

# 10º Fórum PI

## GT SEG Pagamentos Instantâneos

Apresentação da evolução dos trabalhos de segurança do PIX



# GT de Segurança I Motivadores, participantes e metodologia

## Contexto

O GT SEG é um grupo de trabalho 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

## Objetivos

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

## Participantes\*

- |             |                       |
|-------------|-----------------------|
| 1. ABBC     | 11. ZETTA             |
| 2. ABECS    | 12. PSTI ABBC         |
| 3. ABIPAG   | 13. PSTI C&M SOFTWARE |
| 4. ABO20    | 14. PSTI JD           |
| 5. ABRACAM  | 15. SINDTELEBRASIL    |
| 6. ABRANET  | 16. TESOURO NACIONAL  |
| 7. AGEV     | 17. B3                |
| 8. AMPEF    | 18. CIP               |
| 9. FEBRABAN | 19. Claro             |
| 10. PAGOS   | 20. RTM               |

\* Participantes aprovados pelo Banco Central

# GT de Segurança

## Contexto

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

## Agenda

- 1 > Casos de risco, abusos e mitigadores para o uso do QrCode e link
- 2 > Especificação técnica preliminar da API de Recebimento

# GT de Segurança | Casos de risco, abusos e mitigadores para o uso do QRCode e link

## Contexto

Foram mapeados 4 casos de riscos, abuso e seus mitigadores para o uso do QRCode e link, muitos dos riscos apontados já existem atualmente em outros meios de pagamentos e podem ser migrados para o PIX.



### Cenário

- Fraudador cria APP para fraudar imagem QR code estático através de manipulação de acesso a câmera, visto que junto do APP da instituição, outro APP pode ter acesso ao hardware e tentar manipular a imagem.
- Motivador, arquitetura dos Sistemas Operacionais Mobile - Hardware Abstraction Layer)



### Mitigantes

- Certificar que o SDK de leitura da câmera não foi manipulado durante a leitura da imagem.  
(recomendação a ser incluída no manual de segurança)
- BCB e GT SEG devem criar processo para centralizar e comandar o TAKEDOWN de APPs fraudulentos identificados e reportado pelos participantes do PIX junto as lojas de aplicativos.

# GT de Segurança | Casos de risco, abusos e mitigadores para o uso do QRCode e link

## Contexto

Foram mapeados 4 casos de riscos, abuso e seus mitigadores para o uso do QRCode e link, muitos dos riscos apontados já existem atualmente em outros meios de pagamentos e podem ser migrados para o PIX.



### Cenário

- Fraudador cria imagem QRCode estático apontando para URL falsa
- Após leitura pode haver o acionamento do APP de Browser nativo
- Fraudador pega dados da conta/recurso da vítima



### Mitigantes

- Recomendar que o SDK de leitura da câmera receba informação que seja interpretada apenas como texto, impedindo acionamento de outro APP do telefone ou formato de QRCode.  
(recomendação a ser incluída no manual de segurança)

# GT de Segurança | Casos de risco, abusos e mitigadores para o uso do QrCode e link

## Contexto

Foram mapeados 4 casos de riscos, abuso e seus mitigadores para o uso do QrCode e link, muitos dos riscos apontados já existem atualmente em outros meios de pagamentos e podem ser migrados para o PIX.



### Cenário

- Fraudador utiliza técnica de desviar a resolução de nomes DNS a partir da invasão de um serviço local (modem ADSL) ou até mesmo por um ataque cibernético a provedores deste serviço.
- Após leitura pode haver o acionamento do APP de browser nativo do aparelho.
- Fraudador pega dados da conta/recurso da vítima.



### Mitigantes

- Cadastramento centralizado no BCB dos IPS ou site/domínio dos links (QR CODE Dinâmico ou PIX LINK-futuro) das instituições participantes do PIX, disponibilizando esse cadastro via API. Desta forma, o APP da instituição no Onboarding poderá validar se o domínio recebido corresponde a um participante e se a tradução DNS/IP foi correta.

# GT de Segurança | Casos de risco, abusos e mitigadores para o uso do QrCode e link

## Contexto

Foram mapeados 4 casos de riscos, abuso e seus mitigadores para o uso do QrCode e link, muitos dos riscos apontados já existem atualmente em outros meios de pagamentos e podem ser migrados para o PIX.



### Cenário futuro

- Fraudador cria um link falso se passando pelo Pix.
- Fraudador envia link falso para possíveis vítimas.
- Fraudador pega dados da conta/recurso da vítima.



### Mitigantes

- URL padrão com endereço exclusivo do PIX (contemplado).
- Criação de domínio exclusivo para o Pix, por exemplo: pix.br, assim como há o b.br
- BCB e GT SEG devem criar processo para centralizar e comandar o TAKEDOWN de URLs falsas identificadas e reportadas pelos participantes do Pix.

# GT de Segurança

## Contexto

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

## Agenda

- 1 > Casos de risco, abusos e mitigadores para o uso do QrCode e link
- 2 > Especificação técnica preliminar da API de Recebimento

# GT de Segurança | Especificação técnica preliminar da API de Recebimento

## Contexto

O GT SEG realizou contribuições com o Banco Central ao longo dos últimos 2 meses com reuniões específicas para detalhamento dos padrões técnicos para autenticação e autorização da API de Recebimentos.

### *Tópico - Recomendações de segurança da especificação técnica preliminar diz:*

Item 4 - Assegurar a segurança do desenvolvimento do software cliente<sup>11</sup> da API, mesmo que desenvolvido por terceiros. Sugere-se que o PSP institua e mantenha processo de homologação dos softwares clientes, **estabelecendo critérios mínimos de segurança para que eles sejam autorizados a interagir com a API**. Nesse caso, a API deve negar tentativas de comunicação de clientes não homologados.

Dentre as contribuições realizadas o GT SEG entende que deveria haver de forma mais clara quais são as recomendações mínimas de segurança para que os estabelecimentos comerciais tenham acesso a API, respeitando o princípio de risco de cada instituição.

- ① Os PSPs utilizarem o NIST Cybersecurity Framework e a ISO 27001 como referências para análise do cliente.
- ② Os itens sobre desenvolvimento seguro que são aplicados ao PSP também devem ser aplicados aos clientes da API
  - i. Adotar metodologia de desenvolvimento seguro, de forma a reduzir os riscos de segurança conforme OWASP Top Ten
  - ii. Adotar CWE/SANS Top 25 Software Errors.
- ③ Possuir processo periódico de análise de vulnerabilidades, tanto estática como dinâmica da API.

Fica a cargo de cada PSP a forma de aplicar as recomendações acima, porém recomendamos que seja aplicado através de contrato

# 10º Fórum PI

## GT SEG Pagamentos Instantâneos

Apresentação da evolução dos trabalhos de segurança do PIX

