

GE-SEG

16ºciclo

Setembro 2025

Pauta de trabalho

Aprimoramento das informações de fraude do DICT (Grupo 1)

- refinamento da taxonomia de fraudes (abertura e fechamento do Med)
- motivo para a rejeição da notificação de infração pelo PSP do recebedor
- ponto adicional -> Revisão dos campos retornados na consulta de estatísticas

Saneamento das marcações de fraude no DICT (Grupo 2)

- identificação de marcações indevidas
- mecanismos de desmarcação
- forma de operacionalização
- prazo para saneamento
- manutenção da base higienizada

Crítérios e procedimentos mínimos para marcação de fraude (Grupo 2)

- critérios mínimos para marcação de fraude e aceitação de NI
- critérios para recusa de notificação
- procedimentos operacionais
- direito ao contraditório do usuário
- prazos de implementação

Aprimoramento das informações de fraude do DICT

Objetivo: Melhorar a classificação de fraudes no DICT, visando aumentar a eficácia na mitigação de riscos de fraude nas transações Pix.

16% das notificações de infração abertas e mais de um terço das marcações de fraude registradas em 2024 foram classificadas com o valor "OTHER".

1 Propostas de Refinamento dos motivos de abertura e fechamento do Med:

- Sugestões para uma nova classificação de fraudes nos campos de abertura e fechamento de Notificação de infração e marcação de fraude (SituationType e FraudType)
- Critérios para classificação de casos para reduzir divergências de interpretação pelos diversos participantes
- Consideração de uma classificação em dois níveis para maior detalhamento, com tipos representando agrupamentos de situações, como golpe (SCAM) e subtipos detalhando as diversas situações (no caso de golpe: pirâmide, golpista se passando por familiar, falsa venda etc.)?

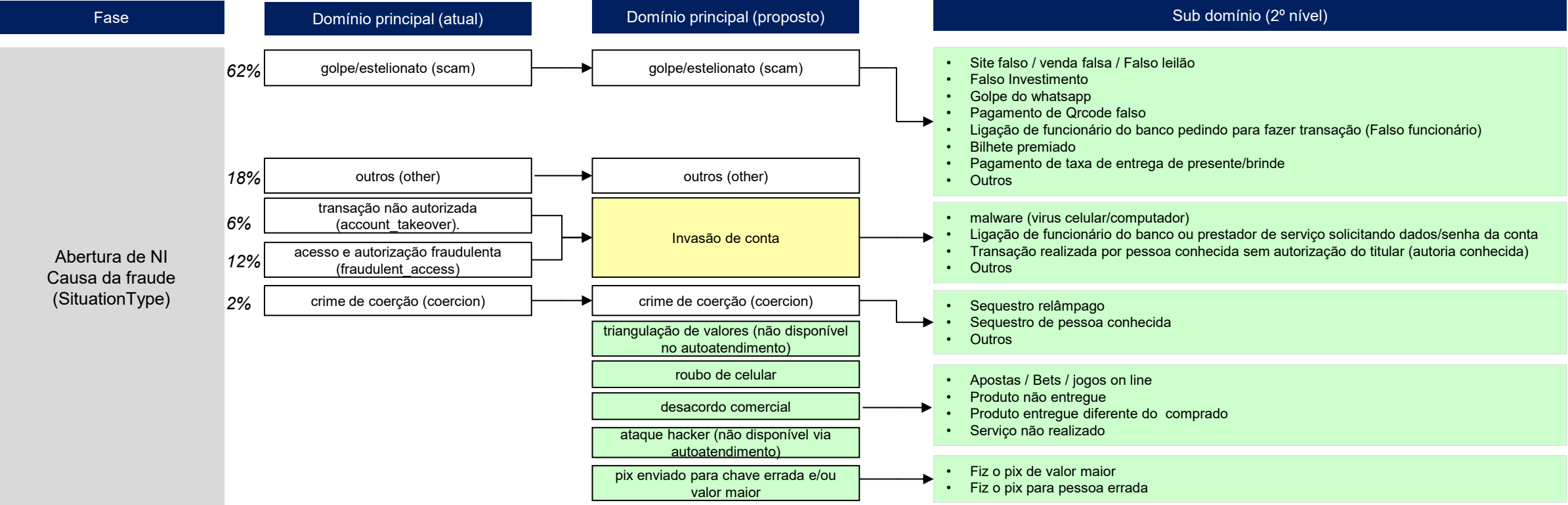
2 Campo de Motivo de Rejeição:

- Proposta de criação de um campo obrigatório para indicar o motivo da rejeição de notificações de infração e/ou de cancelamento da notificação de infração pelo PSP do pagador.
- Discussão sobre os motivos que deveriam constar na taxonomia desse campo, exemplo: desacordo comercial, transações Pix enviadas incorretamente por erro do usuário pagador etc.

3 Pontos adicionais:

- Revisão dos campos retornados na consulta de estatísticas.
- Identificação da natureza jurídica das contas vinculadas a chave pix (principalmente MEI).

Refinamento da taxonomia de abertura do Med



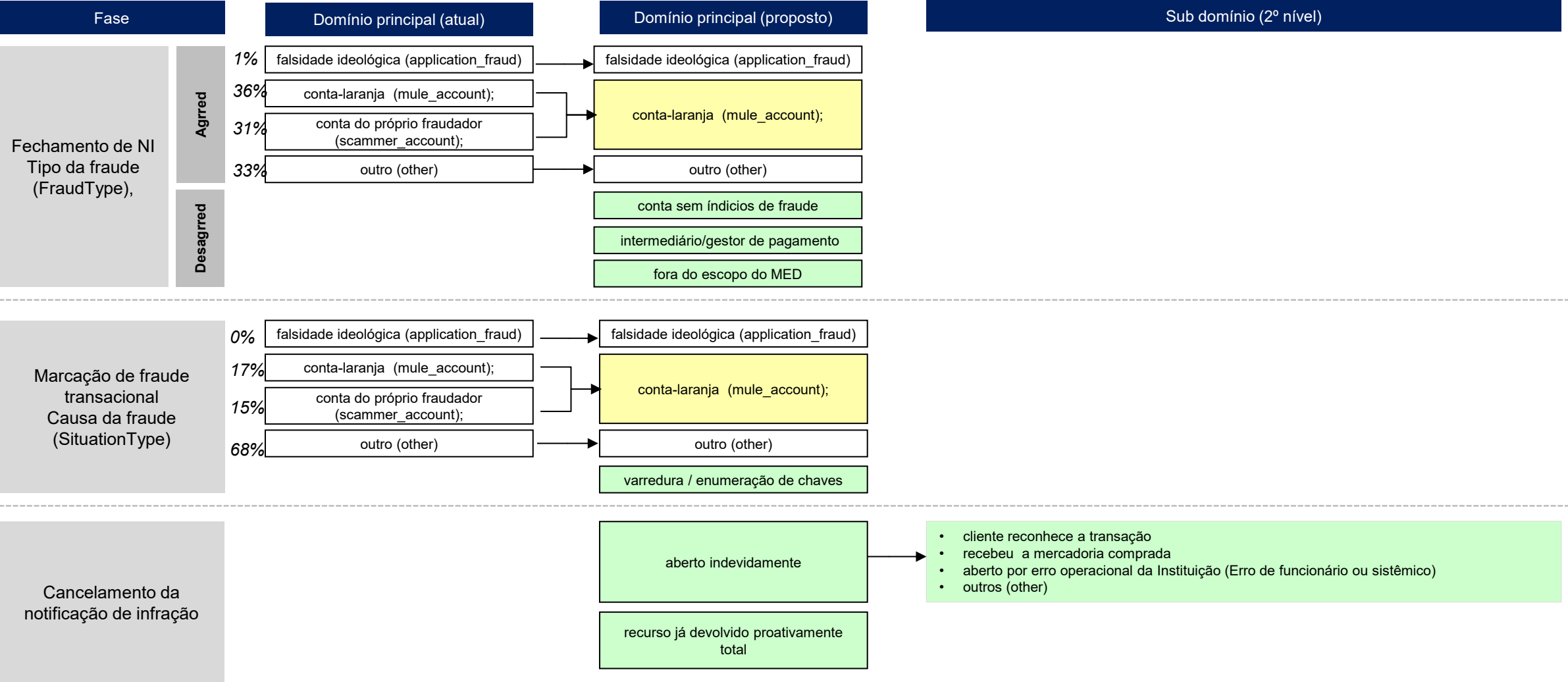
Ponto de atenção: Campo descrição obrigatório em todos os domínios/subdomínio.
Tornar o campo de descrição obrigatório em todas as notificações de infração garante clareza sobre os fatos, reduz falsos positivos, apoia a análise do PSP recebedor e melhora a qualidade dos dados do DICT.

