ABIPAG

GUIA PRÁTICO PARA

Instituições de Pagamento na Segurança Financeira do Ecossistema

MAIO DE 2025

Introdução

A digitalização transformou os serviços financeiros e de pagamento, agregando ganhos expressivos de eficiência, inclusão e inovação. Essa evolução também se refletiu no aprimoramento dos mecanismos de gerenciamento dos mais diversos riscos, com o intuito de prevenir e combater golpes e fraudes, lavagem de dinheiro, financiamento do terrorismo e da proliferação de armas de destruição em massa e crimes cibernéticos – ampliando a proteção dos usuários e a confiança no ecossistema financeiro.

Com vistas a subsidiar instituições de pagamento no desempenho de suas atividades e contribuir com o fortalecimento do setor, a ABIPAG apresenta este guia com orientações práticas para uma defesa integrada, conectando três dimensões:

- Prevenção à Lavagem de Dinheiro e ao Combate ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (PLD/FTP)
- Combate a Golpes e Fraudes
- Segurança Cibernética

A sistematização reunindo essas dimensões de forma integrada não é apenas uma recomendação internacional: é uma necessidade estratégica para promover a confiança e a integridade nas instituições em prol de um mercado mais seguro para a sociedade brasileira.

Boa leitura!

Abipag – Associação Brasileira de Instituições de Pagamentos

Fale Conosco

www.abipag.com.br contato@abipag.com.br

Índice

1. Segurança do Ecossistema Financeiro

1.1. Por que adotar medidas para prevenir lavagem de dinheiro e combater financiamento do terrorismo e da proliferação de armas de destruição em massa (PLD/FTP)? 04

1.2. Por que estabelecer iniciativas de combate a golpes e fraudes? 06

1.3. Por que primar por mecanismos de segurança cibernética? 06

1.4. Por que instituir controles integrados de PLD/FTP, combate a golpes e fraudes e segurança cibernética? 08

2. Boas Práticas de Defesa Integrada

2.1. Como ataques cibernéticos podem desencadear golpes e fraudes e lavagem de dinheiro? 09

2.2. Como implementar modelos de defesa integrados de PLD/FTP, combate a golpes e fraudes e segurança cibernética? 09

2.3. Como desenvolver uma cultura organizacional orientada à defesa integrada? 10

2.4. Como fortalecer o ecossistema a partir de iniciativas de educação financeira? 11

2.5. Como a cooperação intersetorial contribui para a segurança do ecossistema financeiro e de pagamentos? 11

2.6. Quais são os recentes aprimoramentos da regulação financeira aplicável? 12

3. Referências 13

1. Segurança do Ecossistema Financeiro

1.1. Por que adotar medidas para prevenir lavagem de dinheiro e combater financiamento do terrorismo e da proliferação de armas de destruição em massa (PLD/FTP)?

Os controles para Prevenção a Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo e da Proliferação de Armas de Destruição em Massa (PLD/FTP) abrangem o conjunto de políticas, procedimentos e controles internos que têm como intuito evitar que as instituições sejam usadas para ocultar a origem ilícita de recursos ou financiar atividades terroristas, preservando a credibilidade e estabilidade do ecossistema financeiro e de pagamentos e gerando comunicações de operações suspeitas ao COAF.

Sua aplicação deve seguir a Abordagem Baseada em Risco (ABR), conforme exigido pela regulação do Banco Central do Brasil (BCB) e recomendado pelo *Financial Action Task Force* / Grupo de Ação Financeira Internacional (GAFI/FATF)[1]. Isso significa identificar, avaliar e mitigar os riscos de forma proporcional aos perfis de risco da instituição de pagamento (IP), de seus clientes, de suas operações, transações, produtos e serviços, e de funcionários, parceiros e prestadores de serviços terceirizados. Os elementos-chave da PLD/FTP incluem[2]:

- Política formal, documentada e aprovada pelo conselho de administração ou, se inexistente, pela diretoria da IP
- Avaliação interna de riscos considerando perfis de clientes, operações, transações, produtos e serviços, funcionários, parceiros e prestadores de serviços terceirizados da IP
- Procedimentos de identificação, qualificação e classificação de clientes *(Know Your Client* - KYC*)*, incluindo monitoramento contínuo de transações de pagamento
- Comunicação tempestiva e fundamentada de operações ou situações suspeitas ao Conselho de Controle de Atividades Financeiras (Coaf), o que ocorre por meio do Siscoaf por parte de IP autorizadas a funcionar pelo BCB
- Procedimentos de registro, monitoramento, seleção e análise de operações e situações suspeitas
- Procedimentos destinados a conhecer funcionários (*Know Your Employee* - KYE), parceiros (*Know Your Partner* - KYP) e prestadores de serviços terceirizados (*Know Your Supplier* – KYS)
- Avaliação prévia do risco de PLD/FTP em novos produtos, serviços e tecnologias utilizadas pela IP
- Envio e atualização de informações de relacionamento ao Cadastro de Clientes do Sistema Financeiro Nacional (CCS), bem como resposta tempestiva às consultas de detalhamento recebidas[3]

O CCS consiste em sistema gerido pelo BCB para registro de informações sobre os relacionamentos de pessoas físicas e jurídicas com instituições financeiras ou de pagamento autorizadas a funcionar pelo BCB. Ele indica em quais instituições o cliente possui ou manteve conta, investimento ou outro tipo de relacionamento, bem como as datas de início e, se aplicável, de término. No caso das IP, a obrigação de registro **aplica-se somente para emissoras de moeda eletrônica**, que mantêm contas de pagamento do tipo pré-paga de titularidade de seus clientes.

[1]Organização intergovernamental cujo propósito é desenvolver e promover políticas nacionais e internacionais de prevenção à lavagem de dinheiro e combate ao financiamento do terrorismo e da proliferação de armas de destruição em massa.
[2]Cf. Circular BCB nº 3.978/2020.
[3]Cf. Resolução BCB nº 179/2022.

Principais Obrigações de PLD/FTP

Obrigação	Prazo/Periodicidade
Avaliação Interna de Risco[4]	Revisão a cada 2 anos e em caso de alterações significativas nos perfis de risco
Elaboração do Relatório de Efetividade[5]	Anualmente, com data-base em 31 de dezembro
Encaminhamento do Relatório de Efetividade para ciência[6]	Até 31 de março do ano seguinte ao da data-base
Elaboração e envio do Plano de Ação e do respectivo relatório de acompanhamento (caso haja deficiências no relatório)[7]	Até 30 de junho do ano seguinte ao da data-base do relatório
Execução dos Procedimentos de Monitoramento, Seleção e Análise[8]	Para o monitoramento e seleção: até 45 dias da data da ocorrência da operação ou da situação Para a análise da operação ou situação selecionada: até 45 da data da seleção Prazo máximo total para decisão de comunicação: 90 dias
Comunicação ao Coaf de operações e situações suspeitas e de operações em espécie[9]	Até o dia útil seguinte ao da decisão de comunicação
Declaração de não comunicação ao Coaf em cada ano civil[10]	Até 10 dias úteis após o encerramento do ano
Armazenamento de informações coletadas em KYC, KYP, KYE, KYS e registros de operações[11]	Por, no mínimo, 10 anos, a partir do primeiro dia do ano seguinte ao fim da relação/realização da operação
Manter o contrato à disposição do BCB em caso de relação de negócio em arranjo de pagamento com terceiros não sujeitos à autorização do BCB[12]	Por, no mínimo, 5 anos após o encerramento da relação contratual
Dossiê com análise de operações e situações suspeitas[13]	Por, no mínimo, 10 anos
Armazenamento de versões anteriores de documentos (ex: Avaliação Interna, Relatório de Efetividade)[14]	Por, no mínimo, 5 anos
Armazenamento de manuais e documentos (ex.: KYC, Monitoramento)[15]	Por, no mínimo, 5 anos
Testes periódicos dos mecanismos de controle[16]	Atualização constante (sem prazo específico, mas deve haver periodicidade compatível com os controles internos)

