Validado em 08/10/2025

PRINCÍPIOS ORIENTADORES DA GESTÃO DE FRAUDES

(Iniciativa Regional de Roaming da CEDEAO)

Índice

Resumo 3
1. Contexto: 4
2. Objetivo: 5
2.1 Comités nacionais e regionais de combate à fraude 5
2.2 Riscos potenciais de fraude 8
2.3 Diretrizes gerais para gestão e prevenção de fraudes: 11
2.3.1 Anti-FKPI_001: 13
2.3.1.1 Descrição do controlo/KPI: 13
2.3.1.2 RACI (Responsável/Prestável contas/Consultar/Informar): 14
2.3.2 Anti-FKPI_002: 14
2.3.2.1 Descrição do controlo/KPI: 14
2.3.2.2 RACI (Responsável/Prestador de contas/Consultor/Informador): 14
2.3.3 Anti-FKPI_003: 14
2.3.3.1 Descrição do controlo/KPI: 15
2.3.3.2 RACI (Responsável/Prestador de contas/Consultar/Informar): 15
2.3.4 Anti-FKPI_004: 15
2.3.4.1 Descrição do controlo/KPI: 15
2.3.4.2 Responsável/Prestador de contas/Consultor/Informador (RACI): 16
2.3.5 Anti-FKPI_005: 16
2.3.5.1 Descrição do controlo/KPI: 16
2.3.5.2 Responsável/Consultar/Informar (RACI): 16
2.3.6 Anti-FKPI_006: 16
2.3.6.1 Descrição do controlo/KPI: 16
2.3.6.2 Responsável/Prestador de contas/Consultar/Informar (RACI): 17
2.3.7 Anti-FKPI_007: 17
2.3.7.1 Descrição do controlo/KPI: 17
2.3.7.2 Responsável/Prestador de contas/Consultar/Informar (RACI): 17
2.4 Matriz de Suporte Técnico e Escalonamento 17
2.5 Denúncia de fraudes 18
ANEXO 1 18
ANEXO 2 19
ANEXO 3 20

Resumo

O Regulamento C/Reg.21/12/17 da CEDEAO sobre roaming em redes públicas de comunicações móveis na região da CEDEAO, artigo 15.º, n.º 2, exige que os Estados-Membros criem comités para controlar a fraude na área do roaming comunitário.

As Resoluções 1, 2 e 3 da DG da ARN exigiram a criação de comités nacionais e regionais para desenvolver mecanismos de controlo da fraude a nível nacional e regional, a fim de lidar eficazmente com as questões de fraude quando o serviço de roaming se tornar operacional. Com base no mandato acima referido, o Comité Técnico de Implementação criou um Comité Regional Antifraude (RAFC) a ser liderado pelo Gana.

O primeiro resultado do RAFC foi o desenvolvimento de um plano de trabalho para a gestão da fraude. Este plano de trabalho detalhava as atividades propostas/previstas a realizar para cumprir este mandato.

O Comité desenvolveu então uma matriz de estado da gestão de fraudes para os Estados-Membros preencherem, a fim de permitir ao Comité conhecer o estado dos países no que diz respeito à gestão de fraudes. O Comité identificou então os Termos de Referência (ToR) abaixo indicados para orientar os trabalhos dos Comités Nacionais e Regionais Antifraude.

Termos de Referência dos Comités Nacionais Antifraude

- Documentar as atividades fraudulentas atualmente prevalentes no país.
- Identificar os tipos de fraude potenciais que podem surgir
- Avaliar os quadros jurídicos existentes para a gestão e o controlo da fraude

Termos de Referência dos Comités Regionais Antifraude

- Identificar e destacar os tipos de fraude potenciais que podem surgir após a implementação.
- Desenvolver diretrizes antifraude sob a forma de controlos de mitigação de fraudes e indicadores-chave de desempenho (KPI) de monitorização.
- Coordenar as atividades dos vários Comités Nacionais Antifraude em relação à Iniciativa de Roaming Livre da CEDEAO, entre outras tipologias de fraude
- Fazer um balanço e avaliar a suficiência da infraestrutura de gestão de fraudes dos Estados-Membros para uma gestão eficaz e eficiente das fraudes
- Desenvolver protocolos para orientar o tratamento dos números de fraude detetados (MSISDNs) pelos Estados-Membros.
- Avaliar e recomendar sistemas e ferramentas de gestão de fraudes.
- Desenvolver e implementar requisitos adequados de comunicação de fraudes e rever regularmente os relatórios dos Estados-Membros.
- Prestar apoio técnico aos Estados-Membros para a implementação de controlos e indicadores-chave de desempenho

Com base nas respostas relativas ao estado da gestão da fraude, os Estados-Membros que não dispunham de comités nacionais antifraude receberam ajuda para criar alguns. Aqueles que não dispunham de um quadro jurídico específico para gerir a fraude nas telecomunicações receberam orientações e, em alguns casos, foram partilhados exemplos de quadros jurídicos de outros países para os orientar a este respeito. Quase todos os países tinham algum tipo de sistema de gestão de fraudes ao nível dos operadores. Outros

tinham sistemas tanto ao nível dos operadores como das ANR. Quase todos os países e es tinham implementado um sistema nacional de identificação robusto, com exceção de dois (2). Outros tinham os seus em curso, seja ao nível dos operadores, seja ao nível nacional.

Com base nos resultados dos Termos de Referência e nas atualizações sobre gestão de fraudes fornecidas pelos países, o Comité apresentou potenciais riscos de fraude e KPIs antifraude para servir como controlos de mitigação de fraudes. Também foi desenvolvido um modelo de relatório de fraudes para orientar as operadoras nos Estados-Membros na comunicação de atividades fraudulentas identificadas.

