12º Fórum Pix
GT SEG
Pagamentos Instantâneos

Apresentação da evolução dos trabalhos de segurança do PIX

BANCO CENTRAL DO BRASIL

GT de Segurança l Motivadores, participantes e metodologia

Contexto

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

Ciclos de contribuições

Início das reuniões em dezembro de 2019

- ✓ 1º Ciclo – Apresentado no 07º Fórum PI – Fevereiro/20
- ✓ 2º Ciclo – Apresentado no 08º Fórum PI – Abril/20
- ✓ 3º Ciclo – Apresentação no 09º Fórum PI – Junho/20
- ✓ 4º Ciclo – Apresentação no 10º Fórum PI – Agosto/20
- ✓ 5º Ciclo – Apresentação no 11º Fórum PI – Outubro/20
- ◌ 6º Ciclo – Apresentação no 12º Fórum Pix – Janeiro/21

Objetivos

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

Participantes*

1. ABBC
2. ABECS
3. ABIPAG
4. ABO2O
5. ABRACAM
6. ABRANET
7. AGEV
8. AMPEF
9. FEBRABAN
10. PAGOS
11. ZETTA
12. PSTI ABBC
13. PSTI C&M SOFTWARE
14. PSTI JD
15. SINDTELEBRASIL
16. TESOURO NACIONAL
17. B3
18. CIP
19. Claro
20. RTM

* Participantes aprovados pelo Banco Central

GT de Segurança

Contexto

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

Agenda

1. **Limites Transacionais**
2. **Aprimoramento do Fluxo de *"Takedown"***

GT de Segurança I Revisão dos Limites transacionais

Contexto

A dinâmica sobre limites transacionais do PIX se tornou bastante complexa ao combinarmos as variáveis de UX e segurança, principalmente focada nas questões de segurança pública em limites noturnos e transações via mobile.

Proposta: Limites transacionais PIX – Gestão de limites sob responsabilidade de cada PSP

Por que?

As Instituições Financeiras possuem os estudos dentro de seus motores de crédito, bem como, mantém o perfil e o histórico transacional de seus clientes

Como?

Através dos canais digitais, o cliente poderá solicitar **a redução do seu limite transacional** *(IN 40 e IN 43),* bem como, solicitar o **aumento do limite** transacional para PIX.

Nos horários úteis (6h às 20h) – os PSPs terão até uma hora para majoração dos limites, podendo incluir as validações adicionais de segurança, como por exemplo, envio de token via SMS ou e-mail para confirmação

Nos horários não úteis (20h às 6h) – a alteração do limite, será realizada a partir da próxima grade de **hora útil**, podendo também o PSP incluir validações adicionais de segurança

Já a redução do limite solicitada diretamente pelo cliente deverá ser atendida após a efetivação do pedido, podendo também o PSP incluir validações adicionais de segurança

Pontos de atenção e Motivadores:

- Atribuição de limites deve ser pensado como um **diferencial competitivo** entre os participantes.
- A exposição dos limites transacionais, conforme o novo Manual de Experiência do Usuário – estabelecendo o item “Meus Limites”, deixará a escolha nas mãos dos clientes, podendo este solicitar a Majoração ou a Redução de seus limites.
- Para transações de tickets maiores que o estabelecido pelos PSPs, o recomendável é utilizar processos adicionais de confirmação com o cliente.

GT de Segurança I Revisão dos Limites transacionais

Contexto

A dinâmica sobre limites transacionais do PIX se tornou bastante complexa ao combinarmos as variáveis de UX e segurança, principalmente focada nas questões de segurança pública em limites noturnos e transações via mobile.

Proposta: Limites transacionais PIX – Adequação das Datas Regulatórias

Por que?

As normativas IN40, IN43 e o Manual de Experiência 3.0 estabelecem datas para entregas das funcionalidades de limites diferentes, fazendo com que a entrega ao cliente final seja quebrada, podendo impactar a funcionalidade como um todo

IN 43 – 01/02/21

Obrigatoriedade na oferta da funcionalidade de personalização de limites

Manual de Experiência 3.0 – 31/03

Criação do espaço “Meus Limites” nos aplicativos das instituições

Como?

A junção das datas, visando a adequação de 100% dos aplicativos e dos principais canais de atendimentos dos participantes em **31/03**.

As instituições podem realizar **entregas evolutivas** antes dessa data, permitindo a adaptação caso necessário desde que respeitando a data acima.

