

**Fórum PIX**

**03.10.2023**

**GE SEG – 13º Ciclo**

**2023**

# GE de Segurança I Motivadores, participantes e metodologia

## Contexto

O GE SEG é um grupo de trabalho coordenado pelo Banco Central e secretariado pela FEBRABAN em que as associações abaixo participam colaborando com o debate.

## Objetivos

Apresentar os aspectos de segurança mapeados que necessitam alguma revisão e novos riscos identificados, com seus respectivos planos de ação.

## Ciclos de contribuições

Início das reuniões em junho de 2023



13º Ciclo – Apresentação no  
20º Fórum PI – set/23

## Participantes\*

- |            |                   |              |                       |
|------------|-------------------|--------------|-----------------------|
| 1. ABBC    | 7. ABRANET        | 13. BRASSCOM | 19. PSTI ABBC         |
| 2. ABBI    | 8. ACI WORLD WIDE | 14. CLARO    | 20. PSTI C&M SOFTWARE |
| 3. ABECS   | 9. ACREFI         | 15. CONECTA  | 21. PSTI JD           |
| 4. ABIPAG  | 10. AGEV          | 16. FEBRABAN | 22. RTM               |
| 5. ABO2O   | 11. AMPEF         | 17. Nuclea   | 23. TESOURO NACIONAL  |
| 6. ABRACAM | 12. B3            | 18. PAGOS    | 24. ZETTA             |

\* Participantes aprovados pelo Banco Central

# Pauta

**GE SEG – 13º ciclo**

**abril à setembro/23**

1. Cadastro obrigatório de dispositivo para iniciação de transação Pix e para gerenciamento de chaves
2. Ajustes no Regulamento do Pix para atribuir responsabilidades objetivas aos participantes em casos de fraude
3. Criação de fluxo de desmarcação de chave Pix
4. Estudo sobre o bloqueio cautelar e temporizador

## Escopo



Cadastro obrigatório de dispositivo para iniciação de transação Pix e para gerenciamento de chaves

## Proposta de trabalho



Analisar a proposta do BC sobre inserção no Manual de Segurança do Pix para obrigação do cadastro prévio do dispositivo junto ao detentor de conta para a inicialização transacional de valores PIX e ações no DICT relacionadas a chaves Pix (registro, exclusão, portabilidade, reivindicação de posse e alteração). Avaliando aspectos de segurança, benefícios e custos dessa possível obrigatoriedade.

## Avaliação GESEG



Proposta acatada pelas associações por unanimidade.

# PROPOSTA – Subgrupo 1

## Cadastro obrigatório de dispositivo para iniciação de transação Pix e para gerenciamento de chaves



Proposta foi estruturada em:

FUNDAMENTAÇÃO

### Introdução

Análise e Resumo do Avanço das Tecnologias e do 'Real-Time Gross Settlement' (RTGS), um termo que descreve um sistema de liquidação bruta em tempo real, examinando como outros países o implementaram ou estão implementando sistemas semelhantes para processamento de pagamentos em tempo real.

### Pesquisa Exploratória

O objetivo foi identificar os principais desafios e oportunidades relacionados ao cadastramento de dispositivos, bem como gerar informações para embasar a proposta. Algumas instituições já aplicam cadastro para análise antifraude e tokenização (MFA) do acesso.

### Visão da conformidade do cadastramento de dispositivos e a legislação atual

Ao analisar as normas (a Instrução Normativa n. 6/2020, a Resolução n. 4893/21 e a LGPD) do BC, e a LGPD, juntamente com as orientações da ANPD, nota-se a necessidade de harmonizar as convergências e as divergências das autoridades para orientações precisas e padronização do mercado quanto a transações financeiras e controle de chaves.

### Sobre o Cadastro obrigatório de dispositivo para iniciação de transação Pix para gerenciamento de chaves

É de entendimento do Subgrupo que esse procedimento deve constar no Manual de Segurança do PIX, bem como os métodos obrigatórios que indicamos no tópico de “Regras propostas ao modelo” descritos na proposta.