A fraude nas telecomunicações não é estática, mas sim dinâmica, pelo que o Comité Regional Antifraude recomenda que os operadores cumpram rigorosamente os controlos de mitigação de fraudes identificados. Aqueles que não dispõem do equipamento necessário para mitigar qualquer um dos riscos de fraude previstos devem, com caráter de urgência, adquirir os módulos de equipamento e/ou software necessários para estar em conformidade com os controlos de mitigação de fraudes propostos.

Para além da recomendação acima referida, será necessário dispor de uma plataforma de controlo de gestão de fraudes de terceiro nível para gerir a fraude a nível regional.

Os potenciais fornecedores de soluções e ferramentas de gestão de fraudes foram envolvidos nos
requisitos de risco de fraude. A Equipa Regional será responsável pela entrega de qualquer
implementação tanto a nível nacional como regional.

Por razões de eficiência operacional e proteção de dados, qualquer solução adotada será estruturada de forma a processar dados e aplicar a lógica de deteção a nível nacional, enquanto as informações de alerta e os detalhes resumidos são partilhados a nível regional.

1. Contexto:

A Iniciativa de Roaming da CEDEAO é uma iniciativa proposta pelos Ministros das Telecomunicações/TIC da CEDEAO durante a sua reunião no Níger em 2016. A iniciativa visa, entre outros objetivos:

i. harmonizar as tarifas/encargos de roaming na região da CEDEAO
ii. facilitar as comunicações e o comércio transfronteiriços

Ao abrigo desta política, foi adotado o Regulamento C/REG. 21/12/17 relativo ao roaming em redes públicas de comunicações móveis na região da CEDEAO. O regulamento exige também que os Estados-Membros criem comissões para controlar a fraude na área do roaming comunitário.

Em 2019, houve um novo apelo dos Ministros das Comunicações/Telecomunicações/TIC da sub-região para dar início à Iniciativa de Roaming da CEDEAO, tendo em conta o comércio da CEDEAO, a conectividade transfronteiriça e as tarifas de roaming que podem impedir o progresso do comércio.

Os diretores-gerais e presidentes das autoridades reguladoras nacionais (ARN) da CEDEAO, cientes do potencial afluxo de fraudes de desvio com a implementação da Iniciativa de Roaming Livre da CEDEAO, na sua 2.ªReunião de Alto Nível, em março de 2021, reiteraram a necessidade de criar comités nacionais e regionais de combate à fraude até 31 de maio de 2021, em conformidade com o artigo 20.º do Regulamento n.º C/REG.21/12/17. Além disso, as ARN foram obrigadas a definir um esquema técnico e mecanismos eficazes de controlo da fraude a nível nacional e regional até **30 de junho de 2021.**

Prevê-se que os riscos de fraude inerentes aos serviços gerais de telecomunicações, em particular ao roaming, se manifestem em toda a sub-região após a ativação da importação de cartões SIM através da iniciativa. Por conseguinte, é essencial implementar mecanismos antifraude robustos para mitigar quaisquer riscos previstos.

2. Objetivo:

O objetivo deste quadro é elaborar os principais objetivos da agenda antifraude da WATRA em relação à Iniciativa de Roaming da CEDEAO, como se segue:

1. Coordenar a criação de comités nacionais e regionais de combate à fraude,
   - Assegurar a coordenação administrativa
   - Estabelecer ferramentas de coordenação técnica

2. Identificar e destacar os tipos de fraude potenciais que podem surgir após a implementação.

3. Desenvolver mecanismos de controlo mitigantes e KPIs de monitorização

4. Fornecer suporte técnico para a implementação desses controlos e KPIs

5. Monitorização contínua da eficácia dos controlos e dos KPI.

6. Analisar tecnicamente e propor uma solução de gestão de fraudes aos operadores dos Estados-Membros, quando necessário.

2.1 Comités nacionais e regionais de luta contra a fraude

A gestão da fraude ocorre em três níveis:

- Nível das operadoras móveis: as MNO devem garantir que cada operadora móvel tenha desenvolvido uma solução antifraude

- Nível das ARN: As autoridades reguladoras nacionais devem criar um comité nacional e uma plataforma, bem como mecanismos de colaboração e controlo das atividades antifraude, em conformidade com os regulamentos da CEDEAO.

- Nível regional: O Gana coordenará todas as atividades de denúncia de fraudes ao nível da CEDEAO, enquanto a plataforma regional servirá como principal ferramenta regional de combate à fraude.

Após a seleção do Gana como país líder na gestão antifraude, foi constituída uma equipa do seu Comité Nacional Antifraude para iniciar um compromisso a nível sub-regional. Esta equipa transformou-se posteriormente num **Comité Regional Antifraude (RAFC)**, com a nomeação de dois (2) representantes da ARN de cada Estado-Membro.

O Comité Regional forneceu orientações e apoio às respetivas ARN para constituírem os seus respetivos **Comités Nacionais de Combate à Fraude (NAFC)**.