Legenda:

Alterado

Novo

Refinamento da taxonomia de marcação de fraude transacional, fechamento do Med, criação dos campos de rejeição de med e cancelamento de notificação de infração



Ponto de atenção: Campo descrição obrigatório em todos os domínios/subdomínio.
Tornar o campo de descrição obrigatório em todas as notificações de infração garante clareza sobre os fatos, reduz falsos positivos, apoia a análise do PSP recebedor e melhora a qualidade dos dados do DICT.

Legenda:
Alterado Novo

Revisão dos campos retornados na consulta de estatísticas:

Atual

Dados:

- quantidade de liquidações como recebedor no SPI (Settlements);
- quantidade de NI confirmadas e marcações de fraude transacional criadas com fraude do tipo:
 - “falsidade ideológica” (ApplicationFrauds);
 - “conta laranja” (MuleAccounts);
 - “conta fraudador” (ScammerAccounts);
 - “outros” (OtherFrauds);
 - sem identificação de tipo de fraude (UnknownFrauds);
- valor total das notificações confirmadas (TotalFraudTransactionAmount);
- quantidade de PSP’s distintos que confirmaram pelo menos uma notificação contra a chave ou o CPF/CNPJ consultado (DistinctFraudReporters);
- quantidade de notificações em análise(OpenReports);
- quantidade de participantes distintos que possuem notificações em análise (OpenReportsDistinctReporters);
- notificações de infração rejeitadas totais(RejectedReports);
- quantidade de contas distintas às quais a chave esteve associada (quando uma chave for consultada) (RegisteredAccounts).

Prazos:

- últimos 90 dias;
- últimos 12 meses (sem considerar o mês no qual a consulta é realizada);
- últimos 60 meses (sem considerar o mês no qual a consulta é realizada).

Formato:

- Contadores (acumulado)

Momento da consulta:

- Fluxo transacional do pix
- Consulta por demanda nas API’s getPersonStatistics e getEntryStatistics

Proposto

Dados:

- quantidade de liquidações como recebedor no SPI (Settlements);
- quantidade de NI confirmadas e marcações de fraude transacional criadas com fraude do tipo:
 - “falsidade ideológica” (ApplicationFrauds);
 - “conta laranja” (MuleAccounts);
 - “conta fraudador” (ScammerAccounts);
 - “outros” (OtherFrauds);
 - sem identificação de tipo de fraude (UnknownFrauds);
- valor total das notificações confirmadas (TotalFraudTransactionAmount);
- quantidade de PSP’s distintos que confirmaram pelo menos uma notificação contra a chave ou o CPF/CNPJ consultado (DistinctFraudReporters);
- quantidade de notificações em análise(OpenReports);
- quantidade de participantes distintos que possuem notificações em análise;
- notificações de infração rejeitadas totais(RejectedReports);
- quantidade de contas distintas às quais a chave esteve associada (quando uma chave for consultada) (RegisteredAccounts);
- ID da notificação de infração e marcação de fraude ou chave única para identificação;
- ISPB do participante que aceitou a NI/marcação;
- Causa e subcausa da fraude (SituationType);
- Valor da transação associada;
- Datas de abertura, fechamento e cancelamento da NI;
- Status da notificação e da marcação;
- Motivo e submotivo de cancelamento;
- Tipo de chave utilizada (QR Code, e-mail, telefone, documento, agência/conta);
- Tipo de pessoa associado a chave (PF ou PJ);
- Natureza jurídica do CNPJ vinculado a chave.