- **Benefícios:** Segurança aprimorada; Controle do cliente; Simplificação do processo de autenticação.
- **Desafios:** Usabilidade e experiência do usuário; Suporte a dispositivos múltiplos; Gerenciamento de dispositivos perdidos ou substituídos; Necessidade de atualizações e manutenção contínua; Possíveis limitações de adoção.
- **Custos:** A obrigatoriedade de cadastramento de dispositivos pode incorrer em custos de desenvolvimento ou aquisição de alguma solução de mercado, além de exigir a estrita observância das leis e normativos vigentes que permeiam o assunto.



# PROPOSTA – Subgrupo 1

## Detalhamento do registro

O objetivo foi adicionar às definições de segurança a necessidade de estabelecer uma relação de confiança entre o cliente que opta pelo PIX e o dispositivo (desktop/móvel). Isso se aplica a:

- Empresas que possuem: contrato Corporate, que utilizam hardware criptográfico para autenticação de clientes e que utilizam de autenticação suplementares em soluções Web
- Usuários PJ ou PF que ainda não são clientes das Instituições e usuários que já possuem relação com a Instituição (correntistas)
- Cadastramento de chaves de favorecido

Destacados pontos de atenção: no processo de integração (*onboarding*), confiabilidade do dispositivo, verificação do número de telefone ou e-mail, métodos de autenticação do dispositivo, alterações de processos internos.

## Exclusão

A regra para a exclusão de um dispositivo de acesso pode variar dependendo da instituição ou do participante do SPI. É importante permitir a autoexclusão de um dispositivo cadastrado e associado ao cliente. Recomenda-se que as informações de cadastro de dispositivos devem ser retidas por no mínimo 1 ano após a solicitação de exclusão. O Grupo considera importante registrar os motivos da exclusão de dispositivos de um cliente, uma vez que essa informação seria incorporada ao histórico do cliente e poderia ajudar a identificar quaisquer padrões que possam auxiliar na prevenção de exclusões desnecessárias no futuro.

## Portabilidade, Reivindicação de posse e alteração

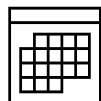
A opção de solicitação de portabilidade, reivindicação de posse ou alteração das chaves DICT associada a um cliente, somente poderá ser realizada por meio do dispositivo (telefone celular ou computador) que tenha sido previamente cadastrado e registrado pelo cliente junto à instituição. Em caso de indisponibilidade desses meios automáticos, a instituição deverá fornecer alternativas de atendimento que permitam a devida validação dos dados do cliente. Para os casos de portabilidade e reivindicação de posse feitas pelo atendimento da instituição é sugerido que o mesmo somente seja concluído após 24 horas do pedido. O cliente deverá obrigatoriamente ser informado sobre tal solicitação.

## Obrigatoriedade de uso da informação do dispositivo cadastrado

Por ter como premissa nesta proposta tornar o cadastramento de dispositivo obrigatório para o registro de chaves no PIX, indicamos que seu uso seja efetuado sempre que ocorrer qualquer transação em qualquer serviço PIX, bem como na modificação ou inclusão de beneficiários e chaves no DICT. O objetivo principal é assegurar a autenticação e identificação segura de nossos participantes, reduzindo os riscos de fraudes e preservando a integridade das contas.

## >>> Comentários gerais e trabalhos futuros

- ❖ Com a efetividade dos itens propostos neste trabalho, sugerimos como trabalho futuro proporcionar que a informação de cadastramento de dispositivo associado a chave DICT também seja disponibilizada no sistema Registrato do BCB. Isso tornaria uma importante fonte de informação ao cliente para verificar a autenticidade dos dispositivos em seu nome e prevenir fraudes.
- ❖ Definição da tecnologia de cadastro/gerenciamento de dispositivo por meio de um mecanismo antifraude, que possibilitaria utilizar o histórico do dispositivo e do próprio cliente (considerando, se possível, o histórico do dispositivo e do cliente em outras Instituições) nas avaliações estabelecidas pelas instituições.
- ❖ Definição de estratégia que permita o uso de informações reputacionais positivas anteriores (ausência de riscos).
- ❖ Definir controles para garantir limites de operação de valores para novos dispositivos cadastrados ou alterados dentro de um prazo de temporal
- ❖ Avaliar impactos e controles equivalentes necessários para iniciadores de pagamentos PIX dentro do OpenFinance
- ❖ Sugestão de habilitação de Geolocalização do dispositivo quando uma transação PIX for iniciada



### Prazo de implementação

➤ **6 à 8 meses** após a publicação do BC.