A composição e o mandato dos comités nacionais e regionais de combate à fraude são os seguintes:

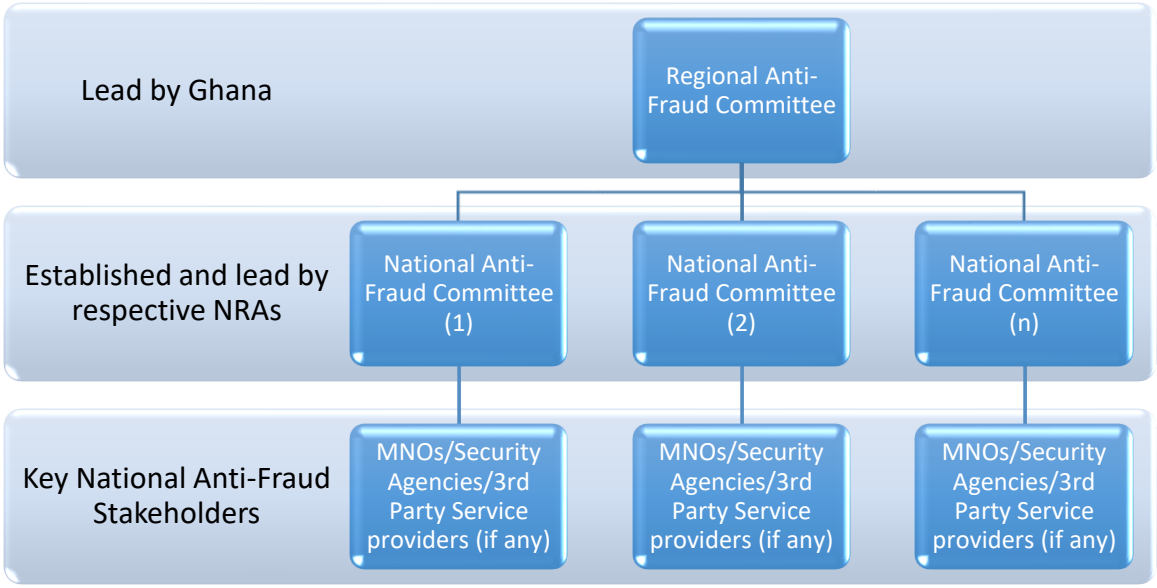
Comité Nacional Antifraude (NAFC)

- **Composição:**
    - Presidente: Representante da Autoridade Reguladora Nacional (ARN)
    - Vice-presidente: nomeado pelos membros da NAFC
    - Membros: Dois (2) representantes de cada operador de rede móvel (MNO) licenciado, representantes das agências de segurança do Estado relevantes e do ministério responsável pelas comunicações.
    - Secretariado: A NRA prestará apoio administrativo.
- **Mandato e objetivos:**
    - Atuar como principal órgão nacional para todas as atividades de gestão de fraudes relacionadas com roaming.
    - Implementar e fazer cumprir as diretrizes regionais antifraude e os KPIs a nível nacional.
    - Identificar, investigar e apresentar relatórios de incidentes de fraude utilizando modelos padronizados.
    - Facilitar a colaboração e a partilha de informações entre as MNOs nacionais e com a RAFC.
    - Avaliar a adequação dos quadros jurídicos nacionais para o julgamento de fraudes nas telecomunicações e recomendar as reformas necessárias.
    - Garantir que todas as MNOs nacionais tenham Sistemas de Gestão de Fraudes (FMS) funcionais em conformidade com as normas regionais.
    - Avaliar a eficácia dos controlos antifraude implementados pelas MNOs.

Comité Regional Antifraude (RAFC)

- **Composição:**
    - Liderado pelo país líder (Gana).
    - Membros: Dois (2) peritos técnicos nomeados pela ANR de cada Estado-Membro da CEDEAO.
    - Observadores: Representantes da ARTAO e da Comissão da CEDEAO.
- **Mandato e objetivos:**
    - Fornecer orientação estratégica e coordenação das atividades dos vários Comités Nacionais Antifraude em relação à iniciativa de Roaming Regional da CEDEAO, entre outros tipos de fraude.
    - Desenvolver, publicar e manter estas diretrizes, controlos e KPIs antifraude.
    - Receber, analisar e agir com base nas denúncias de fraude de todos os NAFC.
    - Identificar tipologias emergentes de fraude transfronteiriça e desenvolver estratégias de mitigação adequadas.
    - Desenvolver protocolos para orientar o tratamento de MSISDN fraudulentos detetados pelos respetivos Comités Nacionais Antifraude.
    - Fornecer planos de ação corretiva para os Estados-Membros com desempenho insuficiente.
    - Avaliar e recomendar sistemas e ferramentas de gestão de fraudes.
    - Realizar campanhas antifraude periódicas em toda a sub-região, com o apoio das respetivas ARN/NAFC.
    - Desenvolver e implementar requisitos adequados de comunicação de fraudes e rever regularmente os relatórios dos Estados-Membros.
    - Reforçar as capacidades e prestar apoio técnico às NAFC e às OMN.
    - Apresentar relatórios periódicos ao Comité de Ministros das Telecomunicações/TIC da CEDEAO sobre a situação da fraude na região de roaming.

As atividades antifraude estão estruturadas da seguinte forma:



2.2 Riscos potenciais de fraude

A iniciativa de roaming da CEDEAO é suscetível a vários tipos de fraude. Abaixo encontra-se uma categorização com base no impacto potencial e na probabilidade:

Tipo de fraude	**Descrição/cenário**	**Nível de risco**	**Mitigação proposta (ver secção 2.3)**
Contorno da SIM Box	Encerramento ilegal de chamadas internacionais através de SIMs locais para evitar taxas de gateway internacional. *Por exemplo, um fraudador configura um dispositivo com vários cartões SIM locais no Benim para encerrar chamadas destinadas a números nigerianos, contornando as tarifas internacionais.*	Alto	Ref: Anti-FKPI_003

