adivinhar a senha de desbloqueio usando dados cadastrais do cliente ou testando combinações comuns (ex. 123456 ou 111111). O fraudador desabilita a função de encontrar o celular para evitar que o dono rastreie ou apague as informações do aparelho. Em seguida, tenta descobrir qual a senha do aplicativo do banco ou de instituições de pagamento procurando por “senha” no campo de busca do celular ou tenta acessar o recurso de “senhas” em “ajustes”. Com essa informação, entra no aplicativo do banco ou da instituição de pagamento e utiliza a função de recuperação de senha.

PLD/FT

Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo.

7. **Proposta de prevenção a fraudes**

7.1 Framework de prevenção a fraudes

Este framework de prevenção a fraudes é aplicável às Participantes, a partir de 4 (quatro) pilares orientadores:

i. Prevenção a Fraudes;
ii. Detecção de Fraudes;
iii. Remediação de Fraudes; e
iv. Repressão a Fraudes.

Para cada um dos pilares orientadores, foram mapeados:

i. Orientações/recomendações a serem observadas pelas Participantes; e

ii. Possíveis riscos ao OBB.

Cada uma das orientações que compõem cada um dos pilares estão a seguir detalhados, conforme níveis de recomendação :

i. crítico, priorizadas pelas Participantes desde o lançamento (Go-Live) da fase 3;

ii. alto, priorizadas pelas Participantes logo após o lançamento (Go-Live) da fase 3.

7. **Proposta de prevenção a fraudes**

7.1.1 Prevenção

I. Recomendações de Nível Critico

1. Campanha de educação de clientes pelas Participantes
2. Autenticação de múltiplos fatores (MFA)
3. Redirect - OpenID
4. Validação de identidade do cliente

Riscos

1. Abertura de Conta Fria e uso de Conta Laranja em Participantes iniciadoras de transações de pagamento
2. Invasão de contas
3. Engenharia social
4. *Phishing*
5. *Pushing*
6. Participantes iniciadoras de transação de pagamento criadas para prática de fraudes
7. Fragilidade no processo de segurança na adesão ao diretório centralizado do Open Banking
8. Aumento de desacordo comercial

7. **Proposta de prevenção a fraudes**

7.1.2 Detecção

I. Recomendações de nível crítico

1. Ferramenta de monitoria transacional paramétrica real-time
2. Monitoramento de transações financeiras e não-financeiras

II. Recomendações de nível alto

1. Modelos de *machine learning* transacional
2. Temporizador transacional

Riscos

1. Ataques de alta velocidade, com transferência e saques em sequência
2. Ataques de força bruta
3. Ausência de capacidade de detecção analítica, modelos de *machine learning* e sistemas de detecção real time
4. Falta de tempo hábil para treino de algoritmos *de machine learning*

7. **Proposta de prevenção a fraudes**

7.1.3 Remediação

I. Recomendações de nível crítico (conforme normas próprias aplicáveis)

1. Operação contínua e integral

Riscos

1. Auto fraude
2. Ausência de bases centralizadas de mercado para consulta de dados utilizados em fraudes no OBB
3. Obrigação de manter os limites transacionais de meios de pagamento similares mas que tenham nível de risco diferentes
4. Ausência de padronização do processo de interferência nas transações de instituições iniciadoras de transação de pagamento
5. Ausência de política de responsabilidade para Participante que abriu a Conta Fria, em inobservância à regulamentação aplicável

7. **Proposta de prevenção a fraudes**

7.1.4 Repressão

I. Recomendações de nível alto

1. Colaboração para identificação de *Phishing* entre os Participantes

8. **Detalhamento das capacidades**

8.1 Prevenção

8.1.1 Campanha de educação de clientes – nível crítico

I.O QUE É?
As campanhas de educação de clientes será promovida diretamente pelas Participantes para orientação de clientes na proteção dos seus dados cadastrais e transacionais no OBB. Incluem dicas de seguranças, alertas nas interfaces das Participantes, informações detalhadas sobre os golpes e fraudes mais praticados e formas de prevenção adequada

II.COMO FUNCIONA?
As Participantes prepararão, de acordo com suas políticas de comunicação e de segurança, campanhas de educação direcionadas aos clientes, por meio de canais digitais, com objetivo de conscientizar os clientes sobre o uso atento e correto das funcionalidades disponíveis no âmbito do OBB e sobre o dever de cada cliente de manter seus dados em segurança.

As campanhas de educação poderão conter as seguintes formas de comunicação:

- Mensagens de esclarecimento sobre o uso das funções do OBB por meio de mídias sociais
- Mensagens de esclarecimento sobre o uso das funções do OBB por meio de canais digitais (APP, Portal, Internet Banking, etc.)