Pontos de atenção:

- A proposta sobre a responsabilidade dos PSPs na determinação do limite também seguiria a data sugerida.
- Com essa flexibilização é possível que as casas **adequem as propostas de limite com o comportamento dos clientes**, evoluindo a funcionalidade da melhor forma até a data final.

GT de Segurança I Parte 2 – Limites transacionais – Tema de Segurança pública

Contexto

A dinâmica sobre limites transacionais do PIX se tornou bastante complexa ao combinarmos as variáveis de UX e segurança, principalmente focada nas questões de segurança pública em limites noturnos e transações via mobile.

Resumo da Proposta

1. **Flexibilização da norma** permitindo a **gestão de limites sob responsabilidade de cada PSP**, de acordo com o perfil de seus clientes *(Canais, horários, etc)*.

2. **Padronização** na alteração dos limites por parte do cliente:
   A. Majoração **dentro** do horário comercial realizada em até uma hora (6h às 20h);
   B. Majoração **fora** do horário comercial realizada em até uma hora da operação da próxima grade útil (20h às 6h);
   C. Redução realizada de forma imediata;
   D. Possiblidade de **oferta de limite para transações esporádicas**;
   E. Fica a cargo de cada instituição os **processos adicionais de segurança para a alteração de limites** *(token, dupla validação, etc);*

3. **Convergência das datas regulatórias** para **31/03**, permitindo a maturação das funcionalidades ofertadas pelos participantes e que as soluções desenvolvidas sejam construídas de forma eficiente e sem colocar em risco o funcionamento atual do Pix. *(Acatado para 01/04 – IN nº71)*

GT de Segurança | Aprimoramento do Fluxo de *Takedown*

Contexto

Vários domínios falsos são criados diariamente usando temas recorrentes para a atrair a atenção dos clientes com a intenção de obter suas credenciais para aplicar golpes e facilitar fraudes.

Os serviços de monitoramento da marca e ***takedown**** identificaram que houve um aumento de domínios falsos registrados com a marca Pix.

Ações de takedown visam remover conteúdo que, disponível na internet, viole direitos de terceiros

Objetivo

O objetivo é criar um processo automatizado e centralizado para que o Banco Central em conjunto com os PSPs possam receber, compartilhar e reforçar o pedido de *takedown*, e também compartilhar as informações fraudulentas com os participantes para que se ganhe força e conhecimento sobre os domínios falsos.

O pedido de *takedown* será de responsabilidade de cada participante.