Tipo de fraude	Descrição/cenário	Nível de risco	Mitigação proposta (ver secção 2.3)
IRSF/PRS (Partilha de receitas internacionais/serviço de tarifa premium) Fraude	Gerar chamadas para números com tarifas elevadas para obter partilha de receitas. *Por exemplo, o cartão SIM de um utilizador em roaming é comprometido e utilizado para ligar para números com tarifas elevadas num país distante, gerando custos elevados para a operadora local.*	Alta	Ref: Anti-FKPI_001
Wangiri (Um toque)	Fazer chamadas perdidas para solicitar chamadas de retorno para números com tarifa premium ( ). *Por exemplo, um utilizador em roaming recebe uma chamada perdida. Ao ligar de volta, é conectado a um número com tarifa premium, incorrendo em custos significativos.*	Médio	Ref: Anti-FKPI_004
Fraude de assinatura	Obter serviços sem intenção de pagamento, muitas vezes usando identidades falsas. *Por exemplo, um indivíduo usa identificação falsificada para adquirir vários SIMs especificamente para iniciar atividades fraudulentas de roaming.*	Médio	Verificações de identificação nacional, Ref: Anti-FKPI_004
Spam de SMS A2P	Contornar as vias legítimas de faturação/cobrança para o envio de SMS em massa de aplicações para pessoas. *Por exemplo, um*	Médio	Ref.: Anti-FKPI_002, Anti-FKPI_006

Tipo de fraude	Descrição/cenário	Nível de risco	Mitigação proposta (ver secção 2.3)
	fornecedor de conteúdos contorna o canal A2P oficial utilizando um banco de cartões SIM de roaming para enviar SMS em massa, evitando taxas mais elevadas.		
Falsificação de CLI	Manipulação da identidade da linha de chamada para mascarar a verdadeira origem de uma chamada. *Por exemplo, um fraudador falsifica o número oficial de um banco para realizar ataques de phishing contra utilizadores em roaming.*	Alto	Segurança de sinalização (por exemplo, STIR/SHAKEN), Ref: Anti-FKPI_004
Fraude com SIM de teste	Uso indevido de SIMs destinados a testar a interoperabilidade da rede e acordos de roaming. Por exemplo, um funcionário de uma operadora fornece um grande número de SIMs de teste a um terceiro que os utiliza para comunicação pessoal ou geração de tráfego ilícito, evitando cobranças.	Médio	Acordos bilaterais rigorosos que limitam a quantidade, a utilização (limites de dados/chamadas/SMS) e a vida útil dos SIM de teste. Auditorias e monitorização regulares para detetar padrões de tráfego anormais. Requer ação da rede responsável dentro de 96 horas
Roaming permanente	Um assinante utiliza um cartão SIM de um país de baixo custo permanentemente num país de custo mais elevado para beneficiar de tarifas de assinatura mais baratas. Por	Alto	Implementar e aplicar «políticas de utilização de roaming» nos termos e condições. Implementar ferramentas de monitorização (Anti-FKPI_005) para

Tipo de fraude	Descrição/cenário	Nível de risco	Mitigação proposta (ver secção 2.3)
	exemplo, um assinante no país A (tarifas elevadas) utiliza um SIM do país B (tarifas baixas) com tarifas de roaming favoráveis, nunca regressando à rede HPMN.		identificar assinantes com duração de roaming excessiva e contínua (por exemplo, >3 meses) e tomar medidas (por exemplo, sobretaxas, restrição de serviço). Requer ação da rede responsável dentro de 48 horas

Entre outros tipos de fraude, prevê-se que a Iniciativa de Roaming da CEDEAO seja suscetível aos seguintes riscos de fraude:

- **SIM Box** – Envolve a contornar do gateway internacional legítimo para terminar o tráfego internacional recebido através de um MSISDN local.

- **Falsificação de CLI e re-registro de número A** – Refere-se à deturpação deliberada de um número de chamada.

- **IRSF/PRS (Fraude de Partilha de Receitas Internacionais/Serviço de Tarifa Premium)** – Caracterizada pela geração de tráfego para destinos com tarifas elevadas e tarifas premium com a intenção de obter uma parte das receitas acumuladas.

- **Fraude de subscrição** – Ocorre através do acesso e utilização de serviços originalmente não pagos como parte da oferta de um utilizador através da manipulação do sistema.

- **Fraude de uso elevado** – Envolve o abuso de uso como resultado de falha de cobrança e/ou outros

- **Spam de SMS A2P** – Implica o envio de mensagens SMS em massa, geradas pelo sistema, através de rotas não autorizadas, contornando mecanismos de faturação legítimos e frequentemente utilizadas para comunicações não solicitadas ou fraudulentas.

2.3 Diretrizes gerais para gestão e prevenção de fraudes:

- Todos os SIMs de roaming de entrada devem ter pelo menos quinze (15) dias de histórico de utilização no seu país de origem antes de serem autorizados a utilizar roaming numa rede visitada. Os SIMs que não cumprirem este critério terão o

acesso a todos os serviços de roaming temporariamente negado. A rede visitada deve sinalizar e comunicar à rede de origem do utilizador em roaming de entrada qualquer utilizador em roaming que apresente atividades suspeitas para verificação adicional do seu estado. A rede visitada só concederá acesso de roaming após a verificação positiva do estado do utilizador em roaming.

- Todas as MNOs devem apresentar um relatório mensal detalhado sobre todas as atividades de gestão de fraudes, conforme a tabela no Apêndice 1.