O conteúdo dessas campanhas de educação abordará os seguintes temas:

- Funcionalidades habilitadas pelo OBB (compartilhamento de dados, iniciação de pagamentos, etc.)
- Dados compartilhados pelo cliente
- Finalidades de uso desses dados compartilhados pelas Participantes
- Dicas de segurança ao cliente
- Deveres e responsabilidades dos clientes quanto à auto fraude

As mensagens dessa campanha de educação poderão ser encaminhadas pelos canais de comunicação de cada Participante diretamente aos seus clientes.

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

As campanhas de educação pretendem mitigar o uso incorreto das funções habilitadas no OBB pelos clientes, por meio dos canais digitais oficiais, além de evitar golpes, fraudes, vazamento de dados, perdas financeiras, entre outros riscos.

Os clientes deverão ser orientados pelas Participantes para se atentar a comunicações não oficiais das Participantes, por e-mails, SMS ou ligações, especialmente comunicações contendo links suspeitos.

IV. EXPERIÊNCIA DO USUÁRIO

Os clientes podem receber as comunicações por meio de: SMS, notificação nos canais digitais (*push*), e-mails, redes sociais (Instagram, Facebook, Twitter, etc.) e demais veículos de comunicação (TV, rádio, jornais, etc.), a critério de cada participante.

8. **Detalhamento das capacidades**

8.1.2 Autenticação de múltiplos fatores (MFA) – nível crítico

I. O QUE É?
A utilização de ferramentas de segurança de Autenticação de Múltiplos Fatores (“MFA”), que consiste em associar mais de uma forma de autenticação para adicionar camadas de proteção aos processos transacionais para autenticar a identidade do usuário.
Os fatores de autenticação são itens ligados ao usuário, inclusive, sem limitação:

- Algo que o usuário possui (uma chave segura ou um smartphone)
- Algo que o usuário sabe (uma senha ou um PIN)
- Algo que o usuário é (uma impressão digital ou reconhecimento facial)

II. COMO FUNCIONA?

As Participantes detentoras de conta e as iniciadoras de pagamento poderão utilizar MFA na jornada de confirmação e autenticação em todas as transações.

A MFA adiciona novas camadas de verificação da identidade, trazendo maior segurança em todo o processo. Quando o cliente inserir seu login e senha, o Portal poderá validar e solicitar, por exemplo, um código randômico, uma biometria ou um dispositivo habitualmente vinculado ao cliente.
O uso de MFA poderá ocorrer de acordo com o nível de risco (score) observado em cada processo executado pelo cliente, seguindo as políticas de segurança específicas das Participantes, conforme as orientações e padrões de segurança recomendados no OBB.

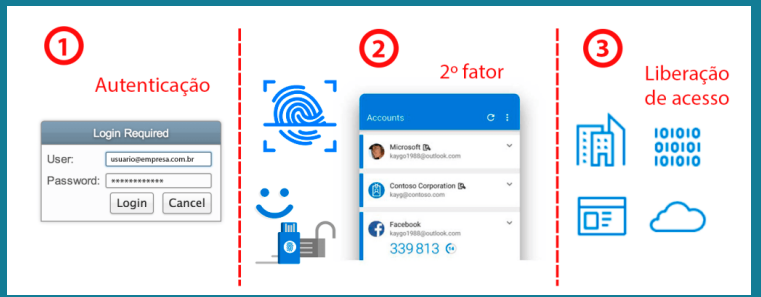

Figura 1 - Exemplo de processo com autenticação com múltiplos fatores

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

A solicitação de MFA traz maior confiabilidade e dificulta a violação de segurança e o comprometimento de dados, minimizando danos graves ou ataques de identidades dos clientes, das Participantes e da Estrutura.
As principais ações a serem evitadas e os principais riscos a serem mitigados com a utilização do MFA no OBB são:

i. consulta indevida de dados,
ii. uso de Engenharia Social e
iii. Invasão de Conta.

IV. EXPERIÊNCIA DO USUÁRIO

Na jornada do cliente no OBB, a aplicação do MFA poderá ser solicitada para maior segurança e confiabilidade nas identificações e transações realizadas.

8. **Detalhamento das capacidades**

8.1.3 Redirect - OpenID – nível crítico

I. O QUE É?

O REDIRECT entre aplicativo (APP) e/ou Browser no Desktop é o fluxo que permite que a Participante iniciadora de pagamento redirecione o processo de uma aplicação (APP) ou navegador de uma Participante para outro aplicativo (APP) ou navegador instalados no mesmo device, recomendando-se o uso de aplicativo (APP) da Participante detentora de conta.

Este processo permite que o cliente realize uma autenticação na Participante enquanto estiver utilizando a Participante iniciadora de pagamentos, com os mesmos métodos de autenticação e login que são utilizados para acessar seu canal digital.

8. **Detalhamento das capacidades**

8.1.4 Validação de identidade do cliente – nível crítico

I. O QUE É?

Na iniciação de pagamentos no canal Open Banking, é obrigatório que as Participantes garantam que a pessoa natural que iniciou a jornada de pagamento seja a mesma pessoa que irá autenticar e concluir a transação na instituição receptora.