[4]Art. 12, Circular BCB nº 3.978/2020.
[5]Art. 62, Circular BCB nº 3.978/2020.
[6]Art. 62, inciso II, Circular BCB nº 3.978/2020.
[7]Art. 65, Circular BCB nº 3.978/2020
[8]Art. 39, parágrafo único, e art. 43, §1º, Circular BCB nº 3.978/2020.
[9]Art. 48, §2º e art. 49, parágrafo único, Circular BCB nº 3.978/2020.
[10]Art. 54, Circular BCB nº 3.978/2020.
[11]Art. 67, incisos I, II e III, Circular BCB nº 3.978/2020.
[12]Art. 66, inciso V, Circular BCB nº 3.978/2020.
[13]Art. 67, inciso IV, Circular BCB nº 3.978/2020.
[14]Art. 66, inciso VIII e XII, Circular BCB nº 3.978/2020.
[15]Diversos, a exemplo do art. 13, §2º e art. 38, Circular BCB nº 3.978/2020.
[16]Art. 61, Circular BCB nº 3.978/2020.

1.2. Por que estabelecer iniciativas de combate a golpes e fraudes?

O combate a golpes e fraudes visa evitar perdas financeiras por atos de engano intencionais. Com pagamentos instantâneos, canais digitais e usuários com diferentes níveis de letramento, a abordagem precisa ser multidimensional e adaptativa. Estratégias eficazes de prevenção incluem:

Monitoramento e adaptação contínua
Acompanhar e responder rapidamente novas modalidades de golpes e fraudes que incidem sobre transações de pagamento

Ações educacionais
Destinadas a clientes e usuários sobre riscos e práticas seguras para realização de transações de pagamento

Compartilhamento de dados
Contribuir para a base de compartilhamento de dados e informações sobre indícios de golpes e fraudes entre instituições reguladas, conforme disciplina do BCB[17]

Suporte ao cliente
Incorporar a dimensão de prevenção a golpes e fraudes no atendimento a clientes, inclusive no componente de Ouvidoria instituído pela IP.

Fraude X Golpe: qual a diferença?

Fraude

Termo mais amplo e abrange qualquer ato ilegal ou enganoso que envolva a manipulação ou falsificação de informações, documentos ou sistemas com o objetivo de obter ganhos ilícitos ou prejudicar outra parte. Pode ocorrer de forma oculta, sem que a vítima perceba a manipulação de seus dados ou a irregularidade em um sistema

X

Golpe

Tipo de fraude que envolve a enganação direta da vítima, geralmente por meio de técnicas de manipulação e convencimento (engenharia social). O golpista incentiva a vítima a tomar uma ação prejudicial, como fornecer dados, clicar em *links* maliciosos ou fazer transferências de dinheiro, acreditando em uma falsa promessa ou situação

1.3. Por que primar por mecanismos de segurança cibernética?

A segurança cibernética tem como intuito proteger dados, sistemas e infraestruturas contra ameaças digitais, assegurando os pilares da segurança da informação. A regulação do BCB exige a IP adote uma política de segurança cibernética, que deve ser compatível com porte, risco, complexidade e modelo de negócios, a fim de assegurar[18]:

Confidencialidade
Acesso restrito a dados sensíveis

Integridade
Proteção contra alteração ou destruição indevida

Disponibilidade
Garantia de acesso contínuo aos ativos críticos

[17]Cf. Resolução Conjunta CMN/BCB nº 6/2023.
[18]Cf. Resolução BCB nº 85/2021.