Prazos:

- Dias do mês vigente;
- últimos 12 meses (sem considerar o mês no qual a consulta é realizada);
- Histórico completo.

Formato:

- Contadores (acumulado)
- Análítico (detalhado)

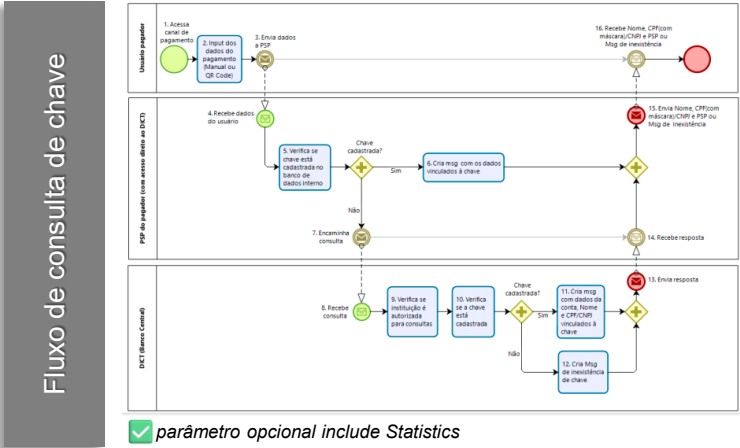
Momento da consulta:

- Contadores (acumulado)
- Análítico (detalhado)

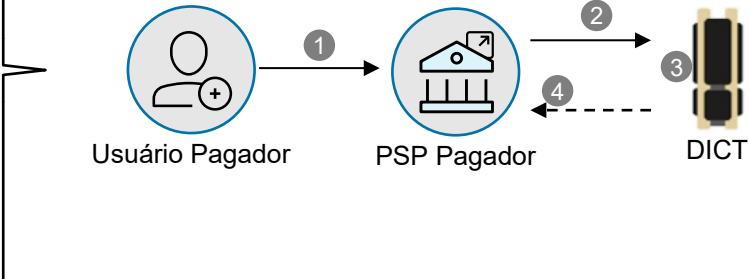
Legenda:

Alterado Novo

Formato de retorno



Manter o formato atual de retorno (contadores)
Sem impacto no fluxo transacional



Detalhamento das etapas

- 1 Usuário pagador acessa seu canal de atendimento e insere os dados da chave do usuário recebedor
- 2 PSP do usuário pagador envia mensagem de consulta ao DICT incluindo o parâmetro "include Statistics".
- 3 DICT recebe mensagem com solicitação de consulta e faz as devidas verificações cria mensagem e envia resposta à consulta
- 4 PSP recebe mensagem com a resposta à consulta

Retorno da consulta da API de Estatísticas do DICT

Propostas para alteração do formato de retorno das informações de consulta

Proposta 1

Alteração do formato para tabela detalhada

Prós

- ✓ Maior granularidade para análises de risco;
- ✓ Visão completa do documento/chave consultado;
- ✓ Permite cruzamento de dados e identificação de padrões complexos;
- ✓ Melhora a eficácia dos sistemas antifraude e modelos preditivos;
- ✓ Facilita a identificação de modus operandi e fraudes estruturadas;
- ✓ Possibilita análises históricas detalhadas e segmentação por perfil;
- ✓ Ajuda a validar a confiabilidade do dado recebido e evitando inconsistência nas análises de risco;

Contras

- ✗ Maior volume de dados pode exigir ajustes tecnológicos;
- ✗ Potencial aumento no tempo de processamento das consultas.

VS

Proposta 2

Manutenção do formato de contadores

Prós

- ✓ Menor impacto tecnológico e adaptação mais rápida;
- ✓ Mantém padrão atual, reduzindo curva de aprendizado;

Contras

- ✗ Limita a capacidade analítica na detecção de fraudes;
- ✗ Não permite análises detalhadas;
- ✗ Reduz a efetividade na prevenção proativa e no combate a fraudes.