Agenda *Takedown*

- MISP
- Arquitetura
- Fluxo

GT de Segurança | Aprimoramento do Fluxo de *Takedown*

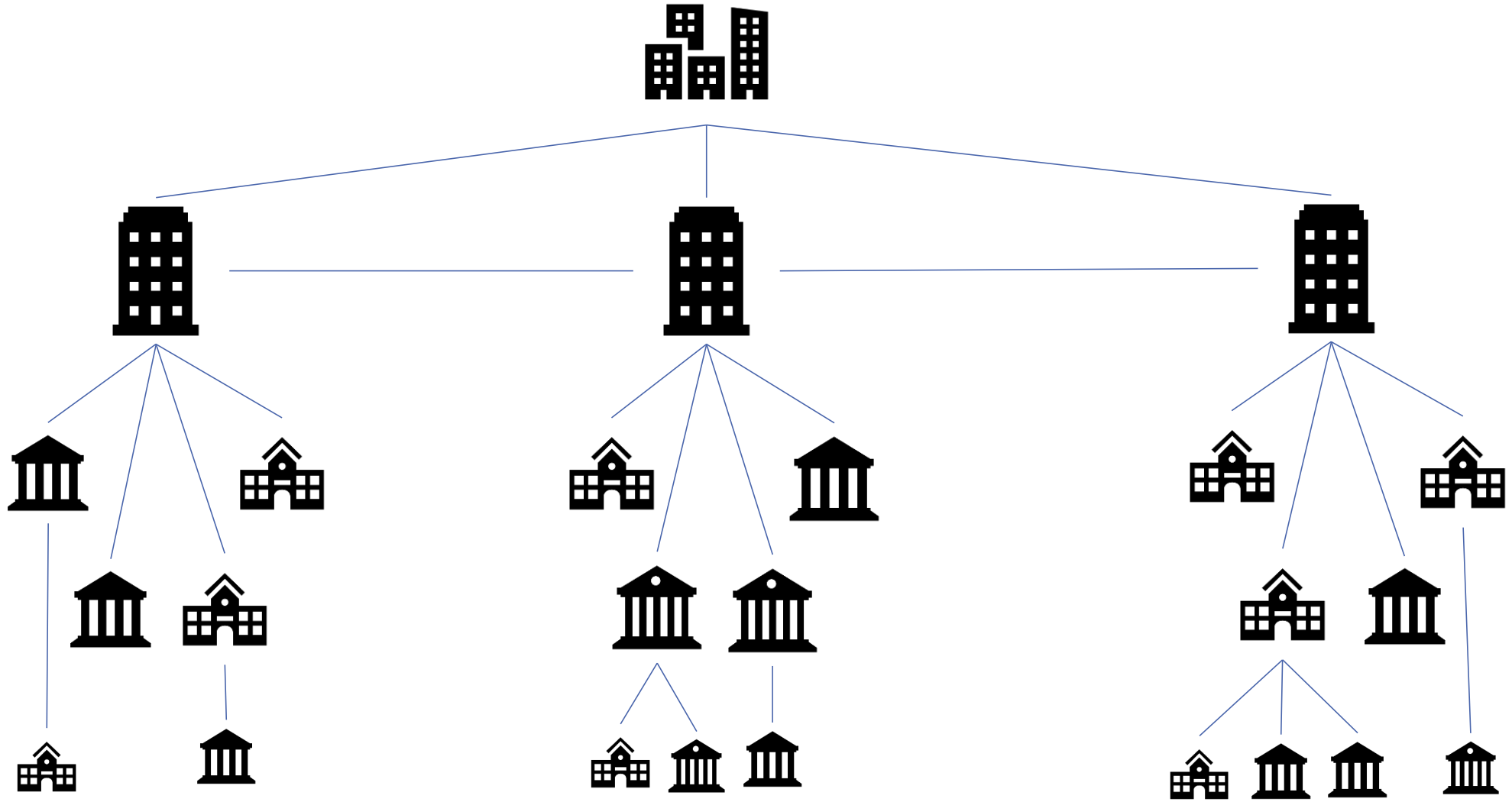
MISP, o que é?

MISP é uma plataforma de **inteligência de ameaças** para compartilhar, armazenar e correlacionar indicadores de comprometimento de ataques direcionados, inteligência de ameaças, informações de fraude financeira, informações de vulnerabilidade ou mesmo informações de contraterrorismo.

Benefícios

- **Automatizar o processo**, utilizando uma plataforma aberta, gratuita e amplamente utilizada pela comunidade internacional
- **Permite compartilhamento** de dados para a troca e sincronização automática com outras partes e grupos de confiança usando o MISP;
- Possui uma **interface de usuário intuitiva**, interface gráfica e funcionalidade de gráficos para criar e visualizar relacionamentos entre objetos e atributos;
- Uma **rede sustentável** para o compartilhamento contínuo de informações, agregando conhecimento e prevenindo as ameaças;
- É uma plataforma ***Open Source***

Arquitetura



- **BCB e Associações deverão conter as suas instâncias**;
- **PSP Direto** irá utilizar a instância da sua respectiva **associação**;

- BCB e Associações deverão integrar as suas instâncias;
- **PSP Indireto** irá integrar com o seu respectivo PSP Direto, integração será sob responsabilidade do PSP Direto

GT de Segurança | Aprimoramento do Fluxo de *Takedown*

Fluxos de *Takedown*

O Banco Central entende a importância deste tema e solicitou o detalhamento do processo de *takedown* proposto pelo GT Seg no Fórum anterior, bem como, a organização do processo de reforço para pedidos de *takedown*.
Temos 4 fluxos a estudar:

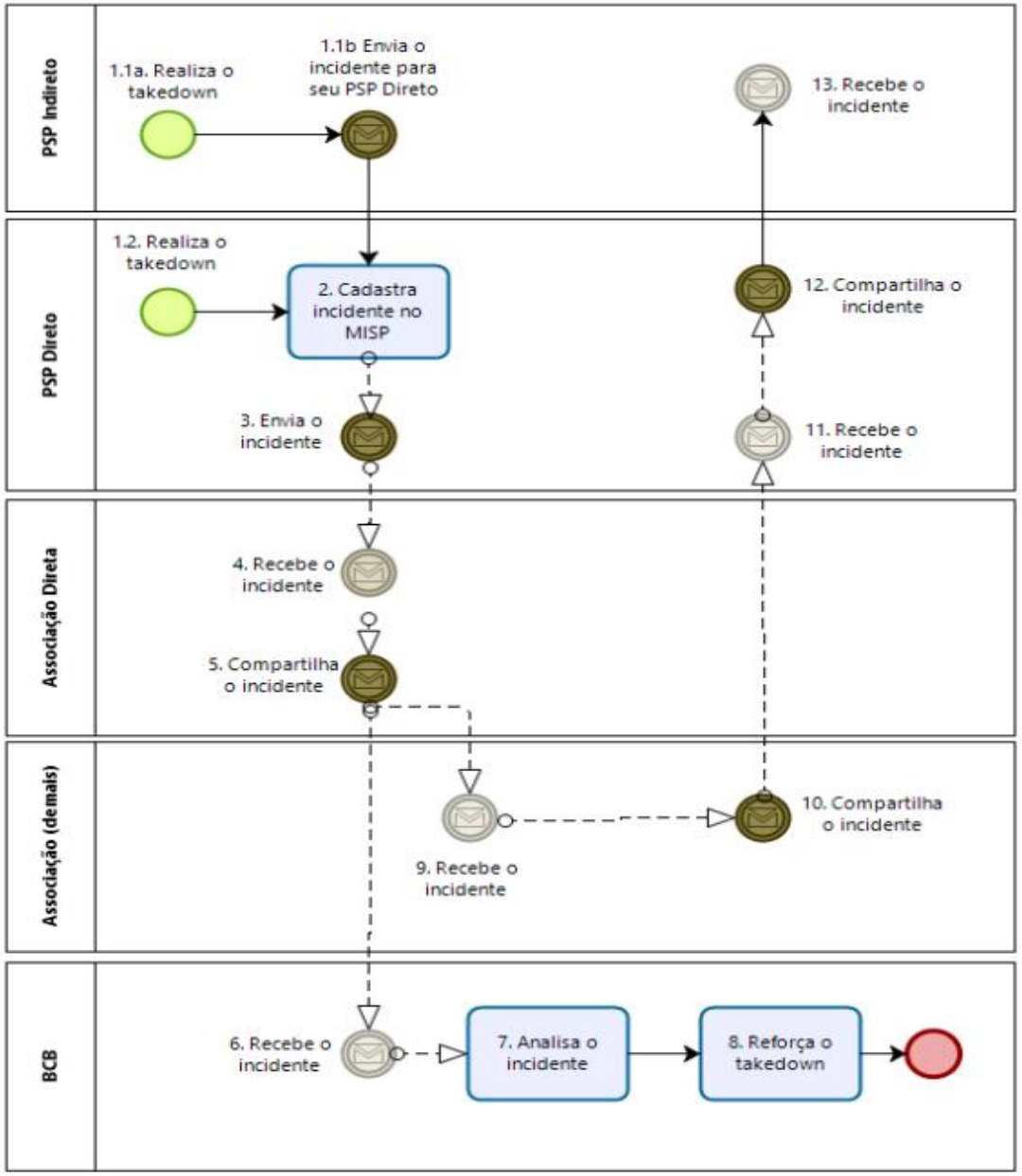
1. **Marca Pix + Instituição:** pedido de *takedown* pela própria instituição + solicitação de *takedown* pelo Banco Central

2. **Somente Marca Pix:** fluxo de envio de alerta ao Banco Central

3. ***Freezing* de pastas:** site legítimo + conjunto de pastas fraudulentas identificadas. Pedido de *freezing* de pastas + solicitação de reforço via Banco Central