### **Escopo**



Ajustes no Regulamento do Pix para atribuir critérios objetivos aos participantes em casos de fraude

### **Proposta de trabalho**



Avaliar os ajustes no Regulamento do Pix propostos pelo BC e sugerir obrigações adicionais.

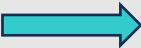
### **Avaliação GESEG**



Proposta acatada pela maioria das associações e com contrapontos de 1 associação.

Ajustes no Regulamento do Pix para atribuir critérios objetivos aos participantes em casos de fraude

| Redação atual                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Redação sugerida (BACEN)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Redação sugerida (Subgrupo)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Art. 41-D. As devoluções de que trata o inciso II do art. 41-C, quando decorrentes de fundada suspeita de fraude:</p> <p>Parágrafo único. Em caso de devolução em valor inferior ao da transação original, o participante deverá realizar múltiplos bloqueios ou devoluções parciais a partir da conta transacional do usuário recebedor, sempre que recursos sejam nela creditados, até que se alcance:</p> <p>I - o valor total da transação objeto da solicitação de devolução; ou II - noventa dias, contados a partir da transação original.</p> | <p>Art. 41-D. As devoluções de que trata o inciso II do art. 41-C, quando decorrentes de fundada suspeita de fraude:</p> <p>§ 1º Caso a conta do usuário com fundada suspeita de fraude não tenha sido encerrada, o participante deverá realizar múltiplos bloqueios ou devoluções parciais a partir da conta transacional do usuário recebedor, sempre que recursos sejam nela creditados, nas seguintes situações:</p> <p>I - solicitação de devolução rejeitada por ausência de fundos na conta; ou II - devolução em valor inferior ao da transação original.</p> <p>§ 2º Os múltiplos bloqueios ou devoluções parciais de que trata o § 1º devem ser realizados até que se alcance:</p> <p>I. – o valor total da transação objeto da solicitação de devolução; ou</p> <p>II. – noventa dias, contados a partir da transação original.</p> | <p>Art. 41-D. As devoluções de que trata o inciso II do art. 41-C, quando decorrentes de fundada suspeita de fraude:</p> <p>§ 1º O bloqueio de que trata o inciso II do ‘caput’ será mantido até a conclusão do procedimento de notificação de infração, observados os prazos previstos no Manual Operacional do DICT.</p> <p>§ 2º Caso a conta transacional do usuário recebedor da transação Pix com fundada suspeita de fraude não tenha sido encerrada, o participante deverá realizar múltiplos bloqueios ou devoluções parciais do valor correspondente ao saldo nela disponível, sempre que recursos forem nela creditados e:</p> <p>I – a solicitação de devolução tiver sido rejeitada por ausência de saldo na conta transacional; ou</p> <p>II - devolução em valor inferior ao da transação original.</p> <p>§ 3º Os múltiplos bloqueios ou devoluções parciais de que trata o § 1º devem ser realizados até que se alcance:</p> <p>I. – o valor total da transação objeto da solicitação de devolução; ou</p> <p>II. – noventa dias, contados a partir da transação original.</p> |