As especificações mínimas da política de segurança cibernética incluem[19]:

1. Objetivos de segurança cibernética da IP
2. Procedimentos e controles adotados para reduzir a vulnerabilidade da IP a incidentes e atender aos demais objetivos de segurança cibernética
3. Registro, análise da causa e do impacto, bem como controle dos efeitos de incidentes relevantes para as atividades da IP
4. Diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios da IP
5. Iniciativas para compartilhamento de informações sobre os incidentes relevantes com as demais instituições autorizadas a funcionar pelo BCB
6. Mecanismos para disseminação da cultura de segurança cibernética na IP
7. Definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição; à classificação de dados e informações quanto à relevância; e à definição de parâmetros a serem utilizados na avaliação da relevância dos incidentes

Principais Obrigações de Segurança Cibernética

Obrigação[20]	Aprovação/Apresentacão	Responsável	Periodicidade
Formalização/implementação de Política de Segurança Cibernética (PSC)[21]	Conselho de Administração (ou Diretoria, se inexistente)	Diretor responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes	**Anual (mínimo)**
Manutenção de documentos que atendam às regras de contratação de serviços no exterior[22]	Não obrigatória		**Por evento**
Elaboração de relatório de implementação de plano de ação e resposta a incidentes[23]	Apresentado ao Conselho (ou Diretoria)		**Anual**
Manutenção de documentos que atendam às regras de prestadores de serviços relevantes[24]	Não obrigatória		**Por evento**

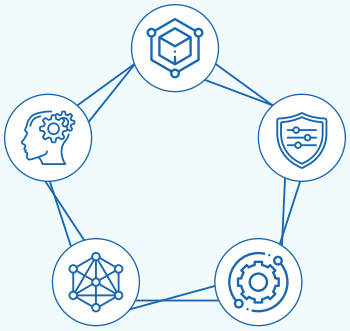
[19]Art. 3° da Resolução n° 85/2021.
[20]Vale notar que deve ser indicado no sistema Unicad o diretor responsável pela Política de Segurança Cibernética e pela execução do Plano de Ação e de Resposta a Incidentes, ambos sujeitos à aprovação do conselho de administração ou, na sua inexistência, da diretoria da IP (art. 9°, Resolução BCB n° 85/2021). Para mais informações: Guia Prático para Administradores de Instituições de Pagamento.
[21]Art. 2°, Resolução BCB n° 85/2021.
[22]Art. 6°, Resolução BCB n° 85/2021.
[23]Art. 8°, Resolução BCB n° 85/2021.
[24]Art. 12, Resolução BCB n° 85/2021.

1.4. Por que instituir controles integrados de PLD/FTP, combate a golpes e fraudes e segurança cibernética?

Estes três pilares se reforçam ou se enfraquecem mutuamente, de modo que a integração é estratégica em razão de:

Complementariedade
Cada pilar cobre uma faceta do risco (licitude da origem e da destinação dos recursos, legitimidade da transação, segurança do canal de acesso)

Dinamicidade
Ataques atuais são multifásicos e combinam técnicas das três áreas, exigindo uma resposta igualmente integrada



Profundidade
Controles integrados criam múltiplas barreiras, aumentando a chance de detectar ou prevenir atividades ilícitas

Interconectividade
Uma falha em um dos pilares (ex.: vazamento de dados por falha cibernética) cria vulnerabilidades em outros (ex.: fraude usando dados vazados, lavagem do dinheiro oriundo de fraude)

Eficiência
Operar de forma coordenada reduz redundâncias, melhora a eficácia dos controles e diminui os riscos legais, financeiros e reputacionais associados à fragmentação

2. Boas Práticas de Defesa Integrada

2.1. Como ataques cibernéticos podem desencadear golpes e fraudes e lavagem de dinheiro?

Ameaças ao ecossistema financeiro e de pagamentos raramente ocorrem de forma isolada. Ataques cibernéticos, golpes e fraudes e lavagem de dinheiro frequentemente operam em sequência ou de forma coordenada, explorando vulnerabilidades tecnológicas, humanas e processuais.