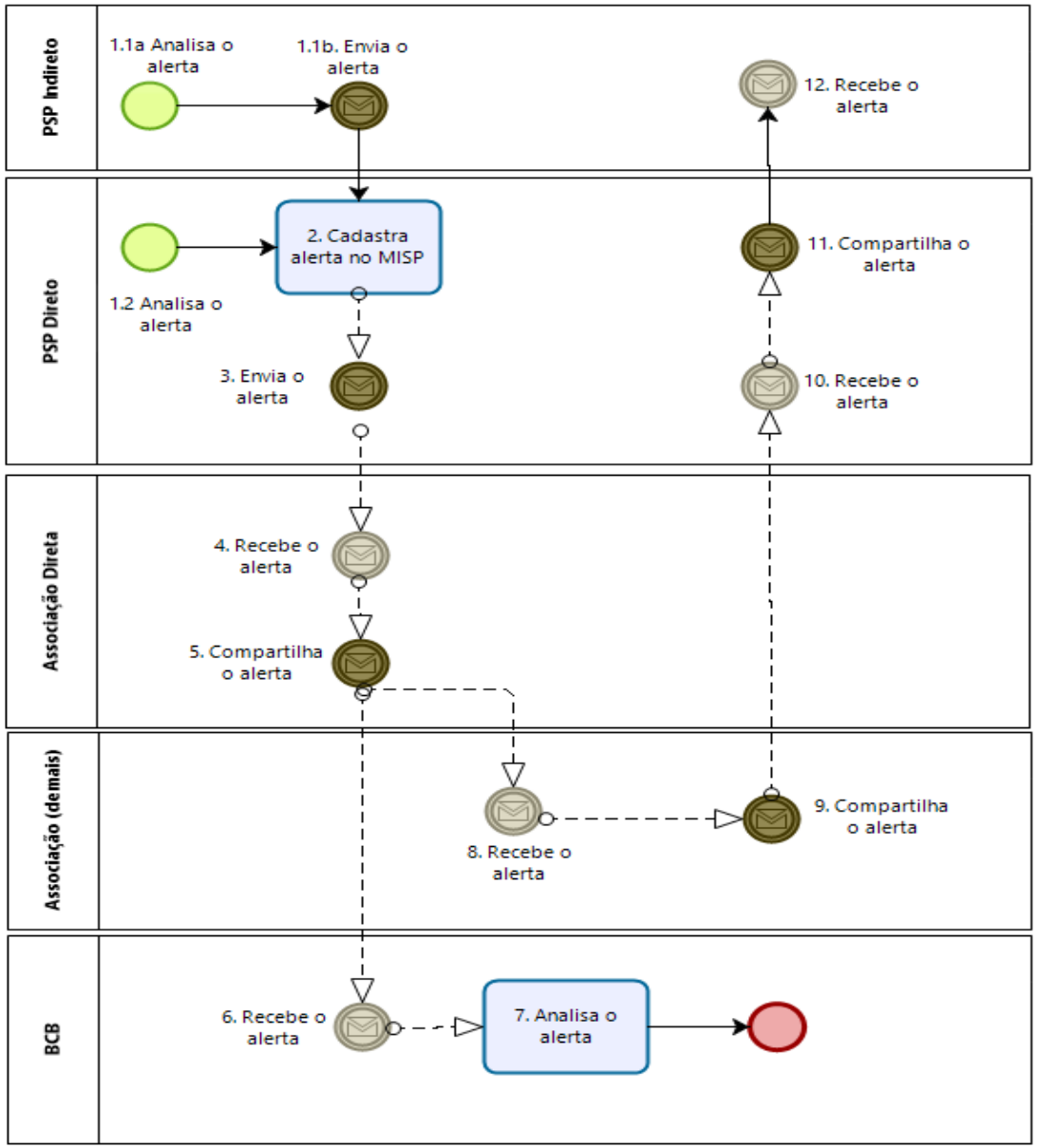
4. **Fluxo reverso:** Banco Central identifica sites suspeitos, envia formulário a Instituição Financeira solicitando análise.

Fluxo 1. Marca Pix + Instituição: pedido de *takedown* pela própria instituição + solicitação de *takedown* pelo Banco Central