# PROPOSTA – Subgrupo 2

| Redação atual                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Redação sugerida (BACEN)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Redação sugerida (Subgrupo)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Seção II</p> <p>Do Gerenciamento do Risco de Fraude</p> <p>Art. 89. Adicionalmente ao gerenciamento de risco operacional disposto na Seção I deste Capítulo, os participantes do Pix devem adotar mecanismos robustos para garantir a segurança:</p> <p>I. - do processo de autenticação de usuários pagadores e de identificação de usuários recebedores;</p> <p>II. - dos procedimentos de iniciação do Pix; e</p> <p>III. - do processo de abertura de contas transacionais.</p> | <p>Seção II</p> <p>Do Gerenciamento do Risco de Fraude</p> <p>Art. 89. Adicionalmente ao gerenciamento de risco operacional disposto na Seção I deste Capítulo, os participantes do Pix devem adotar mecanismos robustos para garantir a segurança:</p> <p>IV - da entrada e da saída de recursos nas contas transacionais por meio de transações Pix.</p> <p>§ 1º Os participantes devem adotar, no mínimo, os seguintes mecanismos para garantir a segurança da entrada e da saída de recursos nas contas transacionais por meio de transações Pix:</p> <p>I - utilizar solução de gerenciamento de risco de fraude que contemple as informações de segurança armazenadas no DICT e que seja capaz de identificar transações atípicas ou não compatíveis com o perfil do cliente para:</p> <p>II. não permitir o uso de contas mantidas por usuários identificados como fraudadores, incluindo terceiros que recebam recursos oriundos de fraudes; e</p> <p>III. - disponibilizar para todos os seus clientes, no aplicativo no qual uma transação Pix pode ser iniciada, informações sobre os cuidados que os clientes devem ter para evitar fraudes.</p> <p>§ 2º Os participantes devem manter base de dados que contenha informações de segurança de seus clientes, atualizadas pelo menos uma vez a cada seis meses por meio de consulta às informações de segurança armazenadas no DICT.</p> <p>§ 4º A identificação de usuários fraudadores de que trata o § 1º, inciso II, deve ser feita com base nas informações de segurança armazenadas no DICT, devendo o participante considerar a existência de pelo menos uma marcação de fraude contra o usuário.</p> | <p>Seção II</p> <p>Do Gerenciamento do Risco de Fraude</p> <p>Art. 89. Adicionalmente ao gerenciamento de risco operacional disposto na Seção I deste Capítulo, os participantes do Pix devem adotar mecanismos robustos para garantir a segurança:</p> <p>IV - da entrada e da saída de recursos nas contas transacionais por meio de transações Pix.</p> <p>I - utilizar solução de gerenciamento de risco de fraude que contemple ao menos as informações de segurança armazenadas no DICT e que seja capaz de identificar <b>transações Pix</b> atípicas ou não compatíveis com o perfil do cliente para:</p> <p>II. não permitir o uso de contas mantidas por usuários identificados como fraudadores, incluindo terceiros que recebam recursos oriundos de fraudes; e</p> <p>III. <b>disponibilizar, em canal eletrônico de acesso amplo dos clientes nos quais uma transação Pix pode ser iniciada, informações sobre os cuidados que os clientes devem ter para evitar fraudes.</b></p> <p>§ 2º Os participantes devem manter base de dados que contenha informações de segurança de seus clientes, atualizadas pelo menos uma vez a <b>cada 6 (seis) meses</b> por meio de consulta às informações de segurança armazenadas no DICT.</p> <p>§ 4º A identificação de usuários fraudadores de que trata o § 1º, inciso II, deve ser feita com base nas informações de segurança armazenadas no DICT, devendo o participante considerar a <b>existência de marcações de fraude</b> contra o usuário.</p> |



## Prazo de implementação

➤ 3 meses para adequação após a publicação do BC.

### Escopo



Criação de fluxo de desmarcação de chave Pix

### Proposta de trabalho



Analisar a proposta do BC dos benefícios e riscos no compartilhamento com cidadãos e com empresas, por meio do Registrato, informações sobre chaves Pix e CPFs/CNPJs marcados e sugerir uma linha de ação para o BC; e a necessidade de existência de um fluxo, por meio do DICT, em que um usuário pudesse solicitar a desmarcação de uma chave Pix ou de um CPF/CNPJ.

### Avaliação GESEG



Proposta acatada pelas associações por unanimidade.

# PROPOSTA – Subgrupo 3

## Criação de fluxo de desmarcação de chave Pix

### POSICIONAMENTOS

- ❖ O grupo recomenda que as informações de marcações não sejam disponibilizadas no Registrato.
- ❖ O fluxo de pedido e aceitação de desmarcação deve permanecer sob responsabilidade de cada instituição, dada sua experiência e conhecimento no atendimento aos clientes. Nesse caso, o Registrato é responsável por direcionar o cliente à instituição adequada.