Incidentes cibernéticos são regularmente o ponto de partida para crimes financeiros. Ao comprometer sistemas ou capturar dados, criam a oportunidade para golpes e fraudes, e, consequentemente, para a lavagem dos recursos obtidos ilicitamente.

São exemplos de vetores comuns de exploração cibernética que levam a crimes financeiros:

A A invasão de sistemas para roubo de dados ou credenciais de acesso

B O comprometimento de contas corporativas para autorizar pagamentos fraudulentos

C Os vazamentos de dados explorando APIs inseguras, configurações inadequadas ou falhas de criptografia

D Os ataques de *phishing*, *smishing* (*SMS phishing*) e *malware* direcionados a clientes para obter ilicitamente senhas e informações pessoais

E Os golpes e fraudes internos em que funcionários abusam de acessos legítimos

! *Organismos internacionais como o GAFI e o Bank for International Settlements (BIS) reconhecem essa cadeia e recomendam tratar o ecossistema de ameaças de forma coordenada.*

2.2. Como implementar modelos de defesa integrados de PLD/FTP, combate a golpes e fraudes e segurança cibernética?

A natureza interligada das ameaças força a convergência dos mecanismos de defesa. Controles e processos antes vistos como exclusivos de cada área hoje compartilham dados, objetivos e ferramentas. Essa convergência é uma resposta necessária à complexidade dos riscos atuais. A título ilustrativo, são pontos de convergência:

- **Monitoramento transacional:** Plataformas que analisam transações de pagamento cada vez mais adotam abordagens complementares, em que procedimentos voltados à detecção de fraude e de indícios de lavagem operam de forma coordenada, ainda que distintos
- **Identidade digital:** Controles de identidade de usuários de serviços de pagamento que servem a propósitos das três dimensões como forma de controle de acesso
- **Compartilhamento de Dados Estruturados:** Troca de informações sobre incidentes (golpes, fraudes e ataques) entre equipes da mesma instituição
- **Arquitetura de Segurança Holística:** Proteção que abrange tanto a infraestrutura (ex.: servidores, redes) quanto os dados críticos (ex.: para fins de compliance e análise de riscos)

A estruturação da defesa evolui em níveis de maturidade e pode abranger diversos graus de integração. Isso significa dizer que a interdependência entre PLD/FTP, prevenção a golpes e fraudes e segurança cibernética exige cooperação operacional, interoperabilidade de sistemas, cultura alinhada e processos orientados aos

É possível terceirizar as atividades de segurança?

A IP deve manter o controle estratégico e decisório sobre PLD/FTP, prevenção à fraude e segurança cibernética, sendo possível, de modo geral, terceirizar aspectos operacionais, tais como serviços de apoio à análise, bem como procedimentos de monitoramento e seleção. Em alguns casos, a terceirização é vedada em norma[25].

Atenção!

Além das normas do BCB, as IP devem estar atentas, como subsídio para seus controles internos, a estudos e relatórios de riscos nacionais e internacionais como:

- Guia de Práticas de Supervisão do BCB[26]
- Avaliação Nacional de Riscos[27]
- Relatórios do GAFI[28]

E a listas internacionais de ameaças:

- Lista de países com alto risco conforme GAFI[29]
- Sanções da ONU[30]

As IP são obrigadas a consultar continuamente as listas de sanções da ONU[31]*. Se identificarem clientes ou operações relacionados a pessoas ou entidades sancionadas, devem bloquear imediatamente os ativos, sem aviso prévio ou necessidade de ordem judicial, e comunicar o fato às autoridades competentes. Além disso, devem manter controles internos para garantir o cumprimento dessas obrigações.*