A. Processo de gestão de fraudes por etapas:

1. Prevenção: As MNOs devem implementar controlos proativos (por exemplo, registo de SIM, incubação de SIM de 15 dias, troca NRTRDE).
2. Detecção: Monitorizar o tráfego 24 horas por dia, 7 dias por semana, em relação aos limites de KPI configurados no FMS.
3. Resposta: Após o alerta, suspender automaticamente ou manualmente o serviço de acordo com os gráficos RACI abaixo e iniciar a investigação.
4. Relatórios: Documentar o incidente nos portais nacionais e regionais (Apêndice 1).
5. Análise: A equipa regional correlaciona os dados para identificar tendências e refinar a lógica de detecção.
6. Aperfeiçoamento: Atualizar as regras e os controlos do FMS com base na análise.

B. Matriz RACI padrão (visão geral):

- Responsável (R): Entidade que executa a tarefa.
- Responsável (A): Entidade que responde em última instância pela conclusão correta.
- Consultada (C): Entidade que fornece informações.
- Informado (I): Entidade que é mantida atualizada sobre o progresso. *(O RACI detalhado é fornecido para cada KPI nas secções 2.3.1-7)*

C. Incubação SIM e limite mínimo de gastos:

- A regra do histórico de utilização de 15 dias (Secção 2.3) é um período de incubação obrigatório para estabelecer um comportamento legítimo do assinante.
- As ARN podem considerar, além disso, um *limite mínimo de gastos* na rede doméstica como um indicador adicional de credibilidade, garantindo o cumprimento das regulamentações de proteção ao consumidor.

D. Responsabilidade partilhada e escalonamento:

- A gestão da fraude é uma responsabilidade partilhada entre as redes domésticas e visitadas, conforme detalhado no RACI por KPI.
- Caminho de escalonamento: Equipa de Fraude da MNO -> NAFC Nacional -> RAFC Regional -> ARTAO/CEDEAO. Os prazos de escalonamento devem ser definidos no MoU

E. NRTRIE (Intercâmbio de dados de roaming quase em tempo real):

- A implementação de mecanismos NRTRIE é obrigatória para todas as MNOs, a fim de permitir a troca quase em tempo real de dados de utilização de roaming. Isto é fundamental para o controlo de crédito em tempo real, monitorização de fraudes e prevenção de surpresas nas contas, conforme complementado pelo Anti-FKPI_005. Todas as MNOs devem implementar sistemas para trocar ficheiros TAP (ou registos de dados padronizados equivalentes) para utilizadores em roaming no exterior dentro de um intervalo de tempo minimizado e mutuamente acordado (por exemplo, a cada 2-4 horas). Isto permite que a rede doméstica realize

monitorização de utilização quase em tempo real, controlo de crédito e deteção de fraudes com base nos dados de utilização reais da rede visitada, evitando assim surpresas nas contas e melhorando significativamente as capacidades de mitigação de fraudes. O meio e o formato escolhidos devem ser acordados em acordos bilaterais de roaming.

F. Funções na suspensão do serviço:

- A rede doméstica é responsável por suspender os serviços para os utilizadores em roaming com base em alertas recebidos das redes visitadas ou nos seus próprios controlos de crédito/fraude.

G. Penalidades por incumprimento:

- As NRAs, com o apoio da RAFC, devem desenvolver um quadro de penalidades financeiras condicionais para as MNOs que falham consistentemente em implementar controlos, responder a alertas ou fornecer os dados necessários, levando a disputas de faturação não resolvidas ou perdas de receitas evitáveis para os parceiros.

H. Controlos preventivos e políticas de utilização justa:

  - Limites de roaming grossista: As MNOs devem implementar limites financeiros grossistas para limitar a exposição financeira a atividades fraudulentas de roaming.
  - Política de uso justo (FUP): As MNOs podem implementar a FUP para:
    - Roaming permanente: Para impedir que os assinantes residam e operem permanentemente numa rede visitada.
    - Chamadas recebidas gratuitas: para evitar o abuso de ofertas de chamadas recebidas ilimitadas.
    - Promoções de retalho: para definir a duração e o âmbito de quaisquer ofertas de roaming com desconto.
  - Número máximo de contas por assinante: As redes domésticas devem implementar regras para limitar o número de SIMs de roaming ativos por assinante a um número razoável (por exemplo, 2-3).

- Aproveitamento de ferramentas avançadas: as MNOs são incentivadas a aproveitar os módulos de Inteligência Artificial (IA) e Aprendizagem Automática (ML) dentro do seu FMS para deteção proativa e preditiva de fraudes, indo além das regras estáticas baseadas em limites.

Controlos específicos de mitigação de fraudes e matriz de KPI

2.3.1 Anti-FKPI_001:

Monitorização do tráfego para destinos da lista de alertas por assinantes visitantes (roamers de entrada)

2.3.1.1 Descrição do controlo/KPI:

Durante o roaming numa rede visitada, o tráfego gerado por um roaming de entrada deve ser
monitorizado quanto a atividades fraudulentas IRSF/PRS. O controlo deve ser configurado no

FMS da rede visitante e monitorizado 24 horas por dia, 7 dias por semana. Os serviços devem ser suspensos para números que violarem os controlos e os detalhes devem ser comunicados à rede doméstica e à respetiva autoridade reguladora. (Consulte o Apêndice 2 para o limite de controlo aplicável)

A rede doméstica deve ser notificada para bloquear o intervalo de números suspeitos. Após um período sem resposta, a rede visitada deve bloquear completamente a rede desses números.

2.3.1.2 RACI (Responsável/Prestável contas/Consultar/Informar):

R - Operador da rede anfitriã/visitada
I – Comité Nacional Antifraude
A/C – Operador da rede doméstica.

2.3.2 ANTI-FKPI_002:

Monitorização de utilização elevada.
* Este KPI abrangerá as seguintes métricas, conforme previsto no apêndice 2:
*Média de SMS enviados por um utilizador em roaming dentro de uma hora e 24 horas.
*MOU médio de saída por um utilizador em roaming dentro de uma hora e 24 horas.
*Volume médio de utilização de dados por um utilizador em roaming dentro de uma hora e 24 horas.