Os métodos de autenticação e identificação das pessoas ficam sob a responsabilidade de cada Participante detentora de conta, que deverá validar as credenciais e informações disponibilizadas pelas instituições iniciadoras de pagamentos.

II. COMO FUNCIONA?

Maiores orientações estão no Guia de Experiência do Usuário.

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

Ao implementar esse controle, é possível mitigar o risco de um fraudador, em posse de uma conta iniciadora de pagamento, iniciar inúmeras transações em contas de diferentes Participantes.

IV. EXPERIÊNCIA DO USUÁRIO

Na situação em que um cliente idôneo tente iniciar uma transação em nome de outra pessoa natural, o cliente receberá uma mensagem de negativa devido ao fato de o seu CPF ser diferente da conta da iniciadora, como por exemplo, um marido tentando realizar um pagamento em nome da esposa.

8. **Detalhamento das capacidades**

8.1.5 Segurança de device – nível crítico

I. O QUE É?

Segurança de device consiste em todas as ferramentas que podem ser usadas por Participantes nas jornadas de consentimento e na iniciação de pagamentos no OBB, a fim de tornar mais robustas as camadas de proteções e criar uma jornada mais segura para os clientes.

II. COMO FUNCIONA?

Para o cliente, os processos de segurança do device são praticamente imperceptíveis durante as interações. As variáveis digitais e as validações dos componentes irão mapear o perfil seguro do cliente autenticado, tornando-o elegível à jornada requerida e garantindo vias de segurança durante suas solicitações e transações.

As proteções ofertadas, tanto nativas quanto de bordas e de processos, podem ser adicionadas a variáveis digitais e *machine learning* de análises de risco, reforçando o processo naquele device.

Alguns exemplos de funcionalidades que podem diminuir as fragilidades do canal OBB, a serem adotadas pelas Participantes, são:

- Aplicação Anti-automação
- Certificado Digital
- Criptografia end-to-end
- Geolocalização
- Habitualidade do device
- Identificação do dispositivo (ID Sessão, Device ID, IP, UserAgent)
- *Machine learning*
- Múltiplos Fatores de Autenticações (MFA)
- Ofuscação de Código (técnicas de desenvolvimento de código para dificultar o entendimento e evitar ataques)
- *Firewall* de borda
- Componentes de verificação comportamental do device e usuários
- Variáveis digitais

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

Os protocolos de segurança que envolvam o *device* têm o objetivo de assegurar melhor jornada e experiência, além de garantir:

- Confiabilidade do usuário
- Inibição de *hacking*
- Melhor perfilamento do cliente durante as transações
- Aperfeiçoamento da experiência do cliente
- Maior proteção dos dados do cliente
- Aumento da robustez da aplicação (APP)

.

IV. EXPERIÊNCIA DO USUÁRIO

O cliente poderá ter uma jornada mais completa e satisfatória se seus dados estiverem sendo protegidos com uma segurança robusta em cada etapa da interação. Dessa maneira, ele mantém um relacionamento de confiança durante o uso da aplicação (APP), compartilhamento de seus dados e realização de transações.

8. **Detalhamento das capacidades**

8.2 Detecção

8.2.1 Ferramenta de monitoria transacional paramétrica real-time – nível crítico

I. O QUE É?

Trata-se de uma ferramenta com capacidade técnica de receber e processar em tempo real dados inerentes às transações e às interações efetuadas no OBB.
O objetivo é monitorá-las de forma automatizada, sob a ótica de prevenção e detecção de fraudes e PLD/FT, baseada em parâmetros pré-estabelecidos e regras de monitoramento de cada Participante.

II.COMO FUNCIONA?

As Participantes devem implementar, em até 12 (doze) meses, uma ferramenta que funcionará como filtro de operações fraudulentas e suspeitas de PLD/FT.

As Participantes que já possuem tal ferramenta deverão implementar uma rotina de monitoramento e de regras de prevenção e detecção de fraudes e PDL-FT para todas as transações do OBB. Tal ferramenta deverá permitir a criação e manutenção dessas rotinas de monitoramento, com respeito a avaliações internas de risco das Participantes, em tempo real, objetivando o monitoramento das transações financeiras e não financeiras efetuadas no ecossistema do OBB.

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

Com os dados das transações financeiras e não financeiras recebidos e processados pela ferramenta em tempo real, as Participantes terão a capacidade de elaborar regras baseadas em parâmetros de suspeitos anteriormente conhecidos, filtrando transações regulares de transações irregulares. Dessa forma, será possível monitorar e dar tratamento a situações suspeitas, reduzindo o risco de perdas financeiras e aumentando o nível de segurança e a credibilidade do OBB para clientes e Participantes.