2.3. Como desenvolver uma cultura organizacional orientada à defesa integrada?

A cultura é o que transforma políticas em prática diária. Uma cultura preventiva eficaz adotada por IP possui, por exemplo:

Comunicação clara
Políticas de PLD/FTP, combate a golpes e fraudes e cibersegurança divulgadas e adaptadas a cada função

Treinamento contínuo
Abordando engenharia social, *red flags*, proteção de dados e canais de denúncia

Simulados periódicos
Exercícios práticos de incidentes integrados

Tone at the Top
Ações concretas e visíveis que demonstrem o comprometimento da alta administração

Formação de equipes
Considerar segurança e integridade na contratação, avaliação e desligamento de colaboradores

[25]Exemplos de normas que dispõem sobre a terceirização de serviços relacionados à segurança do sistema de pagamentos: Resolução BCB nº 85/2021 (segurança cibernética); Resolução BCB nº 343/2023 (prestação de serviço de compartilhamento de dados e informações com indício de fraude); e Circular nº 3.978/2020 (PLD/CFT).
[26]Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/guias_PLD
[27]Disponível em: https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/avaliacao-nacional-de-riscos
[28]Disponível em: https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatf-recommendations.html
[29]Disponível em: https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html
[30]Disponível em: https://main.un.org/securitycouncil/en/sanctions/information
[31]Cf. Lei nº 13.810/2019, regulamentada pela Resolução BCB nº 44/2020

2.4. Como fortalecer o ecossistema a partir de iniciativas de educação financeira?

A tecnologia e os controles internos são fundamentais, mas a defesa contra crimes financeiros digitais também depende da conscientização de clientes. Criminosos focam no usuário buscando induzi-lo a fornecer dados confidenciais (ex.: senhas, códigos) ou a realizar ações prejudiciais (ex.: transferências, cliques em links maliciosos). Golpes e fraudes baseadas em engenharia social, que exploram a manipulação da vítima, representam a vasta maioria dos incidentes atuais.

Atenção!
O BCB estabeleceu a obrigatoriedade de IP adotarem medidas de educação financeira[32], sendo recomendável que incluam a prevenção a golpes e fraudes nessas medidas educacionais.

2.5. Como a cooperação intersetorial contribui para a segurança do ecossistema financeiro e de pagamentos?

A eficácia das medidas para garantia da integridade exige, além de forte cooperação público-privada, ampla colaboração intersetorial (ex.: telecomunicações, empresas de tecnologia). São exemplos de iniciativas:

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro (Enccla)[33]

Principal foro para a formulação de políticas públicas e soluções voltadas ao combate da corrupção e da lavagem de dinheiro. Em 2025, a Abipag contribuiu para encontro da Enccla ao apresentar aspectos relevantes do setor de pagamentos[34]

Aliança Nacional de Combate a Golpes e Fraudes Bancárias Digitais

Lançada em 2025 pelo Ministério de Justiça do Estado de São Paulo, a iniciativa ampliou a cooperação público-privada no combate aos golpes e fraudes em uma perspectiva multissetorial, mobilizando diversos setores, como o setor de pagamentos, bancário, de telefonia e de varejo. A Abipag integra a Aliança e contribui para seus grupos de trabalho, em linha com o seu comprometimento com o combate aos crimes financeiros

Política Nacional de Cibersegurança (PNCiber)[35]

Visa orientar a atividade de segurança cibernética no país. Para sua implementação, foi criado o **Comitê Nacional de Cibersegurança (CNCiber)**, um órgão colegiado multissetorial de caráter consultivo, responsável por acompanhar a implementação da PNCiber

[32]Cf. Resolução Conjunta CMN/BCB nº 8/2023
[33]Disponível em: https://www.gov.br/mj/pt-br/acesso-a-informacao/perguntas-frequentes/ativos_cooperacao/estrategia-nacional-de-combate-a-corrupcao-e-a-lavagem-de-dinheiro-enccla
[34]Ação nº 08/2025
[35]Cf. Decreto nº 11.856/2023