2.3.2.1 Descrição do controlo/KPI:

As transações/volumes de roaming de entrada devem ser monitorizados quanto ao uso fora do limite.
Esses limites devem ser configurados no FMS da rede visitante e monitorados 24 horas por dia, 7 dias por semana.
A rede doméstica deve ser notificada para suspender os serviços dos assinantes que ultrapassarem o limite.

***Implementar uma rede doméstica responsável pelo bloqueio de voz, dados e SMS.**

2.3.2.2 RACI (Responsável/Prestável contas/Consultar/Informar):

R - Operador da rede anfitriã/visitada
I – Comité Nacional Antifraude
A/C – Rede doméstica

2.3.3 ANTI-FKPI_003:

Monitorização do Desvio de Terminação de Tráfego Internacional (SIM Box).

2.3.3.1 Descrição do controlo/KPI:

Os roamers de entrada devem ser monitorizados quanto a atividades de desvio de terminação de tráfego internacional
tanto na rede doméstica como na rede visitante. Deve ser implementada uma solução de deteção de SIM Box
ser implantada e configurada para sinalizar esses cartões SIM.
Os SIMs detetados devem ser removidos da base de dados VLR da rede anfitriã e os detalhes relevantes devem ser comunicados à rede doméstica.

*A rede visitada é capaz de detetar e sinalizar os utilizadores em roaming que contornam o sistema no seu VLR, em coordenação com a rede doméstica. É imperativo que a rede visitada comunique todas as deteções à rede doméstica para garantir esforços sincronizados de mitigação de fraudes.
*Após a deteção, a rede visitada deve notificar imediatamente a rede doméstica, iniciando o bloqueio dos cartões SIM identificados**.**

2.3.3.2 RACI (Responsável/Prestável contas/Consultar/Informar):

R - Operador de rede anfitrião/visitado
I – Comité Nacional Antifraude
A/C – Rede doméstica

2.3.4 ANTI-FKPI_004:

Monitorização de comportamentos e/ou padrões de chamadas invulgares.

2.3.4.1 Descrição do controlo/KPI:

Devem ser configuradas regras no Sistema de Gestão de Fraudes (FMS) para monitorizar e sinalizar
comportamentos e padrões incomuns de chamadas durante o roaming. Esses comportamentos podem incluir, mas
não se limitam a:

- **Primeira chamada feita após o registo em roaming**: pode indicar ativação automática da SIM Box.
- **Chamadas com duração invulgarmente longa**: pode sugerir geração artificial de tráfego ou aumento de chamadas.
- **Chamadas iniciadas através da funcionalidade de reencaminhamento de chamadas**: frequentemente exploradas em cenários de desvio.
- **Elevado volume de chamadas de curta duração**: típico de SIM Box ou fraude de terminação.
- **Chamadas para destinos de alto risco ou números com tarifas premium**: pode indicar fraude de partilha de receitas.

- **SIMs que geram tráfego sem eventos de mobilidade correspondentes**: sugere uso não humano.

- **Atividade de roaming inconsistente com o perfil ou histórico do assinante**: um sinal de alerta para uso indevido.

- **Vários SIMs exibindo padrões de chamadas idênticos**: pode indicar fraude coordenada.

Os serviços devem ser suspensos para números que violem o controlo e os detalhes comunicados à rede doméstica.

2.3.4.2 Responsável, Contabilizável, Consultar, Informar (RACI):

R - Operador da rede anfitriã/visitada e rede doméstica
I – Comité Nacional Antifraude
A/C – Rede doméstica

2.3.5 ANTI-FKPI_005:

Intercâmbio de dados de roaming (NRTRDE).

2.3.5.1 Descrição do controlo/KPI:

As transações de roaming de saída são normalmente processadas e faturadas pelas respetivas Operadoras Domésticas. No entanto, o registo inicial dessas transações é realizado pela Rede Visitada. Portanto, é essencial que a Rede Visitada compartilhe prontamente essas informações com a Rede Doméstica do assinante por meio de um canal de comunicação acordado. Isso garante o monitoramento eficaz dos limites de uso e crédito e ajuda a evitar surpresas desagradáveis na conta no final do ciclo de faturamento.

2.3.5.2 Responsável/Responsável/Consultar/Informar (RACI):

R/A - Operador da Rede Anfitriã/Visitada
C – Rede doméstica

2.3.6 ANTI-FKPI_006:

Definir e monitorizar o limite de utilização de dados.

2.3.6.1 Descrição do controlo/KPI:

Os assinantes de roaming de entrada acedem aos dados através do Nó de Suporte GPRS do Gateway do Visitante (GGSN). Um limite em termos de volume de utilização de dados deve ser acordado e definido pelas Redes Visitantes para os respetivos assinantes parceiros como base para a monitorização e controlo de utilização elevada.
O limite acordado deve ser configurado no FMS da rede visitante para um monitoramento eficaz.
Nota:
** O que importa é o volume e não o custo, uma vez que cada operador móvel tem tarifas específicas.

Os números sinalizados devem ser comunicados à Rede Doméstica**.**

2.3.6.2 Responsável/Responsável/Consultar/Informar (RACI):

R/A - Operador da Rede Anfitriã/Visitada
I – Comité Nacional Antifraude
C – Rede doméstica

2.3.7 ANTI-FKPI_007:

Prevenir a troca de SIM para Roamers de saída.