IV. EXPERIÊNCIA DO USUÁRIO

A implementação e manutenção de uma ferramenta de monitoramento em tempo real agregará positivamente para a experiência do usuário, uma vez que possa ajudar as Participantes a diferenciarem de maneira mais fácil e rápida operações fraudulentas de operações não fraudulentas, contribuindo, inclusive, para manter taxas mais altas de conversão e aprovação das transações com maior segurança e sustentabilidade.

8. **Detalhamento das capacidades**

8.2.2 Monitoramento de transações financeiras e não- financeiras – nível alto

I. O QUE É?

O monitoramento é a capacidade de as Participantes coletarem e analisarem informações de forma massiva, com o objetivo de prever e identificar possíveis irregularidades nas transações efetuadas pelo OBB.

As transações não-financeiras podem ser configuradas por algumas interações dentro do ecossistema do OBB, tais como criação de cadastro ou conta, alteração de dados cadastrais, uso de credenciais, alteração de senhas de acesso a sistemas e aplicativos (APP).

As transações financeiras são aquelas que envolvem movimentações financeiras, como, por exemplo, pagamentos, liberação de crédito, entre outras.

II. COMO FUNCIONA?

As Participantes deverão elaborar e manter atualizadas as políticas e processos internos de monitoramento e resposta a transações suspeitas de irregularidades no âmbito de fraudes e PLD/FT em observância à regulamentação e à legislação vigentes. As Participantes também deverão implementar controles internos por meio de relatórios, indicadores, regras e parâmetros de monitoramento pré-estabelecidos por essas políticas, a fim de monitorar as transações efetuadas no OBB. O monitoramento das transações deve ser construído conforme uma abordagem baseada em riscos de cada Participante. Esse monitoramento deverá se basear principalmente no perfil das transações efetuadas, com avaliação de parâmetros, inclusive, horário das transações, valor, localização, finalidade da transação, histórico e perfil de utilização do cliente. Caso se identifiquem irregularidades, a Participante poderá gerar alertas ou interromper transações, a seu critério, observada a regulamentação e legislação vigentes.

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

O monitoramento de fraude e a PLD/FT permitem a identificação e o tratamento de transações suspeitas de irregularidade, fatores essenciais para a segurança, confiabilidade e manutenção do OBB.
Ainda, esse monitoramento colabora com a manutenção de baixos índices de fraudes no ecossistema do OBB, com potencial redução do nível de reclamações e insatisfações de clientes. Mitiga também o risco de perdas financeiras para Participantes e clientes, em decorrência da possibilidade de intervenção rápida para tratamento de transações irregulares.

IV. EXPERIÊNCIA DO USUÁRIO

O monitoramento de transações melhora a experiência do cliente no que se refere à segurança, à sustentabilidade e à confiabilidade do OBB, ao maximizar a prevenção a fraudes e a PLD/FT.
Esse monitoramento pode gerar maior tempo de espera na aprovação da transação para um pequeno percentual de transações que necessitem de análise mais aprofundada, devido a uma suspeita de fraude ou lavagem de dinheiro e financiamento a terrorismo. De todo modo, esse é um procedimento comum já aplicável a outros produtos e serviços no mercado financeiro, com o qual os clientes já têm familiaridade.

8. **Detalhamento das capacidades**

8.2.3 Modelos de *machine learning* transacional – nível alto

I. O QUE É?

O *Machine Learning*, ou aprendizado de máquina, é uma das principais aplicações conhecidas no campo da inteligência artificial e se utiliza de um ou mais algoritmos matemáticos para resolver problemas anteriormente estabelecidos. É altamente aplicável ao processo de prevenção, detecção e investigação de fraudes e PLD/FT.

II. COMO FUNCIONA?

Os modelos de machine learning baseados em algoritmos matemáticos têm capacidade de interpretar, avaliar e correlacionar diversos dados e eventos nas transações efetuadas, de forma veloz, precisa e automatizada, e apoiarão significativamente a identificação de eventuais desvios na utilização do OBB para aplicação de fraudes.

Esses modelos devem ser aplicados no processo transacional, a fim de antever e detectar eventuais tentativas de fraudes e de atividades ilícitas.

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

O uso de modelos de *machine learning* aumenta significativamente a capacidade de as Participantes identificarem desvios comportamentais no padrão comum dos clientes e no ecossistema do OBB.

Tal tecnologia, quando aplicada na prevenção a fraudes em transações financeiras ou não financeiras, pode apoiar as Participantes na prevenção, detecção e remediação de um maior número de fraudes em menor tempo e de forma automatizada, com redução do falso-positivo na identificação de situações suspeitas.

Esses modelos minimizam a chance de sucesso do fraudador, uma vez que são capazes de interpretar e processar grande quantidade de dados.

IV. EXPERIÊNCIA DO USUÁRIO

Não há impacto significativo perceptível na experiência dos usuários. Trata-se de uma camada extra de segurança nas transações, normalmente aplicada antes ou em conjunto do processo de autorização.