2.6. Quais são os recentes aprimoramentos da regulação financeira aplicável?

A regulamentação do BCB tem recepcionado as novas dinâmicas do mercado, aprimorando a disciplina de PLD/FTP, combate a golpes e fraudes e cibersegurança. Destaques dessa evolução incluem:

Compartilhamento de Dados de Indícios de Fraude: o BCB estabeleceu a obrigatoriedade do compartilhamento de dados sobre indícios de fraude, e detalhou medidas para sua execução, criando um ecossistema de troca de informações para fortalecer a prevenção a ilícitos[36]

Segurança desde a Concepção: A disciplina do BCB[37] enfatiza enfatizam a avaliação de riscos cibernéticos e a implementação de controles desde a concepção de produtos e serviços (Segurança por Concepção – *Security by Design*)

Segurança no Open Finance: O ecossistema do Open Finance exige que os procedimentos e controles de autenticação e segurança adotados pelas instituições participantes sejam robustos e compatíveis com suas políticas de segurança cibernética[38]

Disciplina de *Banking-as-a-Service (BaaS)*: Com o intuito de regulamentar a prestação de serviços de BaaS, em que entidade não autorizada pelo BCB toma serviços de instituição autorizada, o BCB publicou consulta pública com proposta de norma direcionada a conferir maior transparência e segurança para usuários do ecossistema financeiro e de pagamentos – com especial ênfase no aprimoramento de controles associados a PLD/FTP[40].

Gestão Integrada de Riscos: Regulamentações específicas, como aquelas referentes aos arranjos de pagamento, apontam para a necessidade de uma visão abrangente[39], considerando as interconexões entre riscos operacionais, como aqueles relacionados a PLD/FTP, a segurança da informação e a prevenção a golpes e fraudes

Medidas de Segurança no Pix

Atualizações no regulamento do arranjo de pagamento Pix[41] demonstram a adaptação regulatória contínua para mitigar riscos emergentes, especialmente golpes e fraudes que exploram a instantaneidade das transações. Nesse sentido, IP participantes desse arranjo devem observar requisitos como:

- **A** *Implementação do Mecanismo Especial de Devolução (MED)[42]*
- **B** *Criação de limites noturnos[43]*
- **C** *Definição de soluções de gerenciamento de risco de fraude que contemplem as informações de segurança armazenadas no BCB e que seja capaz de identificar transações Pix atípicas ou não compatíveis com o perfil do cliente[44]*
- **D** *Verificação do status do CPF/CNPJ na Receita Federal e descadastrar chaves Pix associadas a dados irregulares[45]*

[36]Cf. Resolução Conjunta CMN/BCB nº 6/2023 e Resolução BCB nº 343/2023
[37]Cf. Resolução BCB nº 85/2021
[38]Cf. Resolução Conjunta CMN/BCB nº 1/2020
[39]Cf. Resolução BCB nº 150/2021
[40]Edital de Consulta Pública nº 108 e 115. Disponível em: https://www3.bcb.gov.br/audpub/DetalharAudienciaPage?5&audienciaId=701
[41]Cf. Resolução BCB nº 1/2020
[42]Cf. Resolução BCB nº 103/2021, que altera a Resolução BCB nº 1/2020
[43]Cf. Resolução BCB nº 142/2021
[44]Cf. Resolução BCB nº 403/2024, que altera a Resolução BCB nº 1/2020
[45]Cf. Resolução BCB nº 457/2025, que altera a Resolução BCB nº 1/2020

3. Referências

- **Lei nº 9. 613/1998:** *Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e dá outras providências.*

- **Decreto nº 11.856/2023:** *Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança.*

- **Resolução BCB nº 28/2020:** *Dispõe sobre a constituição e o funcionamento de componente organizacional de ouvidoria pelas instituições de pagamento, pelas administradoras de consórcio, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.*