2.3.7.1 Descrição do controlo/KPI:

As MNOs devem proibir a troca de cartões SIM enquanto o número do assinante estiver em roaming internacional
. Tal atividade representa um risco significativo para a integridade do serviço, prevenção de fraudes e
precisão da faturação.

Os fraudadores empregam essa estratégia para assumir o controle de contas de serviço legítimas para fins fraudulentos
.

2.3.7.2 Responsável/Responsável/Consultar/Informar (RACI):

R/A - Rede doméstica.
I – Comité Nacional Antifraude

2.4 Matriz de Suporte Técnico e Escalonamento

A. Balcões dedicados à fraude:
Cada ANR e MNO deve estabelecer um balcão dedicado à fraude 24 horas por dia, 7 dias por semana, com detalhes de contacto publicados (e-mail, telefone) partilhados com todas as redes parceiras e o RAFC.
B. Caminho de escalonamento padrão:

Nível de gravidade	**Critérios**	**Ação e cronograma**	**Caminho de escalonamento**
Nível 1 (crítico)	Grande perda de receita (>$10 mil), ataque contínuo, violação crítica do sistema.	Ação imediata necessária.	Gabinete de Fraudes da MNO -> Gabinete de Fraudes da MNO Parceira -> NAFC -> RAFC (dentro de 1 hora)
Nível 2 (Grave)	Perda significativa de receita, vários MSISDNs envolvidos.	Ação dentro de 2 a 4 horas.	Gabinete de Fraudes da MNO -> Gabinete de Fraudes da MNO Parceira -> NAFC (no prazo de 4 horas)

Nível de gravidade	Critérios	Ação e cronograma	Caminho de escalonamento
Nível 3 (Menor)	Incidente isolado, baixo impacto financeiro.	Ação dentro de 24 horas.	Gabinete de Fraudes da MNO -> Gabinete de Fraudes da MNO Parceira (dentro de 24 horas)

2.5 Notificação de fraudes

Deve ser implementada uma ferramenta/portal centralizado para a comunicação direta de incidentes pelas respetivas MNOs em todos os países com acordos de roaming.

Notificação obrigatória: independentemente de sinais de fraude individuais ou mecanismos de deteção, cada MNO é obrigada a enviar relatórios de deteção de fraude através do portal centralizado. Este portal funciona independentemente de qualquer FMS específico da operadora para garantir consistência e transparência nas notificações.

Formação e integração: Todos os pontos de contacto únicos (SPOCs) designados das MNOs participantes receberão formação sobre a utilização adequada do portal e procedimentos padronizados para a comunicação de incidentes fraudulentos. Isto garante a uniformidade na apresentação de dados e melhora a colaboração entre redes na mitigação da fraude**.**

Os dados serão analisados pela Equipa Regional e os resultados servirão como verificação de incidentes que serão sinalizados ou não pela solução FMS Regional e também para ajudar no ajuste da lógica das respetivas soluções FMS (MNO e NAFC) ao longo do tempo.

ANEXO 1

Os incidentes de fraude registados pelas MNOs nos respetivos Estados-Membros relacionados com a Iniciativa Regional de Roaming da CEDEAO devem ser comunicados mensalmente através do modelo abaixo:

Data do incidente	Tipo de fraude	Número de MSISDNs envolvidos	Nome/país da operadora de origem	Receitas perdidas (USD)	Receita perdida evitada (USD)	Ação tomada	Estado do incidente

ANEXO 2

Limites de controlo para KPIs de fraude (dados de amostra de operadoras móveis do Benim e Gana)

	Número de preocupações	
Tipo de fraude	**Sim**	**Não**
SIM Box	6	0
Caixa SIM internacional	6	0
Falsificação de CLI e reenvio de número A	5	1
IRSF/PRS (fraude internacional de partilha de receitas/serviço de tarifa premium)	6	0
Fraude de assinatura	4	2
Fraude por uso excessivo	6	0
Spam de SMS A2P (incluindo chamadas flash)	6	0

	Percentagem	
Tipo de fraude	**Sim**	**Não**
Caixa SIM	100	0
Caixa SIM internacional	100	0
Falsificação de CLI e reenvio de número A	83	17
IRSF/PRS (Fraude internacional de partilha de receitas/serviços com tarifas premium)	100	0
Fraude na assinatura	67	33
Fraude de uso elevado	100	0
Spam de SMS A2P (incluindo chamadas flash)	100	0

	Número de preocupações	
KPI	**Sim**	**Não**
Monitorização do tráfego para destinos da lista de favoritos por assinantes visitantes (roamers de entrada)	5	1
Monitorização de utilização elevada	6	0
Média de SMS enviados por um utilizador em roaming de entrada dentro de uma hora e 24 horas	3	3
MOU médio de saída por um utilizador em roaming de entrada dentro de uma hora e 24 horas	3	3
Volume médio de utilização de dados por um utilizador em roaming de entrada dentro de uma hora e 24 horas	3	3
Monitorização do desvio de tráfego internacional (SIM Box)	6	0
Monitorização de comportamentos e/ou padrões de chamadas invulgares	5	1
Troca de dados de roaming (NRTRDE/CAMEL)	6	0

	Número de preocupações	
KPI	**Sim**	**Não**
Monitorização do tráfego para destinos da lista de favoritos por assinantes visitantes (roamers de entrada)	83	17
Monitorização de utilização elevada	100	0
Média de SMS enviadas por um utilizador em roaming de entrada num período de uma hora e 24 horas	50	50%
MOU médio de saída por um utilizador em roaming de entrada dentro de uma hora e 24 horas	50	50
Volume médio de utilização de dados por um utilizador em roaming de entrada num período de uma hora e 24 horas	50	50
Monitorização de desvio de tráfego internacional (SIM Box)	100	0
Monitorização de comportamentos e/ou padrões invulgares nas chamadas	83	17
Troca de dados em roaming (NRTRDE/CAMEL)	100	0