8. **Detalhamento das capacidades**

8.3 Remediação

8.3.1 Operação Contínua e Integral (24x7x365) – nível crítico

I. O QUE É?

Trata-se de um serviço de atendimento e suporte ao cliente para tratamento das demandas e de remediação com foco em fraudes ou suspeitas de fraude, com disponibilidade de 24h por dia, todos os dias da semana e do ano. Essa operação pode ser totalmente sistêmica, híbrida (sistêmica mais humana) ou totalmente humana.

II.COMO FUNCIONA?

Às Participantes, sugere-se manter um serviço de atendimento ao cliente seguindo os padrões de atendimento da legislação vigente, com o objetivo de dar ao cliente o primeiro atendimento e dar o suporte para eventuais queixas.

Esse serviço de atendimento deve suportar processos decorrentes de fraude confirmada ou casos de suspeita de fraudes, conforme reportados pelos clientes e/ou por outras Participantes; quando necessário, as solicitações devem seguir para tratativa interna das Participantes ou, se for o caso, a Participante poderá se valer da resolução de disputas do OBB.

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

A disponibilização desse serviço de atendimento mitiga eventuais reclamações do cliente, melhorando a experiência do cliente e colabora para identificação e mitigação mais ágil de fraudes.

IV. EXPERIÊNCIA DO USUÁRIO

Os serviços de atendimento contribuem para que clientes sanem eventuais dúvidas sobre transações, com suporte necessário nos casos de reporte de fraude ou de suspeitas de fraudes no momento de sua constatação. Em sua experiência, é importante comunicar os clientes para que tenham clareza da existência e do funcionamento desse serviço.

8. **Detalhamento das capacidades**

8.3.2 Ressarcimento em confiança – nível crítico

I. O QUE É?

O processo de ressarcimento em confiança (crédito em confiança) tem o objetivo de efetuar restituição imediata ao cliente nos casos de transação não reconhecida proveniente de uma ação de fraude. Caberá a cada instituição definir se implementará e sua estratégia para aplicação.

II.COMO FUNCIONA?

A partir do início das operações via Open Banking, os usuários poderão relatar o não reconhecimento de uma transação, iniciando um processo de contestação na instituição.

Em casos em que seja necessário reestabelecer imediatamente o saldo do cliente, poderá haver o lançamento de crédito em confiança na conta do usuário, enquanto a análise do caso está em andamento. Nessas situações, cada instituição deve estabelecer as premissas para a aplicação do crédito em confiança, assumindo os riscos da decisão .

É necessário observar que, nos casos em que seja necessário realizar a reversão do crédito em confiança, a conta deve possuir saldo suficiente.

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

O processo de ressarcimento em confiança viabiliza que as instituições regularizem a conta de um usuário de forma ágil e evitando maiores atritos. Além disso, ele minimiza possíveis ações judiciais, reclamações em mídias sociais e em órgãos regulados por usuários que foram vítimas de ações de fraudadores.

IV. EXPERIÊNCIA DO USUÁRIO

Na percepção do usuário, entender que a instituição possui uma forma ágil de resolver e devolver recursos traz maior confiança e colabora para que relacionamento se mantenha. É importante que o cliente tenha clareza dos processos internos do ressarcimento em confiança, quando aplicado.

8. **Detalhamento das capacidades**

8.4 Repressão

8.4.1 Colaboração para derrubada de *Phishing* entre os Participantes – nível alto

I. O QUE É?

Phishing é um termo originado do idioma inglês, relacionado a palavra fishing, que significa pescaria.
Tal termo ilustra de forma clara uma técnica empregada por meios digitais para coleta e obtenção de dados de pessoas físicas e jurídicas, inclusos senhas, credenciais e dados pessoais que possam permitir a criação de uma identidade ou credencial falsa.
A melhor identificação do Phishing pode ser feita a partir do aumento da capacidade das Participantes de monitorar, identificar e inutilizar os canais utilizados para a coleta e utilização indevida dos dados na aplicação de fraudes e lavagem de dinheiro ou financiamento ao terrorismo.

II.COMO FUNCIONA?

O objetivo da iniciativa é promover a cultura de monitoramento, pelas Participantes, de canais utilizados por fraudadores para esta coleta indevida de dados.
Os fraudadores normalmente se aproveitam de desconhecimento ou falso vínculo de confiança para obtenção desses dados.
Dessa forma, sugere-se a atuação em 3 frentes no combate e identificação do *Phishing:*

1. Monitoramento próprio: Cada Participante deve buscar monitorar sua própria marca e seus canais de comunicação, buscando identificar, de forma mais célere, eventuais canais usados para o Phishing, e manter canais de denúncias para reporte dessas situações ou suspeitas. Ainda, deve divulgar e participar de campanhas de orientação a clientes.

8. **Detalhamento das capacidades**

II.COMO FUNCIONA?