Justificativa para cada informação solicitada

- **ID da notificação e marcação ou chave única:** Permite vincular eventos relacionados à mesma ocorrência dentro dos sistemas internos, garantindo consistência no histórico e evitando duplicidades. Essa identificação única é essencial para análises estatísticas, correlação de dados e construção de perfis de risco mais precisos.
- **ISPB do participante:** Ajuda a validar a origem da informação e a confiabilidade do dado recebido, permitindo que a instituição ajuste pesos e relevância nos seus modelos internos. Essa informação é usada para calibrar regras antifraude e melhorar a qualidade das análises de risco.
- **Causa e subcausa da fraude:** Fundamentais para compreender o modus operandi e alimentar modelos preditivos com tipologias específicas. Essa granularidade permite ajustar regras internas, identificar padrões recorrentes e antecipar novas estratégias de fraude.
- **Valor da transação:** Permite mensurar impacto financeiro das fraudes e identificar perfis de risco. Permite calibrar limites de alerta, ajustar políticas internas e direcionar esforços preventivos para faixas de valor mais visadas.
- **Datas de abertura, fechamento e cancelamento:** Auxiliam na identificação de comportamentos atípicos ou cancelamentos frequentes, que podem indicar falhas nos processos de análise das IF's. Ajuda a validar a confiabilidade do dado recebido e evitando inconsistência nas análises de risco.
- **Status da notificação e da marcação:** Indica a situação final do evento, permitindo que a instituição diferencie casos confirmados, cancelados ou pendentes. Essa informação é usada para refinar indicadores internos e melhorar a assertividade dos modelos antifraude.
- **Motivo e submotivo de cancelamento:** Essenciais para entender por que uma marcação foi revertida, ajudando a identificar possíveis vulnerabilidades no processo e ajustar regras internas para evitar que mecanismos legítimos sejam explorados de forma indevida.
- **Tipo de chave utilizada:** Permite identificar quais tipos de chaves apresentam maior incidência de fraude e direcionar medidas de mitigação específicas.
- **Tipo de pessoa (PF ou PJ) e natureza jurídica:** Essenciais para segmentar riscos por perfil de cliente, calibrar modelos internos e aplicar políticas diferenciadas conforme características do usuário, aumentando a eficácia das estratégias de prevenção.

Saneamento das marcações de fraude no DICT

Objetivo: Identificar, corrigir e prevenir marcações indevidas de fraude no DICT, visando aumentar a confiabilidade das informações e a efetividade dos mecanismos de prevenção a fraudes no Pix.

Pontos avaliados:

- **Identificação de marcações indevidas:** Quais critérios e mecanismos podem ser utilizados para detectar inconsistências?
- **Forma de operacionalização:** Como será conduzido o processo de correção? Haverá validação cruzada entre participantes?
- **Prazo para saneamento:** Qual o tempo adequado para que os participantes realizem a limpeza da base?
- **Manutenção da base higienizada:** Quais controles e rotinas devem ser implementados para evitar reincidência?

Mecanismos de Desmarcação:

- Avaliação da efetividade dos métodos atuais de remoção de marcações.
- Necessidade (ou não) de criação de formas alternativas de desmarcação, especialmente em casos de erro evidente ou contestação válida.

Instrução Normativa nº 425, em 16/10/2024

131 mil

Marcações canceladas em dois meses (Out. e nov.24)

↓ 15%

Aceitação de Med

↓ 80%

Taxa de reversões das marcações

- 1º movimento de saneamento das marcações de fraude
- maior precisão nas sinalizações após a implementação da IN nº 425.

Propostas



API do contraditório



Dashboard de Governança

API contraditório

Objetivo: Estabelecer um processo estruturado e automatizado que permita às Instituições Financeiras (IFs) solicitarem a revisão de marcações de fraude realizadas por outras IFs, com base em critérios objetivos e previamente definidos..