### PRINCIPAIS PREMISSAS

- O Registrato deverá direcionar o cliente para a Central de Atendimento em casos de questionamento de marcação. Não haverá acionamento direto através do Registrato.
- Em caso de reclamação cada instituição define de acordo com a sua política a forma de comunicar e orientar o cliente sobre a fraude.
- Somente a instituição responsável pela chave poderá realizar a desmarcação.
- Em caso de reconsideração da marcação da chave, a instituição deve sensibilizar essa informação no DICT, garantindo assim que outras instituições tenham acesso à esse dado.
- O acesso ao registrado deve ter duplo fator de autenticação.
- Saneamento prévio da base histórica da DICT, excluindo marcações indevidas, garantindo melhor confiabilidade das informações de segurança.
- Manter o histórico das marcações excluídas.



# PROPOSTA – Subgrupo 3

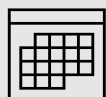
## PRINCIPAIS RISCOS

- Aumento exponencial de reclamações e procedências no BC: não dar procedência em caso de erro de marcação, conforme a porcentagem definida pela ANS. Além disso, as evidências e provas no âmbito interno dos bancos para confirmação de fraude/golpe não são adequadamente compreendidas nem consideradas válidas pelo Judiciário
- Aumento exponencial de ações jurídicas contra os bancos que realizaram as marcações de fraude
- Custo de operacionalização desde processo (aumento de capacity nas centrais, backoffice e etc.)
- Abrir precedente (único na história) de dar visibilidade de marcações de fraude para o mercado/usuários

## >>> COMENTÁRIOS GERAIS

As informações sobre as Chaves Pix registradas no CPF dos clientes já estão disponíveis no Registrato, porém entendemos vantajoso a exposição também dos dados relativos à segurança dessas chaves.

Importante salientar que o acesso do Registrato é feito através do login “gov.br”, o que já estabelece uma camada de segurança que garante a privacidade e autenticidade das consultas. Em outras palavras, o cliente só consegue acessar as informações apenas das chaves sob o seu CPF.



### Prazo de implementação

➤ **Mínimo de 6 meses** após a publicação do BC.

### **Escopo**



Estudos sobre o bloqueio cautelar e sobre temporizador

### **Proposta de trabalho**



Elaborar um diagnóstico sobre o funcionamento atual do bloqueio cautelar e do temporizador e criar proposta de melhoria nas funcionalidades

### **Avaliação GESEG**



Proposta acatada pelas associações por unanimidade.

# Subgrupo 4

## Estudo sobre Bloqueio Cautelar



**Proposta:** O Grupo analisou a Resolução nº 147 e sugeriu alterações, explicitando os impactos e benefícios, com o objetivo de reduzir o atrito dos clientes e o tempo para o bloqueio cautelar com a resposta do PSP pagador através de MED.

### Impactos

- **PSP Pagador:** criação de fluxo para receber e tratar os alertas do PSP recebedor que terão origem do bloqueio cautelar
- **DICT:** preparar base para intermediar os alertas que serão feitos entre PSP recebedor e PSP Pagador
- **PSP Recebedor:** criação de fluxo para alertar ao PSP pagador e receber resposta do alerta no fluxo de análise do bloqueio cautelar