2. Monitoramento entre Participantes: As Participantes podem denunciar eventuais suspeitas de utilização da marca de outras Participantes em ações de *Phishing*, visto que, muitas vezes, os fraudadores utilizam-se de diversas marcas simultaneamente para maximizar seus resultados. Ainda, podem manter grupos de discussão ativos, com periodicidade razoável, para troca de melhores práticas no combate ao Phishing.

3. Monitoramento da marca Open Banking: contempla o monitoramento vinculado à marca Open Banking e compreende o alerta e reporte de situações suspeitas por todas as Participantes, somada à colaboração na averiguação e nas ações conjuntas e efetivas para identificação e derrubada de Phishing que envolvam o Open Banking.

A estruturação da colaboração para averiguação, constatação, identificação e derrubada de Phishing, pode ser feita por meio da utilização da ferramenta MISP (*Malware Information Sharing Platform*), já empregada no PIX, com criação, na ferramenta, de uma instância para colaboração na identificação e derrubada de Phishing envolvendo Open Banking.

Outra sugestão é a criação de uma nova categoria destinada ao Open Banking na ferramenta e no fluxo adotado para o PIX , a fim de reportar, receber e dar a devida tratativa, com acompanhamento do BCB.

8. **Detalhamento das capacidades**

III. MITIGAÇÃO DE RISCOS

A iniciativa mantém as Participantes atentas e reduz significativamente o risco de perdas financeiras, pois impacta diretamente na obtenção indevida de dados pelo fraudador, o que minimiza o potencial de aplicação de fraudes e protege os dados de clientes e a credibilidade do OBB.

IV. EXPERIÊNCIA DO USUÁRIO

A iniciativa não tem impacto negativo na experiência do cliente, mas tem um caráter preventivo, visando minimizar os meios disponíveis para obtenção indevida de dados por meio de *Phishing.*

9. **Prevenção à lavagem de dinheiro**

A implementação do OBB traz como premissa a não criação de nenhum novo arranjo de pagamento ou nova dinâmica de transferência de recursos entre instituições, com relação às atualmente existentes, o que mantém as transações do OBB sujeitas a responsabilidades já existentes de PLD/FT.

Dessa forma, é recomendado que, para as transações executadas via OBB, as Participantes, já reguladas pelo BCB, devem se manter aderentes aos requisitos e diretrizes definidos na legislação e regulamentação em vigor para PLD/FT. Essa regulamentação já fornece o respaldo mínimo necessário para uma atuação aderente das Participantes no OBB quanto à PLD/FT, conforme políticas, procedimentos, controles internos, avaliações internas de risco, registros e monitoramentos de operações suspeitas, comunicações ao COAF.

A Circular do Banco Central que apresenta tais requisitos e diretrizes é ilustrada nas sub seções abaixo.

9. **Prevenção à lavagem de dinheiro**

9.1 Políticas, Procedimentos e Controles Internos das Participantes

A Circular BCB nº 3.978, conforme em vigor, dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo BCB para assegurar a PLD/FT, levando em consideração o conceito da abordagem baseada em risco.

A política de PLD/FT, devidamente documentada e aprovada pelo Conselho de Administração ou pela Diretoria, conforme o caso, deve ser mantida atualizada e compatível com os perfis de risco dos clientes, das Participantes, das operações, dos produtos e serviços e dos empregados, parceiros e prestadores de serviços terceirizados, com o comprometimento da alta Administração da Participante com a efetividade e a melhoria contínua da política, dos procedimentos e dos controles internos relacionados com a PLD/FT. Esses são elementos essenciais para a mitigação de riscos aos quais as Participantes estão expostas.

9. **Prevenção à lavagem de dinheiro**

Essa política deve ser formulada com base em princípios e diretrizes de PLD/FT e conter, no mínimo:

i. a definição de papéis e responsabilidades para o cumprimento das obrigações de que trata a Circular BCB nº 3.978;
ii. a definição de procedimentos voltados à avaliação e à análise prévia de novos produtos e serviços, bem como da utilização de novas tecnologias;
iii. a avaliação interna de risco e a avaliação de efetividade;
iv. a verificação do cumprimento da política, dos procedimentos e dos controles internos de bem como a identificação e a correção das deficiências verificadas;
v. a promoção de cultura organizacional de prevenção à lavagem de dinheiro e ao financiamento do terrorismo, contemplando, inclusive, os funcionários, os parceiros e os prestadores de serviços terceirizados;
vi. a seleção e a contratação de empregados, parceiros e de prestadores de serviços terceirizados;
vii. a capacitação dos empregados sobre o tema da PLD/FT, incluindo os empregados dos correspondentes no País que prestem atendimento em nome das Participantes, sempre compatível com as atividades por ele exercidas;
viii. a coleta, verificação, validação e atualização de informações cadastrais, visando a conhecer os clientes, os funcionários, os parceiros e os prestadores de serviços terceirizados;
ix. o registro de operações e de serviços financeiros;
x. o monitoramento, seleção e análise de operações e situações suspeitas; e
xi. A comunicação de operações ao COAF

9. **Prevenção à lavagem de dinheiro**

As Participantes devem implementar uma estrutura de governança compatível com o porte, volume e complexidade das suas operações, com indicação de um diretor responsável pela PLD/FT, e instituir, ainda, mecanismos de acompanhamento e de controle de modo a assegurar a implementação e a adequação dessa política, dos procedimentos e dos controles internos adequados PLD/FT, de acordo com a legislação e regulamentação aplicáveis.