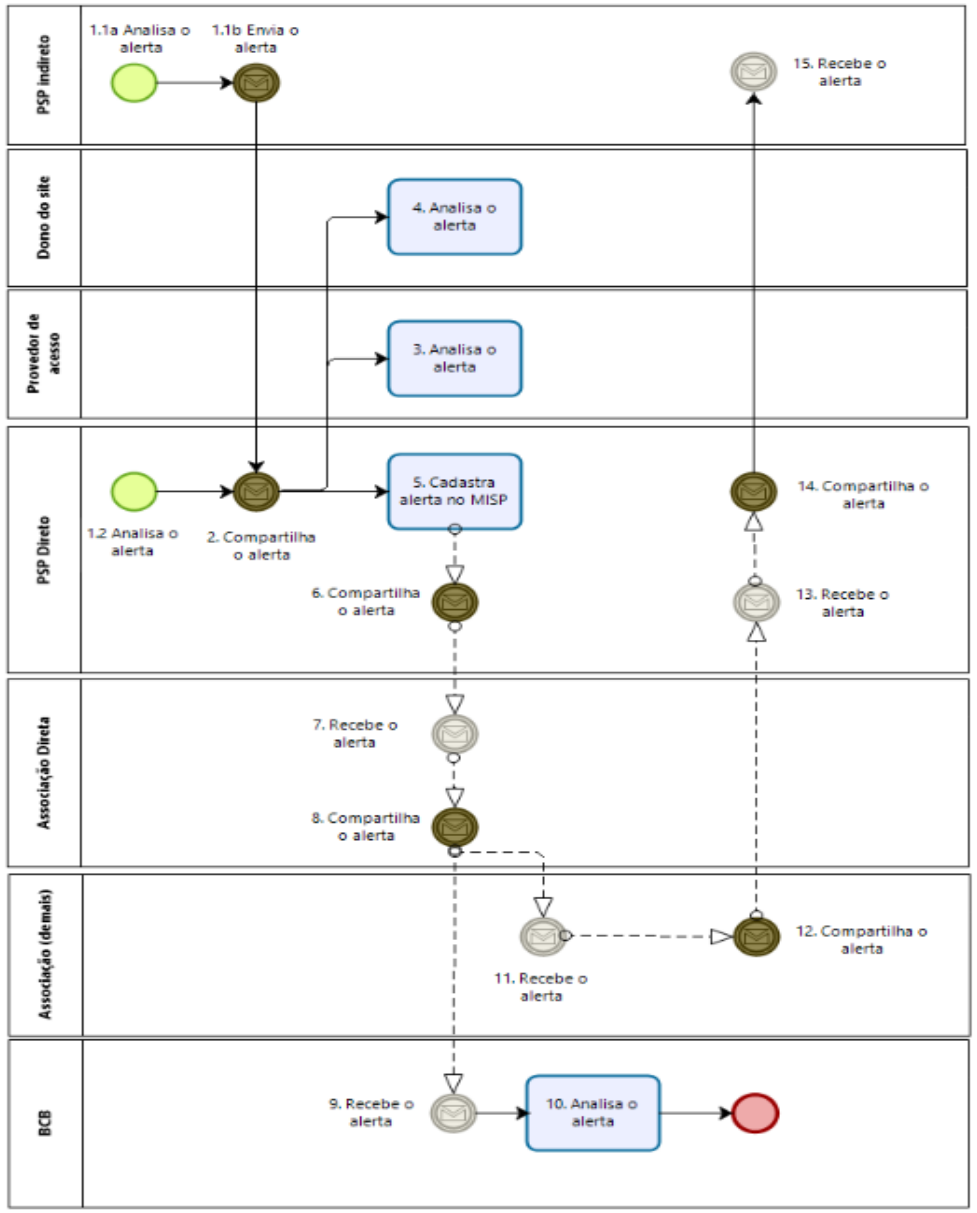
#	Camada	Tipo	Descrição
1.1a	PSP Indireto	Ação	Realiza o Takedown
1.1.b	PSP Indireto	Comunicação	Envia o incidente para o seu PSP Direto
1.2	PSP Direto	Ação	Realiza o Takedown
2	PSP Direto	Ação	PSP Direto cadastra o evento de incidente no MISP
3	PSP Direto	Comunicação	Envia o incidente para a sua associação
4	Associação	Comunicação	Associação do PSP Direto recebe o evento de incidente
5	Associação	Ação	Associação do PSP Direto compartilha o evento de incidente com o BCB e com as demais Associações
6	BCB	Comunicação	BCB recebe o incidente
7	BCB	Ação	BCB analisa o incidente
8	BCB	Ação	BCB reforça o takedown
9	Associações	Comunicação	Demais Associações recebem o incidente da Associação
10	Associações	Comunicação	Demais associações compartilham o evento de incidente com os seus PSP Diretos (opcional para compartilhar conhecimento)
11	PSPs Diretos	Comunicação	PSPs Diretos recebem da sua Associação o evento de incidente.
12	PSPs Diretos	Comunicação	PSPs Diretos compartilham o evento de incidente com os seus PSP Indiretos (opcional para compartilhar conhecimento)
13	PSPs Indiretos	Comunicação	PSPs Indiretos recebem o incidente dos seus PSPs Diretos.