Definir e monitorizar o limite de utilização de dados	3	3			Definir e monitorizar o limite de utilização de dados	50	50
Impedir a troca de SIM para roaming de saída	1	5			Prevenir a troca de SIM para utilizadores em roaming no estrangeiro	17	83
Número médio diário de números diferentes chamados	3	3			Número médio diário de números diferentes chamados	50	50
O número médio de chamadas efetuadas por dia	3	3			Número médio de chamadas efetuadas por dia	50	50
O número médio de chamadas recebidas por dia	3	2			Número médio de chamadas recebidas por dia	50	33
A proporção de MOC/MTC por IMSI	1	5			A proporção de MOC/MTC por IMSI	17	83
A duração média das chamadas efetuadas por dia	3	3			A duração média das chamadas efetuadas por dia	50	50
A duração média das chamadas recebidas por dia	4	2			A duração média das chamadas recebidas por dia	67	33
Monitorizar o comportamento do consumidor para detetar atividades fraudulentas	5	1			Monitorizar o comportamento do consumidor para detetar atividades fraudulentas	83	17
As linhas ISDN devem ser bloqueadas para impedir o acesso não autorizado	1	5			As linhas ISDN devem ser bloqueadas para impedir o acesso não autorizado	17	83
Número médio de chamadas feitas diariamente	2	4			Número médio de chamadas feitas diariamente	33	67
Número médio de chamadas recebidas diariamente	2	4			Número médio de chamadas recebidas diariamente	33%	67%
Subsídio acordado para variação	1	5			Margem acordada para variação	17	83

ANEXO 3

Três prazos para a implementação da estratégia do mecanismo regional antifraude

Esta estrutura de gestão de fraudes proposta deve ser implementada de acordo com os seguintes prazos para lidar com quaisquer fraudes e consequências de segurança a serem identificadas.

PRINCIPAIS ATIVIDADES	DETALHES DAS AÇÕES A REALIZAR	CALENDÁRIO	PARTES INTERESSADAS	COMENTÁRIOS

1. Criação de Comités Nacionais Antifraude	Cada país deve criar um Comité Nacional Antifraude	Janeiro de 2022	NRA	Concluído
2. Criação de Comités Regionais Antifraude	Cada país deve nomear dois (2) especialistas para integrar o comité regional antifraude	Outubro de 2021	GANA	Concluído
3. Identificar potenciais tipos de fraude	O comité regional antifraude irá discutir e identificar potenciais tipos de fraude	Abril de 2022	Comité regional antifraude	Concluído
4. Avaliar os quadros jurídicos existentes	Cada país deve avaliar as suas leis nacionais para descobrir se existem disposições específicas para processar e denunciar os autores de fraudes nas telecomunicações.	30 de junho de 2022	ANR	Concluído
5. Desenvolvimento de diretrizes antifraude	Elaborar princípios regionais de combate à fraude	31 de julho de 2022	Comité regional antifraude /	Concluído
6. Infraestrutura de gestão de fraudes dos Estados-Membros	Recolher o estado das plataformas nacionais existentes e as suas características	31 de julho de 2022	NRA / MNO	Parcialmente concluído
7. Implantação de um sistema/ferramenta(s) sub-regional(is) de combate à fraude	Conceção, implementação e configuração das regras do sistema.	A determinar	GANA+CEDEAO/WATRA	A organizar
8. Desenvolver protocolos padronizados para orientar os Estados-Membros no tratamento de números fraudulentos detetados pelos Estados-Membros.	Diretrizes que descrevem como as atividades fraudulentas detetadas devem ser tratadas	A determinar	GANA	Organizar
9. Desenvolver e implementar requisitos adequados para a comunicação de fraudes	Deve ser implementada uma ferramenta/portal central de denúncia para a denúncia direta de incidentes pelas respetivas operadoras móveis em toda a sub-região	A determinar	GANA	Organizar
10. Monitorizar Sistema/mecanismo regional antifraude	Analisar os dados sobre todas as atividades fraudulentas denunciadas para saber quais foram interrompidas e quais persistem.	A determinar	GANA	Organizar

ANEXO 4 - SIGLAS

A2P SMS: SMS de aplicação para pessoa

Anti-FKPI: Indicador-chave de desempenho antifraude

CLI Spoofing: Falsificação da identidade da linha chamadora

ECOWAS: Comunidade Económica dos Estados da África Ocidental

FMS: Sistema de Gestão de Fraudes

FUP: Política de Utilização Justa

GGSN: Nó de suporte GPRS de gateway

HPMN: Rede móvel pública doméstica

Fraude IRSF/PRS: Fraude Internacional de Partilha de Receitas / Fraude de Serviços com Tarifas Premium

MNO: Operador de Rede Móvel

MSISDN: Número de Diretório Internacional de Assinantes de Estação Móvel

NAFC: Comité Nacional Antifraude

NRA: Autoridade Reguladora Nacional

NRTRDE: Intercâmbio de dados de roaming quase em tempo real

RAFC: Comité Regional Antifraude

Matriz RACI: Um quadro de atribuição de responsabilidades que define as funções e responsabilidades das tarefas. Significa Responsável, Responsável, Consultado e Informado.

TAP: Procedimento de Transferência de Conta

VLR: Registo de Localização de Visitantes

VPMN: Rede móvel pública visitada

ARTAO: Assembleia dos Reguladores de Telecomunicações da África Ocidental