9. **Prevenção à lavagem de dinheiro**

9.2 Avaliação interna de risco (“AIR”)

As Participantes devem realizar AIR com adoção da abordagem baseada em risco; ou seja, com aplicação de medidas e controles proporcionais ao risco e a alocação de esforços de maneira mais eficiente. O objetivo é identificar e mensurar o risco de utilização de seus produtos e serviços nas práticas de lavagem de dinheiro e financiamento do terrorismo.

O risco deve ser avaliado quanto à sua probabilidade de ocorrência e à magnitude dos efeitos financeiro, jurídico, reputacional e socioambiental para as Participantes.

Essa AIR deve considerar, no mínimo, os perfis de risco de:

i. clientes;
ii. Participantes, inclusive o modelo de negócio e a área geográfica de atuação;
iii. operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias; e
iv. atividades exercidas pelos empregados, empregados de correspondentes, parceiros e prestadores de serviços terceirizados.

9. **Prevenção à lavagem de dinheiro**

Devem ser definidas categorias de risco e adotados os respectivos controles de gerenciamento e de mitigação, reforçados para as situações de maior risco e simplificados nas situações de menor risco.
Além disso, devem ser utilizadas, quando disponíveis, avaliações realizadas por entidades públicas do país relativas à PLD/FT, por exemplo, a Avaliação Setorial de Riscos e a Avaliação Nacional de Riscos.
A AIR deve ser formalizada e aprovada, com revisão periódica ou alterações significativas em perfis de risco pré-definidos, pelo diretor responsável pela PLD/FT, bem como encaminhada internamente para ciência de comitês de risco e de auditoria, conforme aplicável, e para o Conselho de Administração e/ou Diretoria das Participantes.

9. **Prevenção à lavagem de dinheiro**

9.3 KYC (know your customer)

As Participantes devem implementar procedimentos destinados a conhecer seus clientes, formalizados em manual específico aprovado e atualizado pela diretoria das Participantes, de acordo com a legislação e regulamentação vigentes.

Os procedimentos devem contemplar, inclusive:

i. Identificação dos clientes;
ii. Qualificação dos clientes, inclusive qualificação como PEP (Pessoa Exposta Politicamente); e
iii. Classificação dos clientes.

Os procedimentos de identificação devem permitir verificar e validar a identidade do cliente, incluir a obtenção, a verificação e a validação da autenticidade de informações de identificação, inclusive mediante confrontação de informações com aquelas disponíveis em bancos de dados e a manutenção de informações atualizadas.

A qualificação de clientes verifica-se por meio da coleta, verificação e validação de informações, inclusive a avaliação da capacidade financeira do cliente e verificação e validação de acordo com o perfil de risco do cliente e com a natureza da relação de negócio, além de coleta de informações adicionais compatíveis com o risco de utilização de produtos e serviços, a verificação da condição de PEP, de seu representante, familiar ou estreito colaborador.

Os procedimentos de qualificação devem ser compatíveis com o perfil de risco do cliente, contemplando medidas reforçadas para clientes classificados em categorias de maior risco, de acordo com a avaliação interna de risco referida e com a política de PLD/FT, e com a natureza da relação de negócio, bem como prever a análise da cadeia de participação societária até a identificação da pessoa natural caracterizada como seu beneficiário final, no caso de pessoa jurídica.

9. **Prevenção à lavagem de dinheiro**

I. Registro de Operações

As Participantes deve possuir infraestrutura e procedimentos adequados de forma a manter registro de todas as operações realizadas e produtos e serviços contratados, inclusive saques, depósitos, aportes, pagamentos, recebimentos e transferência de recursos, a fim de possibilitar a identificação da origem e o destino de recursos, seus remetentes e destinatários.

Os registros devem ser segmentados em:

i. Registro de operações de pagamento, recebimento e transferência de recursos independentemente do valor ou espécie de produto ou valor;
ii. Registro de operações em espécie: operações com utilização de recursos em espécie de valor individual superior a R$2.000,00 (dois mil reais) e operações de depósito ou aporte em espécie de valor individual igual ou superior a R$50.000,00 (cinquenta mil reais).