Fluxo 2. Somente Marca Pix: Fluxo de envio de alerta ao Banco Central



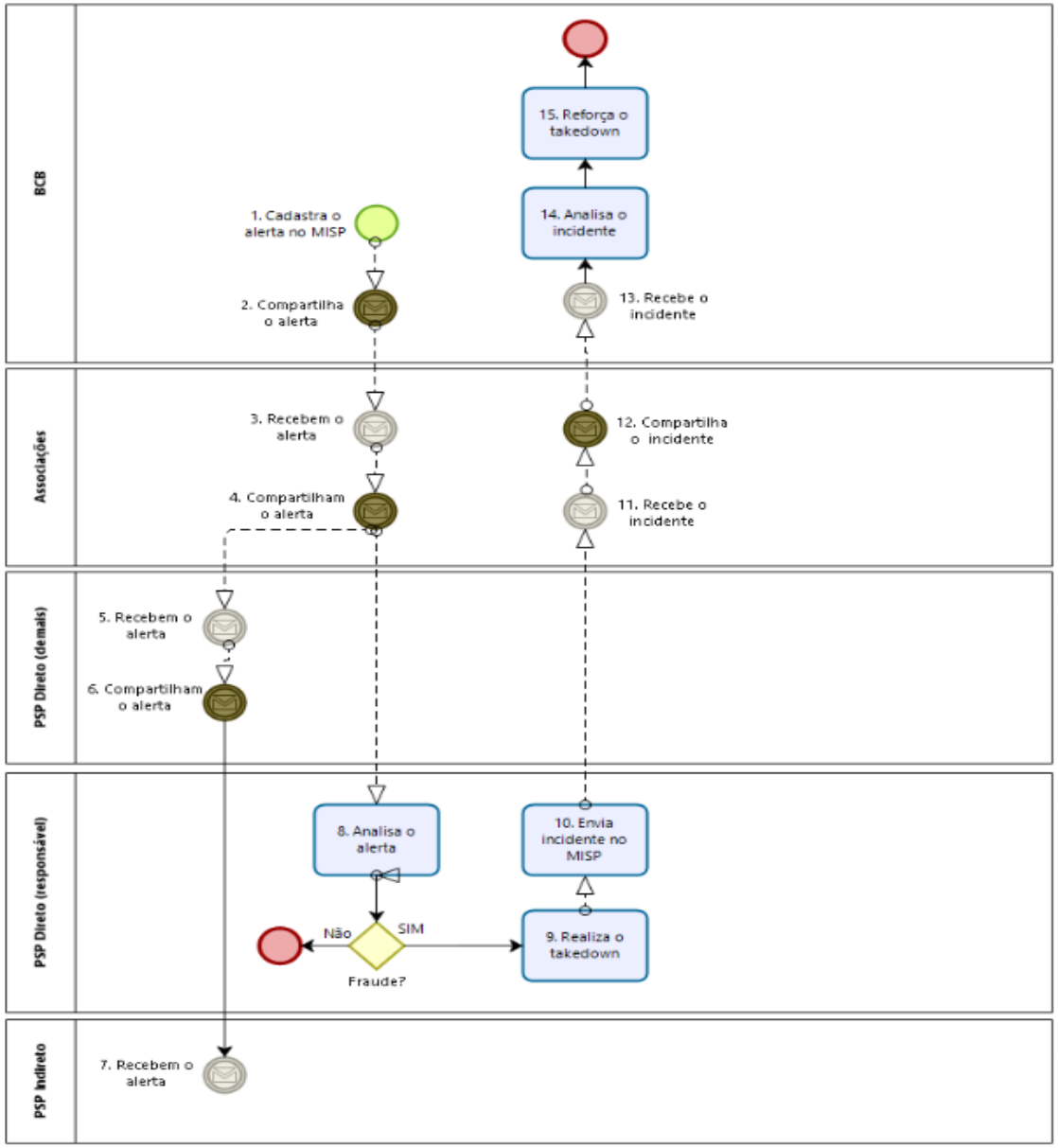
#	Camada	Tipo	Descrição
1.1a	PSP Indireto	Ação	Analisa o alerta
1.1.b	PSP Indireto	Comunicação	Envia o alerta para o seu PSP Direto
1.2	PSP Direto	Ação	Analisa o alerta
2	PSP Direto	Ação	PSP Direto cadastra o evento de alerta no MISP
3	PSP Direto	Comunicação	PSP Direto envia o evento de alerta para sua Associação
4	Associação	Comunicação	Associação recebe o evento
5	Associação	Ação	Associação compartilha o evento de alerta com BCB e demais Associações
6	BCB	Comunicação	BCB recebe o evento de alerta
7	BCB	Ação	BCB analisa o evento de alerta
8	Associações	Comunicação	Demais Associações recebem o evento de alerta da Associação
9	Associações	Comunicação	Demais associações compartilham o evento de alerta com seus PSP Diretos (opcional para compartilhar conhecimento)
10	PSPs Diretos	Comunicação	PSPs Diretos recebem o evento de alerta da sua Associação
11	PSPs Diretos	Comunicação	PSPs Diretos compartilham o evento de alerta com seus PSPs Indiretos (opcional para compartilhar conhecimento)
12	PSPs Indiretos	Comunicação	PSPs Indiretos recebem o alerta