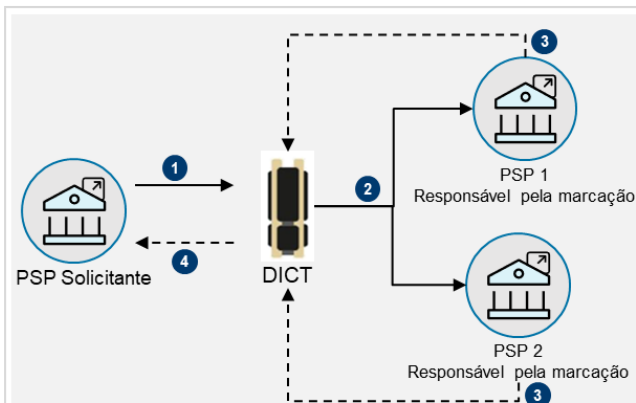
Premissas

- Solicitações devem ser feitas de forma individual (não em lote).
- O usuário deve possuir uma ou mais marcações de fraude confirmada e ativa no DICT.
- Não pode haver notificações de infração em aberto associadas ao CPF/CNPJ.

Critérios de solicitação

- Apenas uma solicitação de revisão por CPF/CNPJ /IF detentora da marcação
- Nos casos de múltiplas marcações, a solicitação é encaminhada automaticamente a todas as IFs envolvidas.
- Limite mensal por instituição recebedora: até 0,5% da média de MEDs recebidos nos últimos seis meses.
- **Exemplo de funcionamento:** caso uma IF já tenha revisado a marcação de um CPF, o sistema impede novas revisões para o mesmo caso, retornando aviso de “marcação já revisada via API do Contraditório”. Exceto no cenário que a marcação tiver sido cancelada e posteriormente incluída nova marcação pela mesma IF. Neste caso, poderá ser aberto nova solicitação de revisão, pois trata-se de nova marcação, inserida após a ultima revisão via API contraditório.
- Em caso de portabilidade de chave, a marcação de fraude continua vinculada a IF que marcou, a qual será responsável pela revisão.

Macro fluxo de acionamento da API



Detalhamento das etapas

- 1 IF abre solicitação para revisão de marcações (API contraditório). A requisição inclui:
 - Identificador da chave (CPF/CNPJ)
 - Motivos:
 - Suspeita de conta fria
 - Desacordo comercial
 - Solicitação de abertura de conta
 - Análise de relacionamento comercial (histórico de boa conduta)
 - Outros (Obrigatório descrever a justificativa para revisão)
- 2 O BCB envia a requisição aos PSP's responsáveis pelas marcações no CPF/CNPJ (pode ser mais de 1)
- 3 IF's recebe a requisição, reavalia o caso e decide:
 - Aceitar e cancelar a marcação de fraude;
 - Recusar, manter a marcação, justificando a decisão, incluindo:
 - Data de abertura ou tempo de conta.
 - Data de criação da chave.
 - Valor da contestação que gerou a marcação.
 - Detalhes do tipo de golpe e análise da IF;Ausência de resposta em até 7 dias úteis: exclusão automática da marcação da instituição que não respondeu (marcações das demais instituições serão mantidas).
- 4 PSP solicitante recebe a resposta

SLA

7 dias úteis

Benefícios esperados

- Redução de falsos positivos.
- Transparência entre instituições.
- Menor judicialização.

Dashboard de Governança (plataforma central de monitoramento e controle)

Objetivo: Fornecer visão centralizada, periódica e automatizada sobre a qualidade e consistência das marcações de fraude realizadas e recebidas pelas IFs.

Ponto de atenção: Os participantes terão acesso aos seus respectivos indicadores e a visão de geral mercado sem identificação dos outros participantes.

Indicadores principais

- Taxa de marcação de fraude por instituição / ISPB.
- Taxa de marcação por tipo de fraude.
- Taxa de reversão por período.
- Tempo médio de cancelamento.
- Comparativo com benchmark de mercado.
- Score de confiabilidade da marcação de fraude.
- Percentual de clientes com marcação de fraude no mercado.
- Solicitações de revisão de marcação (abertas/ recebidas/ não respondidas por período e comparativo de mercado).