9. **Prevenção à lavagem de dinheiro**

9.4 Monitoramento, Seleção, Análise e Comunicação (MASC)

Participantes devem implementar procedimentos de monitoramento, seleção, análise e comunicação de operações e situações, conforme parâmetros, regras e cenários descritos em manual específico, aprovado pela Diretoria das Participantes, com o objetivo de identificar suspeitas de lavagem de dinheiro e do financiamento do terrorismo, compatíveis com políticas de PLD/FT e com as Avaliações Internas de Risco (AIR).

.

Os procedimentos devem contemplar:

i. Monitoramento e seleção de operações e situações suspeitas: as operações realizadas e os produtos e serviços contratados que considerem as partes envolvidas, os valores, as formas de realização, os instrumentos utilizados ou a falta de fundamento econômico ou legal e possam configurar indícios de lavagem de dinheiro ou de financiamento do terrorismo;
ii. Análise de operações e situações suspeitas selecionadas por meio dos procedimentos de monitoramento e seleção, com o objetivo de caracterizá-las ou não como suspeitas de lavagem de dinheiro ou financiamento do terrorismo.

Essa análise deve ser formalizada pelas Participantes em um dossiê, independentemente da comunicação ao COAF, com procedimentos prévios e de apoio na análise, inclusas consultas a bases de dados, serviços tecnológicos e de inteligência artificial, algoritmos, etc.

9. **Prevenção à lavagem de dinheiro**

9.5 Comunicação ao COAF

As Participantes devem comunicar ao COAF as operações ou situações suspeitas de lavagem de dinheiro e de financiamento do terrorismo, de acordo com a legislação e regulamentação aplicáveis, sem dar ciência aos envolvidos ou a terceiros (*tipping-off*).
Essas comunicações devem ser feitas de forma clara, consistente e detalhada, com razões fundamentadas para tanto, por meio do Sistema de Controle de Atividades Financeiras (SISCOAF), do COAF.

A tomada de decisão de comunicação não pode exceder o prazo de quarenta e cinco dias, contados a partir da data da seleção da operação ou situação e a comunicação deverá ser feita até o dia útil seguinte da decisão da comunicação (cf. art. 43, § 1° c/c art. 48, § 2° da Circular 3.978).

9. **Prevenção à lavagem de dinheiro**

9.6 Procedimentos destinados a conhecer empregados, parceiros e prestadores de serviços terceirizados (Know your Partner e Know your Supplier)

As Participantes devem implementar procedimentos destinados a conhecer seus empregados, parceiros e prestadores de serviços terceirizados, que prestem serviços de atendimento em seu nome, inclusive procedimentos e controles internos relacionados à PLD/FT.
Estes procedimentos devem contemplar a identificação e a qualificação dos empregados, parceiros de negócio e prestadores de serviço terceirizados. Além disso, devem prever a classificação das atividades por eles exercidas em categorias de risco definidas na AIR.

Os procedimentos devem ser compatíveis com a política de PLD/FT e com a avaliação interna de risco. As informações relativas aos empregados, parceiros e prestadores de serviços terceirizados devem ser mantidas atualizadas, considerando, inclusive, eventuais alterações que impliquem mudança de classificação nas categorias de risco.

9. **Prevenção à lavagem de dinheiro**

9.7 Acompanhamento e controle

As Participantes devem instituir mecanismos de acompanhamento e de controle de modo a assegurar a implementação e a adequação da política, dos procedimentos e dos controles internos relacionados à PLD/FT, submetidos a testes periódicos pela auditoria interna, quando aplicáveis, compatíveis com os procedimentos e controles internos das Participantes.

9. **Prevenção à lavagem de dinheiro**

9.8 Avaliação de efetividade

As Participantes devem avaliar anualmente a efetividade da política, dos procedimentos e dos controles internos relativos à PLD/FT, em relatório especial, inclusos, no mínimo:

i. procedimentos destinados a conhecer clientes (KYC), inclusive a verificação e a validação das informações dos clientes e a adequação dos dados cadastrais;
ii. procedimentos de monitoramento, seleção, análise e comunicação ao Coaf, incluindo a avaliação de efetividade dos parâmetros de seleção de operações e de situações suspeitas;
iii. governança da política de PLD/FT;
iv. medidas de desenvolvimento da cultura organizacional voltadas à prevenção da lavagem de dinheiro e ao financiamento do terrorismo;
v. programas de capacitação periódica de pessoal;
vi. procedimentos destinados a conhecer os funcionários, parceiros e prestadores de serviços terceirizados; e
vii. ações de regularização dos apontamentos oriundos da auditoria interna e da supervisão do BCB.

O relatório da avaliação de efetividade deve descrever a forma como foi realizada a avaliação efetiva, os testes aplicados e os resultados obtidos e deve servir de base para elaboração de um plano de ação destinado a solucionar as deficiências identificadas por meio da avaliação de efetividade, de modo a buscar o constante aperfeiçoamento das práticas relativas à PLD/FT.

OpenBanking

Guia de recomendações para participantes do Open Banking Brasil

Prevenção a Fraudes & PLD

Versão 4.0. 24.08.2021