Fluxo 3. *Freezing* de pastas: site legítimo + conjunto de pastas fraudulentas identificadas. Pedido de *freezing* de pastas + solicitação de reforço via Banco Central



#	Camada	Tipo	Descrição
1.1a	PSP Indireto	Ação	PSP Indireto analisa o alerta
1.1.b	PSP Indireto	Comunicação	PSP Indireto envia o alerta para o seu PSP Direto
1.2	PSP Direto	Ação	PSP Direto analisa o alerta
2	PSP Direto	Comunicação	PSP Direto compartilha o alerta com o provedor de acesso e o dono do site
3	Provedor de acesso	Ação	Provedor de acesso analisa o alerta
4	Dono do site	Ação	Dono do site analisa o alerta
5	PSP Direto	Ação	PSP Direto cadastra o evento de alerta no MISP
6	PSP Direto	Comunicação	PSP Direto envia o evento de alerta para sua Associação
7	Associação	Comunicação	Associação do PSP Direto recebe o evento de alerta
8	Associação	Ação	Associação compartilha o evento de alerta com o BCB e demais Associações
9	BCB	Comunicação	BCB recebe o evento de alerta
10	BCB	Ação	BCB analisa o evento de alerta
11	Associações	Comunicação	Demais associações recebem o evento de alerta
12	Associações	Comunicação	Demais associações compartilham o evento de alerta com seus PSP Diretos (opcional para compartilhar conhecimento)
13	PSPs Diretos	Comunicação	PSPs Diretos recebem o evento de alerta
14	PSPs Diretos	Comunicação	PSPs Diretos compartilham o evento de alerta com seus PSP Indiretos (opcional para compartilhar conhecimento)
15	PSPs Indiretos	Comunicação	PSPs Indiretos recebem o alerta

Fluxo 4. Fluxo reverso: Banco Central identifica sites suspeitos, envia formulário a Instituição Financeira solicitando análise.



#	Camada	Tipo	Descrição
1	BCB	Ação	BCB cadastra o evento de alerta no MISP
2	BCB	Comunicação	BCB compartilha o evento de alerta com todas as associações
3	Associações	Comunicação	Associações recebem o evento de alerta do BCB
4	Associações	Comunicação	Associações compartilham o evento de alerta com os seus PSP Diretos
5	PSPs Diretos	Comunicação	PSPs Diretos recebem o alerta da sua Associação
6	PSPs Diretos	Comunicação	PSPs Diretos compartillham o alerta com seus PSPs Indiretos
7	PSPs Indiretos	Comunicação	PSPs Indiretos recebem o alerta do seu PSP Direto
8	PSP Direto	Ação	PSP Direto responsável pelo alerta analisa o evento
9	PSP Direto	Ação	PSP Direto solicita o takedown
10	PSP Direto	Ação	PSP Direto devolve o evento como incidente para a sua Associação
11	Associação	Comunicação	Associação recebe o evento de incidente
12	Associação	Comunicação	Associação envia o evento de incidente ao BCB
13	BCB	Comunicação	BCB recebe o evento de incidente
14	BCB	Ação	BCB analisa o evento de incidente
15	BCB	Ação	BCB reforça o takedown

AGENDA – 7º Ciclo GT Seg *(fevereiro / abril)*

BANCO CENTRAL DO BRASIL

Reuniões GT SEG – Quinzenais[1] – Quintas período da manhã

Pauta para o próximo ciclo:

1 **Segunda Semana da Segurança Digital:** campanha coordenada, com participação de BC e participantes do Pix, de educação contra engenharia social.
Proposta: de 22/02 a 26/02

2 Desenho do **fluxo de comunicação** entre os participantes em casos de fraude envolvendo o Pix

3 Análise do **Mecanismo Especial de Devolução Pix**.

[1]Havendo necessidade será convocada reuniões extraordinárias

GT SEG
Pagamentos Instantâneos

Obrigado!

BANCO CENTRAL DO BRASIL