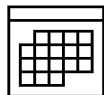
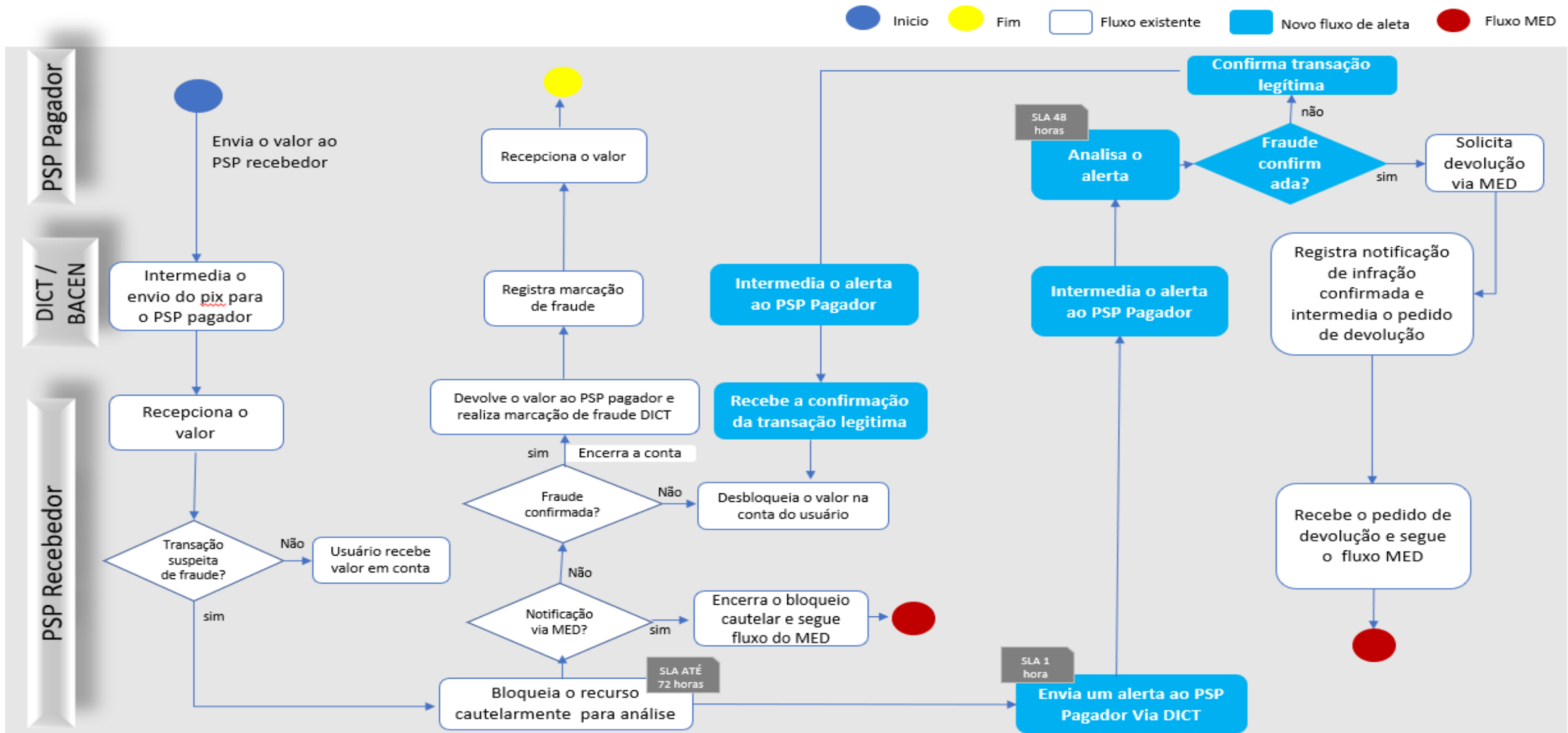
### Benefícios

- Aumento da assertividade na detecção da fraude, devido análise ser feita por ambas as partes;
- Eficiência no fluxo, possibilitando o aumento do alcance de contas analisadas e a maior retenção de recursos fraudulentos;
- Aumento no índice de recuperação de valores;
- Maior segurança no arranjo do PIX.

### Pontos de alteração:

- Criação de fluxo de alerta do bloqueio cautelar para análise do PSP pagador com o SLA de 1 hora para envio do alerta pelo PSP recebedor e 48 horas para análise e resposta do PSP Pagador.
- Abertura de solicitação de devolução via MED com abertura automática da notificação de infração
- Criação de solicitação de devolução com origem Bloqueio Cautelar
- Exclusão da funcionalidade de devolução proativa pelo cliente recebedor enquanto os recursos estão bloqueados – Artigo 39B 9.º

# Proposta de Fluxo de Bloqueio Cautelar



## Prazo de implementação

➤ 9 à 12 meses após a publicação do BC.

**GE SEG**

**Obrigada!**