- **Circular BCB nº 3.978/2020:** *Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016.*

- **Edital de Consulta Pública nº 108 e 115:** *Divulga consulta pública sobre proposta de resolução conjunta do Conselho Monetário Nacional e do Banco Central do Brasil que dispõe sobre a prestação de serviços de BaaS por parte das instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.*

- **Resolução Conjunta CMN/BCB nº 1/2020:** *Dispõe sobre a implementação do Open Finance.*

- **Resolução BCB nº 1/2020:** *Institui o arranjo de pagamentos Pix e aprova o seu Regulamento.*

- **Resolução BCB nº 65/2021:** *Dispõe sobre a política de conformidade (compliance) das administradoras de consórcio e das instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.*

- **Resolução BCB nº 85/2021:** *Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.*

- **Resolução BCB nº 96/2021:** *Dispõe sobre a abertura, a manutenção e o encerramento de contas de pagamento.*

- **Resolução BCB nº 142/2021:** *Dispõe sobre procedimentos e controles para prevenção de golpes e fraudes na prestação de serviços de pagamento a serem adotados pelas instituições financeiras, demais instituições autorizadas a funcionar pelo Banco Central do Brasil e instituições de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).*

- **Resolução BCB nº 150/2021:** *Dispõe sobre os arranjos de pagamento, aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamentos integrantes do Sistema de Pagamentos Brasileiro (SPB), estabelece os critérios segundo os quais os arranjos de pagamento não integrantes do SPB deverão passar a integrá-lo, e dá outras providências.*

- **Resolução BCB nº 155/2021:** *Dispõe sobre princípios e procedimentos a serem adotados no relacionamento com clientes e usuários de produtos e de serviços pelas administradoras de consórcio e pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.*

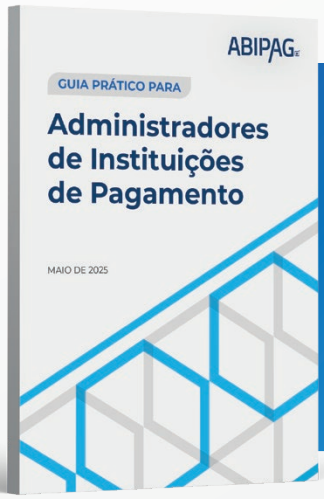
- **Resolução BCB nº 260/2022:** *Dispõe sobre os sistemas de controles internos das administradoras de consórcio e das instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.*

- **Resolução Conjunta CMN/BCB nº 6/2023:** *Dispõe sobre requisitos para compartilhamento de dados e informações sobre indícios de fraudes a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.*

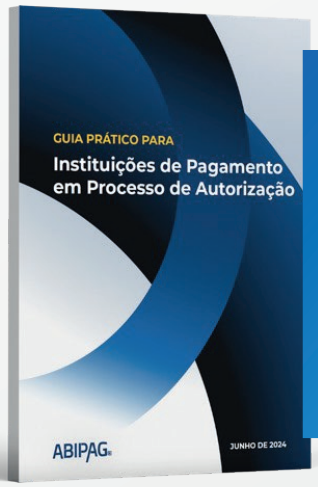
- **Resolução Conjunta CMN/BCB nº 8/2023:** *Dispõe sobre medidas de educação financeira a serem adotadas por instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.*

- **Resolução BCB nº 343/2023:** *Dispõe sobre as medidas necessárias à execução do compartilhamento de dados e informações sobre indícios de fraudes de que trata a Resolução Conjunta CMN/BCB nº 6, de 23 de maio de 2023.*

Conheça nossos Guias Práticos



Escaneie o QR CODE ou acesse aqui



Escaneie o QR CODE ou acesse aqui

Escaneie o QR CODE ou acesse aqui

ABIPAG

Projeto gráfico: Aurora Nexus Marketing