Alertas automáticos

- IFs fora da curva serão notificadas pelo Dashboard.
- Período inicial de adaptação de 180 dias, sem penalidades.
- Após esse prazo, definição de percentuais aceitáveis e obrigações de atuação.

Relatórios mensais

- Lista de marcações com alta probabilidade de indevidas será enviada às IFs.
- IFs devem responder em até 15 dias úteis: aceitar/cancelar ou recusar com justificativa.
- Ausência de resposta gera notificação formal do BCB.

Indicadores e inteligência analítica

Métricas adicionais: taxa de reversão por IF; tempo médio de cancelamento; volume de marcações vs. transações legítimas (índice de confiabilidade do cliente); clusters de marcações por CPF/CNPJ e IFs.

Outputs: score de confiabilidade e justificativas técnicas.

Funcionalidades adicionais

- Filtros por tipo de fraude, período e status da marcação.
- Exportação de relatórios em CSV/PDF..

Benefícios esperados

- Governança contínua da base do DICT.
- Identificação de inconsistências e padrões de marcação indevida.
- Redução de falsos positivos e maior proteção ao consumidor.
- Escalabilidade e retroalimentação contínua.
- Suporte estruturado às decisões das IFs e do BCB.

Critérios e procedimentos mínimos para marcação de fraude

Objetivo: Padronizar e qualificar o processo de análise das notificações de infração, visando aumentar a assertividade do MED, garantir maior clareza e segurança jurídica no processo, e fortalecer a confiança dos usuários e participantes do Pix.

Pontos avaliados:

Critérios mínimos:

- Definição de requisitos mínimos para:
 - Aceitação de notificações de infração com solicitação de devolução.
 - Criação de marcação de fraude transacional.
- Avaliação da necessidade de fluxos distintos para cada tipo de ação.



Critérios para recusa de notificação:

- Fundamentos válidos para recusa da notificação de infração pelo PSP do recebedor.
- Garantia de consistência e transparência na decisão.

Procedimentos operacionais:

- Detalhamento dos fluxos de decisão (aceite, recusa, marcação).
- Documentação mínima exigida para cada etapa.
- Justificativas técnicas e legais para os procedimentos propostos.



Direito ao contraditório:

- Avaliação da viabilidade de um processo de contraditório para o usuário sob suspeita de fraude.
- Identificação de situações em que o contraditório pode ser dispensado.

Prazos de implementação:

- Proposta de cronograma para adequação dos participantes às novas exigências.

Recomendações:

- Manter os critérios de análise e apetite de risco de cada Instituição;
- Critérios **sugeridos** como boas práticas (aceite e marcação):
 - Multifatorial, não binário: combinação de sinais internos e interinstitucionais, ponderados por perfil de risco (PF vs. CNPJ).
 - Consulta às marcações do DICT (pós-saneamento): uso do histórico saneado como variável relevante. Alguns indicadores relevantes:
 - % de infrações do tipo “MULE_ACCOUNT” aceitas em relação ao total de Pix liquidados pelo CPF/CNPJ nos últimos 90 dias.
 - Nº de instituições distintas que enviaram infrações do tipo “MULE_ACCOUNT” nos últimos 90 dias.
- Obrigatoriedade do campo <AnalysisDetails> em toda recusa, com justificativa técnica.

- Respeito aos processos internos de cada instituição, assegurando padronização mínima nos campos de evidência (inclusive <AnalysisDetails>).

- O grupo não recomenda processo de contraditório pelo usuário sob suspeita de fraude durante a etapa da análise da notificação de infração pois pode favorecer golpistas e pessoas que emprestam suas contas, além de expor as instituições a riscos jurídicos.

- Até 180 dias após a publicação das diretrizes técnicas (campos/artefatos no DICT e manual) para ajustes de sistemas, processos e capacitação.

GE-SEG

Obrigado!